Strategic Deterrence Paper

State-Sponsored Influence Operations in the Digital Age: The Challenge of Deterrence

Kjersti Soberg

PS 633 - Strategic Deterrence: Past, Present, Future

July 30, 2023

Abstract

Cybersecurity policy issues have gained attention in Congress in recent years, with a focus on deterrence and organizational readiness. Legislation has been introduced to address these concerns and redefine the roles and responsibilities of both the government and private sector in ensuring the nation's cyber readiness. While the range of cyber threats is vast, this paper aims to specifically highlight the weaponization of social media through state-sponsored influence. The rapidly evolving landscape of cyber threats has necessitated a critical reevaluation of cyber deterrence strategies, particularly in the wake of Russia's election meddling in 2016. This report argues that the U.S. must continue to adapt its cyber deterrence strategy to address the growing threat of sophisticated and persistent cyberattacks on our nation's democracy through social media. It highlights the need for proactive, adaptive, and multifaceted deterrence strategies to effectively safeguard national interests today, and for generations to come.

Evolving Threats & Increasing Relevance

The rapidly evolving landscape of cyber threats has necessitated a critical reevaluation of cyber deterrence strategies. In 2018, Congress passed legislation to create the Cybersecurity and Infrastructure Security Agency (CISA). This marked a significant milestone in the U.S.'s efforts in addressing the ever-evolving threats, as the bill was passed with unanimous support[1]. Against the backdrop of the 2016 election meddling by Russia, which highlighted the severe impact of state-sponsored cyber-attacks on democratic processes and national security, the creation of a dedicated agency like CISA was timely. State-sponsored cyber-attacks have deep socio-economic impacts and can shape the course of history. They can influence elections, destabilize governments, shape public perception, and disrupt critical infrastructure. Moreover, social media can be used nefariously by threat actors that wish to shape future generations[2]. In the future, we can expect to see even more sophisticated and targeted attacks, as well as the rise of new forms of cyber warfare.

Timeliness

A recent study estimates that 308.27 million Americans use social media today and that will continue to trend upwards within the next five years[3]. Social media has unquestionably changed the world. It has made it easier to connect with each other, share information, fostered a more interconnected global community, and even advocate for change.[4] However, it can also be used for spreading misinformation, cyberbullying, hate speech, and radicalization.[5] It has not only changed the way we live our everyday lives, but it has made us redefine how we perceive national security. Historically, national security was primarily defined by physical threats; however, the threat landscape has changed in the digital age. This has led to a redefinition of national security, as governments and organizations now need to consider the threat of social

[1] Department of Homeland Security, "Congress Passes Legislation Standing Up Cybersecurity Agency in DHS." 2018.

[2] Patnaik and Litan. "TikTok Shows Why Social Media Companies Need More Regulation," 6-7.

[3] Dixon, "Social media users in the United States 2019-2028," 2023.

[4] Singer and Brooking. *LikeWar: the Weaponization of Social Media*, 2019, 24.

[5] Thompson, "Radicalization and the Use of Social Media," 2012, 167.

media cyberattacks as well as traditional threats.

In 2019, the Senate Select Committee on Intelligence released its findings on Russia's meddling in the 2016 U.S. presidential election. It stated that the Russian government "directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure at the state and local level." [6] It was also reported that Russian operatives used social media to "conduct an information warfare campaign designed to spread disinformation and societal division."[7] In recent study from the University of Oxford, statistics show that "some 70 countries around the world are engaged in manipulating social media to serve domestic and foreign policy ends. This is up from 48 countries in 2018 and 28 countries in 2017."[8] The rise of social media has created a new and complex threat landscape for national security. This new landscape warrants a well-designed and multifaceted deterrence plan to mitigate these threats and safeguard the democratic processes.[9]

Analysis

The U.S. has recognized the severe consequences that state-sponsored cyberattacks and has adapted its cyber deterrence strategies to address the growing sophistication and complexity of cyber threats. Not only was CISA created in 2018, but the Cyberspace Solarium Commission (CSC) was established in 2019 to "develop a consensus on a strategic approach to defending the U.S. in cyberspace.[10] In 2021, the CSC released a white paper specifically for countering disinformation.[11] It focused on how disinformation is a complex cyberspace threat to democracy and outlined seven specific recommendations to combat the threat. Notably, it addressed how disinformation has been "seen by many an issue largely separate from cybersecurity and cyber policy," and that "policymakers do themselves a disservice by continuing to differentiate between the two when our adversaries do not".[12]

The leaders of the intelligence community today have addressed adversarial foreign influence in reports such as the ODNI's *Annual Threat Assessment.* The 2023 assessment states,

> Russia presents one of the most serious foreign influence threats to the United States, because it uses its intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances and increase its sway around the world, while attempting to undermine U.S. global standing, sow discord inside the United States, and influence U.S. voters and [decisionmaking].[13]

While Russia's activities have attracted a lot of attention since 2016, China's subversions are far

[6] Select Committee on Intelligence United States. "Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections," Volume 1: 2019, 3.

[7] Ibid, Volume 2, 3.

[8] Helmus, "7. Social Media and Influence Operations Technologies: Implications for Great Power Competition," 2020, 153.

[9] Lopez, "Deterrence in Cyberspace Requires Multifaceted Approach," 2019.

[10] Cyberspace Solarium Commission, 2023.

[11] Cyberspace Solarium Commission, 2021, 4.

[12] Ibid.

[13] Office of the Director of National Intelligence, 2023 Annual Threat Assessment, 15.

more sophisticated.[14] The *Annual Threat Assessment* addressed China's capabilities in stating that it is "currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks."[15] China has significantly bolstered its cyber capabilities over the past decade, presenting a formidable threat to the U.S in cyberspace. Urgent questions remain regarding the readiness of the U.S. to counter this challenge, including resourcing military cyber forces and the scope of cybersecurity cooperation between the public and private sectors.[16]

Deterrence Theory and Cyber

In recent years it has been questioned whether or not cyber deterrence is even possible, given the complexity of the threat. To examine this, it is necessary to understand what deterrence theory is. Colonel Timothy McKenzie wrote,

> There is no single definition of deterrence or shortage of theories for its practical application. Joint doctrine defines deterrence as the 'prevention of action by either the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits.' Deterrent options can be either passive or active in nature.[17]

These "deterrent options" can be understood as deterrence by denial or deterrence by punishment, or as McKenzie stated, passive and active deterrence.[18] Passive deterrence in the cyber domain refers to making attacks more costly and difficult to execute, rather than actively preventing them. Much like the moat around a castle, it does not stop an enemy from attacking, but it makes it much harder to succeed. Conversely, active deterrence "threatens retaliation or some type of undesirable response to a [cyberattack] or incident."[19] When speaking about deterrence in the cyber domain, deterrence by entanglement is also applicable, as it seeks to promote responsible state behavior by emphasizing the benefits cooperation on mutual interests.[20] This application of deterrence is also necessary to consider in the age of globalization.

While deterrence options are more readily available to passively safeguard cyber infrastructure (i.e., implementing security controls such as firewalls, encryption, intrusion detection systems etc.), it is more difficult to apply those same deterrence strategies when tackling the threat of state-sponsored influence on social media. This is because social media is more dynamic and constantly evolving, and it is not always clear who is responsible for the

[14] Holstein and McLaughlin, *Battlefield Cyber: How China and Russia are Undermining Our Democracy and National Security*, 2023.

[15] Ibid, 10.

[16] U.S.-China Economic and Security Review Commission. "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States,"418.

[17] McKenzie, *Is Cyber Deterrence Possible? 2017,* 2.

[18] Libicki, Cyber Deterrence, 7; Mazarr, "Understanding Deterrence," 1.

[19] McKenzie, 2.

[20] Fischer, "The Concept of Deterrence and Its Applicability in the Cyber Domain", 2019, 90; Nye, "Deterrence and dissuasion in cyberspace," 2916, 56.

disinformation. Additionally, these attacks may have a variety of motives.[21] If the purpose of a threat actor's weaponization of social media is to sow discord and division, then traditional deterrence methods become more difficult.

The Challenge of Deterrence in the Digital Age

Strategic deterrence is a concept that has evolved over time, especially in the digital age. It is understood that the basic idea of deterrence is to convince an adversary that the costs of attacking you will outweigh the benefits. During the Cold War, strategic deterrence was based on the threat of nuclear retaliation. With both the Soviet Union and the U.S. in possession of nuclear weapons, this paved the path for the threat of mutually assured destruction (MAD). This idea of deterrence is not applicable with the sophistication of threats in the digital age which has necessitated non-nuclear deterrence strategies to be developed. How, then, are these non-nuclear strategies used to prevent conflict when looking through the lens of state-sponsored influence on social media?

In this case, the threat is asymmetrical. It leverages the advantages of anonymity, global reach, and the ability to quickly disseminate information to a vast audience without the need for a direct military confrontation. It exploits the openness and interconnectedness of social media platforms to create asymmetric effects, affecting public sentiment, destabilizing democratic processes, and potentially causing conflict[22]. Today, policymakers "lack good information about the nature of the problem they seek to solve" when combating the threat of state-sponsored influence operations.[23] This makes developing specific strategic deterrence strategies exceedingly difficult without a better understanding of the effects of these influence operations and the tools and techniques that can be used to counter them.

Conflict

There is no conclusive evidence that a cyber-attack or state-sponsored meddling has threatened conventional war within the U.S. that we are aware of. However, in theory, influence campaigns through social media could incite domestic unrest or a civil war, which is akin to warfare. An asymmetrical attack is not conventional, but that is the crux of strategic deterrence in the digital age. The rise of cyberwarfare and state-sponsored influence operations has made it more difficult to deter conflict. These new threats challenge our traditional understanding of deterrence, and there is an ever-growing need to develop new strategies to address them. While the future of warfare may be uncertain, we need to be prepared for new and unconventional threats.

[21] Libicki, 210.

[22] Levite et al., "Managing U.S.-China Tensions Over Public Cyber Attribution," 2022, 36.

[23] Bateman et al., "Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research," 2021.

Conclusion

The rapidly evolving landscape of cyber threats has necessitated a critical reevaluation of cyber deterrence strategies. In order for the U.S. to counter the asymmetrical threat of state-sponsored influence, comprehensive approaches are required, including bolstering cyber defenses, investing in cybersecurity capabilities, enhancing public awareness about disinformation and foreign influence, and promoting digital literacy among citizens. Additionally, policymakers must consider the complexities of the cyber domain and work collaboratively with the private sector, social media platforms, and international partners to effectively mitigate the risks posed by the threat. As technology continues to advance, the challenges posed by state-sponsored influence operations will only become more complex. The U.S. must adopt proactive, adaptive, and multifaceted deterrence strategies to effectively safeguard national interests today and for generations to come.

Bibliography

Bateman, Jon, Elonnai Hickok, Laura Courchesne, Isra Thange, and Jacob N. Shapiro. 2021. "Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research." Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824.

Cyberspace Solarium Commission. 2021. "Countering Disinformation in the United States. https://www.solarium.gov/public-communications/disinformation-white-paper

Cyberspace Solarium Commission. "Cyberspace Solarium Commission." Accessed July 28, 2023. https://www.solarium.gov.

Department of Homeland Security. "Congress Passes Legislation Standing Up Cybersecurity Agency in DHS." November 13, 2018. https://www.dhs.gov/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs.

Dixon, S. "Social media users in the United States 2019-2028." Statista, March 21, 2023. https://www.statista.com/statistics/278409/number-of-social-network-users-in-the-united-states/.

Fischer, Manuel. "The Concept of Deterrence and Its Applicability in the Cyber Domain." Connections 18, no. 1/2 (2019): 69–92. https://www.jstor.org/stable/26948850. https://www.jstor.org/stable/pdf/26948850.pdf?refreqid=excelsior%3A5cbe108ac8f615c28c93a11314650403&ab_segments=&origin=&initiator=&acceptTC=1.

Helmus, Todd C. 2020. "7. Social Media and Influence Operations Technologies: Implications for Great Power Competition." Strategic Assessment 2020: 153-166. https://ndupress.ndu.edu/Portals/68/Documents/Books/SA2020/SA-2020_Ch7.pdf.

Holstein, William J., and Michael McLaughlin. 2023. *Battlefield Cyber: How China and Russia are Undermining Our Democracy and National Security.* United States: Prometheus.

Levite, Ariel E., Lu Chuanying, George Perkovich, and Fan Yang, eds. 2022. *Managing U.S.-China Tensions Over Public Cyber Attribution.* The Carnegie Endowment for International Peace and Shanghai Institutes for International Studies. https://carnegieendowment.org/files/Perkovich_et_al_Cyber_Attribution_web.pdf.

Libicki, Martin C. Cyberspace in Peace and War. Second edition. Annapolis, Maryland: Naval Institute Press, 2021.

Lopez, C. Todd. "Deterrence in Cyberspace Requires Multifaceted Approach." U.S. Department of Defense, September 11, 2019. https://www.defense.gov/News/Feature-Stories/story/Article/1957874/deterrence-in-cyberspace-requires-multifaceted-approach/.

Mazarr, Michael J. 2018. "Understanding Deterrence." The RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.

pdf.

McKenzie, Timothy. 2017. *Is Cyber Deterrence Possible?* Air University, Air University Press. https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF.

Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." International security 41, no. 3 (2016): 44-71. https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf.

Office of the Director of National Intelligence. 2023 Annual Threat Assessment of the US Intelligence Community. February 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

Patnaik, Sanjay and Robert E. Litan. “Tiktok Shows Why Social Media Companies Need More Regulation.” The Brookings Institution, Policy Brief, May 2023. https://www.brookings.edu/wp-content/uploads/2023/05/20230511_CRM_Patnaik Litan_TikTok_FINAL.pdf.

Senate Select Committee on Intelligence United States. 2019. “Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections.” Volume 1: Report 116-XX. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

Senate Select Committee on Intelligence United States. 2019. “Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections.” Volume 2: Report 116-XX. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Singer, P. W., and Emerson T. Brooking. *LikeWar: the Weaponization of Social Media*. Boston: Mariner Books, Houghton Mifflin Harcourt, 2019.

Thompson, Robin L. "Radicalization and the Use of Social Media." Journal of Strategic Security 4, no. 4 (2012): 167-190. DOI: http://dx.doi.org/10.5038/1944-0472.4.4.8. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1146&context=jss.

U.S.-China Economic and Security Review Commission. “China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States.” 418-518, Accessed July 29, 2023. https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf