National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Enhancing Partnerships: Integrated Deterrence in the Cyber Domain

Lieutenant-Colonel Christl A. Kroeten

JCSP 49 DL

Exercise Solo Flight

Disclaimer

PCEMI n° 49 AD

Exercice Solo Flight

Avertissement

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 DL - PCEMI n° 49 AD
2022 - 2024

Exercise Solo Flight – Exercice Solo Flight

Enhancing Partnerships: Integrated Deterrence in the Cyber Domain

Lieutenant-Colonel Christl A. Kroeten

ENHANCING PARTNERSHIPS:
INTEGRATED DETERRENCE IN THE CYBER DOMAIN

The U.S. 2022 National Security Strategy (NSS) highlighted Integrated Deterrence (ID) as the cornerstone of the security strategy. ID is a whole of government approach crossing domains, regions, spectrum of conflict, and combined with allies and partners.[1] The U.S. National Defense Strategy (NDS) lays out how the U.S. intends to implement deterrence in conjunction with partners: by denial, resilience, and cost imposition across all domains.

By adopting a whole-of-government, cross-domain approach to deterrence, the U.S. DoD must contend with implementing ID in cyberspace. Current U.S. networked capabilities have significant personnel shortages and lack of robust infrastructure to support cyber initiatives. Additionally, 42% of global companies reported experiencing "cyber-fatigue" resulting in apathy toward proactively defending against cyber-attacks.[2] To effectively implement ID, allies and partners must not only recognize the importance of cyber-capabilities but be willing to implement capabilities synchronized to communicate deterrence posture and combined resolve.

The international community must strengthen cooperation and information sharing to build a credible integrated cyber-deterrence strategy. The simple costs of cyber-attacks continue to escalate. In 2023 the cost of resolution and repair for a single data breach averaged $4.45 million.[3] Even when attribution can be traced, the chance that a cyber-attacker is prosecuted is only about 0.05%.[4] To maintain international security, allied States must work together to not only respond, but deter malign cyber-activity.

This paper argues that the conventionally based concept of ID is applicable in cyberspace, particularly due to the emphasis on leveraging allies and partners. However, this is also a significant weakness to the strategy. Integrating cyber deterrence capabilities will take significant time, resources, and commitment that may exceed the capability and will of the allied community to fully implement.

An overview of the threats in cyberspace are presented, followed by a description of conventional and integrated deterrence strategies. The elements of the NDS ID strategies are examined further from the cyber perspective. Considerations of international perception and the role of information management are discussed and recommendations for action provided.

The Cyber Domain

Among the most significant international security challenges is threats in the cyber domain. Cyberattacks increased significantly in 2023, impacting more than 120 countries

[1] President, *National Security Strategy* (Washington, DC: White House, 2002), 4-6, https://www.witehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Adminisrations-National -Security-Strategy-10.2022.pdf
[2] Rob Sobers, "161 Cybersecurity Statistics and Trends [updated 2023]," *Varonis*, November 29, 2023, https://www.varonis.com/blog/cybersecurity-statistics
[3] *Ibid*
[4] *Ibid*

particularly in government-sponsored espionage and influence actions.[5] NATO nations accounting for almost 50% of these attacks with 40% targeted at organizations supporting critical infrastructure including healthcare and water supply.[6] While addressing attacks and building cyber security capabilities is essential, consideration of options to deter attacks should be included in cyber strategies.

There are several commissions and initiatives to develop international standards for actions, targeting, and potential consequences for cyber actions.[7] The United Nations and NATO have specific groups exploring preparedness, evaluating countermeasures, and working to identify and assign attribution. Many, but not all, persistent threat capabilities are aligned with a specific originating State, with tell-tale markers and cyber-behaviors enabling identification.[8] However, the desire to obscure attribution has increased the use of proxy groups and cyber-crime organizations to achieve State goals.

Attribution of cyber-attacks to specific States or groups takes time and resources that may not be available to all partners and allies. Determining attribution is complex as many cyber-attacks are actioned across sovereign borders, further complicating legal considerations.[9] Operating across legal jurisdictions or using proxy servers helps to hide attack origins and confuse attribution attempts.[10] Not all countries have invested in sophisticated cyber-capabilities designed to trace and identify attackers. Even if identified, the victim of a cyber-attack may not legally be able to respond.

Consequences may not be able to be brought to bear without an internationally recognized standard of conduct and the capability and willingness to impose consequences. Enhancing readiness, hardening networks, developing countermeasures, and identifying malign actors relies on shared information and leveraging partner capabilities.[11] With the number and severity of attacks on private companies continuing to grow, public-private partnerships can foster innovative solutions to improve security.[12] Sharing information about types of attacks, targets, tactics, and patterns will enhance collective security.

Even if international norms are established and organizations set in place to provide oversight, cyber activities require skilled artisans capable of bringing to bear both public and

---

[5] Tom Burt, "Espionage Fuels Global Cyberattacks," *Microsoft On the Issues*, Oct 5, 2023, https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/
[6] Anna Ribeiro, "US Critical Infrastructure Sector Faces Cyber Threats Surge in 2023, Calls for Urgent Action, Enhanced Measures," *Industrial Cyber*, Dec 10, 2023, https://industrialcyber.co/features/us-critical-infrastructure-sector-faces-cyber-threats-surge-in-2023-calls-for-urgent-action-enhanced-measures/
[7] Shalini Lamba, Vibhu Tripathi, Ansh Kapoor, "Cyberwar: A New Battle Ground," *Advances in Engineering Science and Management*, 1, (2023):149-156
[8] Anh V. Vu, Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton, Ross Anderson. "Getting Bored of Cyberwar: Exploring the Role of Civilian Hactivists in the Russia-Ukraine Conflict." 2023. https://arxiv.org/pdf/2208.10629.pdf
[9] *Ibid*
[10] Mohammed B. E. Saaida, "The Use of Cyber Warfare and its Impact on International Security," *Science For All Publications* 1, no. 1 (2023):1-5
[11] *Ibid*
[12] Cybersecurity & Infrastructure Security Agency, "Partnerships and Collaboration," https://www.cisa.gov/topics/partnerships-and-collaboration

private capabilities within the scope of international security.[13] While many States have cyber agencies, organizations, and commands, balancing security with talent management and credentialing as technologies continue to evolve is particularly difficult.[14] States with more limited cyber-capabilities may rely on partners with greater capability, further straining an already stretched workforce.

Dynamic and evolving threats in the cyber domain present distinct challenges to international security. The expansion of cyber-attacks to include health care, public services, and supply chains highlights the vulnerabilities of the status quo.[15] By proactively addressing collaboration and integrating cyber resources, States can set informal norms for cyber behavior that can be later shaped into formal international norms.

Deterrence

Deterrence is a strategy intended to prevent an adversary from taking an undesirable action, particularly as related to conventional warfare.[16] Three key elements of deterrence are the capability of the deterring entity to affect the deterrence, the communication of that capability such that the potential adversaries recognize there is a deterrence effort, and the willingness of the deterring entity to bring consequences to bear. Perspectives of deterrence in application can be broken down to examine strategy variations.

To successfully deter an adversary, several factors must be considered. First, the deterring actor must have the capability to affect deterrence; meaning the State must be believed to have a capability in order for it to be an effective deterrent. In the U.S. strategic documents, nuclear capabilities are presented as the backstop of deterrence strategies.[17] However, there are a broad spectrum of alternative options able to be brought to bear, not only militarily, but also economically and diplomatically. Deterrence capabilities rarely hinge on a single catastrophic capability but employ a range of options based on the type or severity of infraction.

Another factor is the communication and clarity about which deterrence actions will be taken.[18] This is particularly important when a specific capability or action is to be deterred. By providing clarity of what actions will be taken should deterrence fail there is no question of the potential for retaliation. Some historical examples of lack of clarity include Korea in 1950 and 1990 Iraq. Capabilities and political will were present for deterrence, however the lack of defined

---

[13] Chad Bates & Charlene Rose, "Leveraging Talent to Dominate in Cyber War – An Army Perspective," *The Great Power Competition* 3, (2022):319-346, https://doi.org/10.1007/978-3-031-04586-8_16

[14] Rob Sobers, "161 Cybersecurity Statistics and Trends [updated 2023]," *Varonis*, November 29, 2023, https://www.varonis.com/blog/cybersecurity-statistics

[15] Anna Ribeiro, "US Critical Infrastructure Sector Faces Cyber Threats Surge in 2023, Calls for Urgent Action, Enhanced Measures," *Industrial Cyber*, Dec 10, 2023, https://industrialcyber.co/features/us-critical-infrastructure-sector-faces-cyber-threats-surge-in-2023-calls-for-urgent-action-enhanced-measures/

[16] Michael Mazarr, Arthur Chan, Alyssa Demus, Bryan Frederick, Alireza Nader, Stephanie Pezard, Julia A. Thompson, and Elina Treeyger. "

[17] President, *National Security Strategy* (Washington, DC: White House, 2002), 4-6, https://www.witehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Adminisrations-National -Security-Strategy-10.2022.pdf

[18] Michael J. Mazarr, "Understanding Deterrence," *Perspective*, RAND. (2018) https://rand.org/pubs/perspectives/PE295.html

action should deterrence fail was not understood. Ensuring a strong information management campaign to align narratives and limits of action is essential for successful deterrence.

The third factor is understanding that the deterring actor will carry out the defined action should deterrence fail. The political will of a State to support a course of action may not be as steadfast as presented. The polarization of U.S. public opinion on a variety of topics over the last several years, particularly regarding the recent conflict in Gaza, has called into question the resolve to take swift action should deterrence be challenged.

In addition to these three factors, deterrence strategies depend on the adversary level of motivation to use hostile action to achieve their goal.[19] If low, then the adversary will be easier to deter than if their motivation is high. Examples include dissatisfaction with the status quo, perception of threat or safety concerns, or if trends are moving toward a significantly unfavorable power relationship. When considering deterrent strategies, consideration of the perception of the actions and providing assurances to the global community of the intent of the actions is essential.

On the international stage, there are rarely only two actors, one doing the deterring and one being deterred. Preventing aggression is a balancing act among the perceptions. Deterrence requires keen attention to providing assurances to dissuade the perceived need for aggressive action. Deterrence is in the eye of the deterred and success is a combination of understanding capabilities and motivations, being clear of purpose, and maintaining political will.

Integrated Deterrence

While the NSS presents a broad strategy for deterrence across domains, regions, partners and allies, the NDS distills the key element into actionable priorities for the DoD through ID. It calls upon the DoD to develop or combine strengths to maximum effect, leverage other instruments of national power, build commercial partnerships, and strengthen alliances.[20] Additionally, the NDS points out that the primary focus of broad deterrence efforts is the People's Republic of China, with acute threats from Russia, and persistent threats from North Korea, Iran, and violent extremist organizations.

Considering cyber deterrence through the lens of the NDS and ID provides specific focus on developing international partners in three main areas: denial, resilience, and cost imposition.[21] Deterrence by denial describes a methodology for denying access to high value targets, such as key infrastructure and supporting networks. Deterrence by resilience focuses on withstanding, fighting through, and recovering from disruption. Deterrence by cost imposition specifically looks at leveraging retaliation for attacks. This multi-pronged approach is designed to manage how competitors perceive U.S., allied, and partner positions while being tailorable to specific settings. This deterrence strategy is an ongoing, persistent effort to prevent a broad series of actions while maintaining flexibility to implement immediate deterrence actions against a specific adversary or impending attack.

---

[19] *Ibid*
[20] Secretary of Defense, *National Defense Strategy*, Washington, DC: Pentagon, 2002.
[21] *Ibid*

Cyber Deterrence

To deter adversaries in the cyber domain, States consider options to dissuade actors from initiating cyber-attacks.[22] Inferring cyber strategies from conventional deterrence, we can see the immediate application of the two main deterrence approaches: denial and punishment. Denial strategies intend to make actions seem infeasible or unlikely to succeed. Deterrence by punishment threatens severe penalties such as immediate damage or the wider expansion of consequences. Historically we have seen deterrence by punishment as difficult to impose due to limitations in the political will to potentially inflict punishments, particularly with the backstop of nuclear options. Similarly in cyber, many cyber-attackers escape punishment due to the inability to attribute attacks to a specific group and limited options for retaliation.[23] Here we examine the convergence of these concepts through the lens of ID and international partnerships.

Deterrence by Denial

Deterrence by denial options in cyberspace can be inferred from conventional deterrence literature. Denial convinces the opposition that their goals will not be attained.[24] This denial can be accomplished by enhancing cyber-capabilities so that the perception that the cost in resources expended to sustain an attack would outweigh the benefit of the attack.[25] For example, China perceives a drawn-out conflict with Taiwan as an unacceptable drain to resources which could prevent the PRC from reaching full capacity.[26] If the probability of achieving goals is low and the cost is high, standard deterrence calculus indicates deterrence should be successful.

Denial focuses on objectives as well as strategy and therefore can be calculated as it is not reliant solely on determining intent. The NDS describes deterrence by denial primarily to deter adversaries from rapidly seizing territory.[27] In cyber, there is no geographic territory to be seized, but networks and capabilities can be seized. Additionally, cyber plays an ever-increasing role in cross-domain operations as new capabilities, information sharing, and non-kinetic options emerge. Denying cyber-attackers access to target key infrastructure, healthcare networks, and key financial capabilities are essential aspects of deterrence by denial.

Deterrence by Resilience

The NDS recognizes the difference between denial and defense by highlighting deterrence by resilience, or the ability to secure and withstand attacks should an attack happen. Building resilience in the cyber and space domains specifically includes encryption and zero-trust architecture.[28] Employing capabilities to address attacks or to minimize damage if attacked

---

[22] Nida Shashid and Ahmad Khan, "Addressing Cyber Vulnerabilities Through Deterrence," *The Journal of Contemporary Studies* 11 no. 01 (2022): 50-68
[23] *Ibid*
[24] Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies* 46, no. 3 (2023): 530-69. doi:10.1080/10402390.2021.1977856
[25] *Ibid*, 539
[26] Aiza Azam and Adil Sultan, "U.S. Posture of Integrated Deterrence: China's Response and Implications for the Asian Security," *Strategic Studies*, 43, no. 1 (2023): 54
[27] Secretary of Defense, *National Defense Strategy*, Washington, DC: Pentagon, 2002, 16
[28] *Ibid*

and enabling security should deterrence fail are essential to resilience.[29] Similar to denial, the perception that cyber-attacks will not achieve the desired disruption or destroyed capability is the intent of building network resilience.

Deterrence by Cost Imposition

At times, denial and resilience may not be sufficient to deter cyber-attacks. Much of cyber defense literature suggests strategies employing deterrence by punishment, or the threat of cyber repercussions should an adversary initiate a cyber-attack. In the context of ID, the imposition of direct and collective costs includes offensive cyber and the option for a collective response to aggression. The unique cyber environment with issues of ease of entry, attribution, and offense orientation may create concerns for developing a cyber-deterrence strategy. While some scholars suggest that protection of national interests cannot rely on deterrence as a central strategy, it is currently the key concept in the U.S. National Security Strategy.[30] By leveraging across domains and instruments of national power, it is imperative that the U.S. and allies integrate a comprehensive cyber deterrence strategy within ID.

Conventional deterrence strategies reliant on repercussions or cost impositions have not historically worked well as threat-based deterrence can go tragically wrong or provoke the kinds of conflicts they are trying to avoid. Cost imposition strategies involve threats of degradation or destruction of a capability and are a poor fit in cyber-deterrence.[31] Additionally, not all allies have offensive cyber capabilities or the ability to impose direct costs through cyber and are reliant on extended deterrence through alliances.

Robust cyber capabilities are not always available to effect cost impositions. A study in Norway found that a small state could not independently deter hostile cyber operations from larger powers.[32] Not only was it not guaranteed that the State could acquire or develop the capability to identify and impose costs or retaliation, but communicating the deterrent message and building the reputation as being willing to employ capabilities may be absent, particularly in smaller nations. As a member of NATO, the more robust capabilities of extended deterrence are able to be brought to bear in support of smaller states. However, the benefits of this alliance are not globally available to all allies and partners.

Developing Allies and Partners

From the U.S. NDS deterrence by denial, resilience, and cost imposition span a broad spectrum of deterrence options and required capabilities. Several commissions are working to develop a layered cyber deterrence combining traditional mechanisms and extending to a whole of government approach. Significant efforts by the Cyberspace Solarium Commission 2.0 and Regional Centers for Security Studies are working to build interoperability with international

[29] Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies* 46, no. 3 (2023): 541. doi:10.1080/10402390.2021.1977856
[30] *Ibid*
[31] *Ibid*
[32] Tobjorn Pedersen, "A Small State's Cyber Posture: Deterrence by Punishment and Beyond," *Scandinavian Journal of Military Studies,* 6 no. 1 (2023):58-68

partners and allies.[33] The commission specifically highlights the benefits to U.S. security by developing the cyber capability and security of our partners and allies.

Current capability gaps suggest that ID communicates the resolve of the U.S. to enhance allied and partner capabilities to a common threshold. The implications of integrating deterrence options across domains is not lost on those who are not actively allied with the U.S.[34] Among others, U.S. strategic documents refer to China as the pacing challenge with Russia as an acute challenge along with other identified States.[35] Concerns abound regarding the impact to the regional status-quo and balance of power should capabilities be shared or enhanced. Of note, not all capabilities are available, or desirable, to international partners in support of a fully integrated deterrence effect.

Moving toward a common interoperable cyber deterrence capability will take significant time and investment from multiple partners. Implementing standard cyber requirements has taken several years and is still in progress within the U.S. Department of Defense. Not only do the networked systems and infrastructure require constant updates and integration, but recruiting, retaining, and diversifying the cyber workforce is a continually moving target. Additionally, ID relies on the acceptance of extended deterrence and integration with and support for allies and partners. Aggressors know a state will always fight to defend itself, but not always to honor a promise of support. As we have seen with the U.S. budgetary concerns regarding providing financial and military support to Ukraine through other European nations, political will and support for extended deterrence can be easily swayed.

Counter

Highlighted in the NDS, is the role of information management in deterrence. The U.S. and allies "must seek to avoid unknowingly driving competition to aggression."[36] While the U.S. and allies move toward interoperability and enhancing capabilities to deter identified adversaries of the U.S., regional power dynamics may shift and inadvertently result in hostile actions by other States.[37] In some respects, the integration with allies and partners has already changed or intensified policies in the Indo-Pacific region.

Following the publication of the NSS and NDS, several countries updated their security strategies. Closely mirroring the U.S. policy, Canada published their strategy.[38] Japan also released their security strategy highlighting the intention to maintain a free and open international order, particularly in the Indo-Pacific and criticized the PRC for not cooperating with the international community.[39]

---

[33] Cyberspace Solarium Commission 2.0, "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY24," Washington, DC: Congress of the United States, March 24, 2023, 6
[34] Aiza Azam and Adil Sultan, "U.S. Posture of Integrated Deterrence: China's Response and Implications for the Asian Security," *Strategic Studies*, 43, no. 1 (2023): 49
[35] *Ibid*, 48
[36] Secretary of Defense, *National Defense Strategy*, Washington, DC: Pentagon, 2002.
[37] Aiza Azam and Adil Sultan, "U.S. Posture of Integrated Deterrence: China's Response and Implications for the Asian Security," *Strategic Studies*, 43, no. 1 (2023): 49
[38] *Ibid*, 50
[39] *Ibid*

These documents sparked serious concerns. Pakistani scholars published several studies outlining concerns about the willingness of India to leverage their partnership with the U.S. to the detriment of Pakistan. China's strategic documents had centered on national defense aims of deterrence and resisting aggression.[40] However, following the 2022 documents, those countries identified as targets of ID have adopted a more steadfast posture. In particular, China's opposition efforts toward Taiwan independence as part of preserving national sovereignty and territorial integrity.[41]

Rebuttal

Per the NDS, the importance of managing information regarding ID is essential to implementing the concept.[42] As such, the U.S. and allies must take a deliberate, transparent approach to integrating deterrence capabilities. Not only does the communication of actions taken promote the deterrence, but it will also provide assurance that integration takes into consideration the regional power dynamics so as to not exacerbate tensions.

Particularly with cyber capabilities, misinformation or reports of illicit use or preemptive, unattributable actions in a borderless domain can be manipulated to increase instability and cause panic among populations. Leveraging the close ties between cyber and information and the speed of global communication makes it easy for adversaries to undermine deterrence and push regions into defensive postures or preemptive offensive positions. Building open dialogue and maintaining transparency of integration efforts builds legitimacy for deterrence efforts. Further, diplomatic engagement in regions of particularly tense relations can open communication regarding enhancements and provide insight into concerns and potential mitigations for stability.

Conclusion

The emphasis on integrating allies and partners highlights the ways the conventionally based concept of ID is applicable in cyberspace. The publication of ID as the cornerstone of the U.S. NDS and the emphasis on collective responses with allies and partners provides guidance for implementation.[43] Examining elements of ID through cyber implementation shows how the conventional deterrence concepts are applicable in the cyber-domain.

Cyber threats are continually evolving and so too must strategies to deter attacks. Significant challenges due to dynamics of the domain, emerging technologies, and developing infrastructure may impede the implementation of ID. However, the basic tenets are achievable through efforts toward interoperability, information sharing, and common resolve. Allies and partners must present a synchronized cyber- deterrence posture. Otherwise, the costs of not adopting a credible cyber-deterrence strategy will continue to climb.

---

[40] *Ibid*, 48
[41] *Ibid*, 50
[42] Secretary of Defense, *National Defense Strategy*, Washington, DC: Pentagon, 2002.
[43] President, *National Security Strategy* (Washington, DC: White House, 2002), 4-6, https://www.witehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Adminisrations-National -Security-Strategy-10.2022.pdf

BIBLIOGRAPHY

Azam, Aiza and Adil Sultan. "U.S. Posture of Integrated Deterrence: China's Response and Implications for the Asian Security." *Strategic Studies*, 43, no. 1 (2023):45-63

Borghard, Erica D. and Shawn W. Lonergan. "Deterrence by Denial in Cyberspace." *Journal of Strategic Studies* 46, no. 3 (2023): 5369. doi:10.1080/10402390.2021.1977856

Burt, Tom, "Espionage Fuels Global Cyberattacks," *Microsoft On the Issues*, Oct 5, 2023, https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

Cybersecurity & Infrastructure Security Agency, "Partnerships and Collaboration," https://www.cisa.gov/topics/partnerships-and-collaboration

Cyberspace Solarium Commission 2.0. "Letter to the U.S. House Appropriations Committee Regarding Appropriations Requests for FY24." Washington, DC: Congress of the United States. March 24, 2023.

Lamba, Shalini, Vibhu Tripathi, Ansh Kapoor, "Cyberwar: A New Battle Ground," *Advances in Engineering Science and Management*, 1, (2023):149-156

Mazarr, Michael J. "Understanding Deterrence." *Perspective*. RAND. (2018) https://rand.org/pubs/perspectives/PE295.html

Pedersen, Tobjorn. "A Small State's Cyber Posture: Deterrence by Punishment and Beyond." *Scandinavian Journal of Military Studies,* 6 no. 1 (2023):58-68. https://doi.org/10.31374/sjms.191.

President. *National Security Strategy.* Washington, DC: White House, 2002. https://www.witehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Adminisrations-National -Security-Strategy-10.2022.pdf

Ribeiro, Anna. "US Critical Infrastructure Sector Faces Cyber Threats Surge in 2023, Calls for Urgent Action, Enhanced Measures." *Industrial Cyber*, Dec 10, 2023. https://industrialcyber.co/features/us-critical-infrastructure-sector-faces-cyber-threats-surge-in-2023-calls-for-urgent-action-enhanced-measures/

Saaida, Mohammed B. E. "The Use of Cyber Warfare and its Impact on International Security," *Science For All Publications* 1, no. 1 (2023):1-5

Secretary of Defense, *National Defense Strategy*, Washington, DC: Pentagon, 2002. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf

Shashid, Nida and Ahmad Khan. "Addressing Cyber Vulnerabilities Through Deterrence." *The Journal of Contemporary Studies* 11 no. 01 (2022): 50-68Sobers, Rob "161

Cybersecurity Statistics and Trends [updated 2023]," *Varonis*, November 29, 2023, https://www.varonis.com/blog/cybersecurity-statistics

Vu, Anh V., Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton, Ross Anderson. Getting Bored of Cyberwar: Exploring the Role of Civilian Hactivists in the Russia-Ukraine Conflict. 2023. https://arxiv.org/pdf/2208.10629.pdf