Sir Syed Journal of Education & Social Research
Vol. 7, Issue 2, 2024 (April – June)
ISSN 2706-6525 (online), ISSN 2706-8285 (Print)
ISSN 2706-9362 (CD-ROM), ISSN 2706-6525 (ISSN-L)
DOI: https://doi.org/10.36902/sjesr-vol7-iss2-2024(1-7)

SJESR
Sir Syed Journal of Education & Social Research

Nuclear Deterrence in the Cyber Age: Intricacies and Prospects

* Ayesha Abrar

Abstract

Nuclear deterrence is confronting unprecedented challenges in the contemporary era, particularly with the emergence of cyber warfare. As the world becomes increasingly dependent on digital technologies, the intersection of cyber and nuclear domains will have significant implications for global security. Nonetheless, prominent theorists, policymakers, and military strategists are attempting to reconsider its application in a post-Internet and cyber-ready world. There exists a C4ISR vulnerability to attacks on adversary command and control systems. Nuclear deterrence and cyber warfare are separate, but interrelated, challenges. Nonetheless, the cyber-nuclear link holds significant importance in modern crisis management. This paper investigates the complexities and challenges of nuclear deterrence in the cyber age, examining the evolution of cyber threats and the vulnerabilities of nuclear systems. Furthermore, it discusses the necessity for adaptable strategies to address these emerging risks. This research aims to provide a more profound comprehension of the challenges and opportunities arising from the convergence of the cyber and nuclear domains by conducting a comprehensive literature review and employing an extended nuclear deterrence theoretical framework.

Keywords: Nuclear Deterrence, Cyber Warfare, Cyber Security, Digital Age, Arms Control.

Introduction

For seven decades, the notion of deterrence has dominated Western strategic thought and continues to hold a significant position in security discourses. When faced with new threats like terrorism or cyber-attacks, a common question arises: "Is this deterred?" The concept of nuclear deterrence, however, has lost its former prominence, prompting theorists, policymakers, and military strategists to embark on what is commonly referred to as the 'Quest for Concept'. This shift includes rethinking the use of nuclear weapons in a post-Internet, cyber-ready world, where missions for deterrence will inevitably evolve. In order to meet the demands of rapid and adaptive decision-making and military action, governments and their armed forces are transforming their rigid bureaucratic structures. This transformation increasingly relies on cyber capabilities, making them more susceptible to cyber threats. This raises critical questions about what happens when ideas and methods for cyber-war and nuclear deterrence overlap. What impact does this convergence have on our strategies for managing these two types of conflict?

The emergence of the fifth-generation mobile technology (5G) and cloud technologies will enhance the dissemination of the Internet of Things. Critical processes will gradually be transferred to these technologies, and cyber risks will rise exponentially as the new devices create more opportunities for potential breaches. Furthermore, by controlling physical assets, physical harm can be caused.

Digital warfare provides a means to disrupt or disable enemy assets with minimal physical violence, whereas nuclear weapons entail significant destruction. Nuclear deterrence has historically been aimed at avoiding war by manipulating risk, rather than through actual use. However, nuclear deterrence and cyber warfare cannot be considered separate policy spheres. Their convergence will have significant implications for upcoming conflicts and global relations. The information age has revolutionized military affairs, but nuclear deterrence theory and policy struggle to adapt to this new, cyber-driven landscape. Future conflicts, including those involving nuclear deterrence and crisis management, will undoubtedly incorporate digital components. Cyber warfare has become a key component of modern conflict, particularly when it comes to targeting an enemy's command, control, communications, computers, intelligence, surveillance, and reconnaissance. It is critical to recognize that nuclear deterrence and cyber warfare are interconnected aspects of modern conflict. By treating

* National Defence University, Pakistan Email: ayeshabrar04@gmail.com

them as distinct challenges, one overlooks the reality of nuclear deterrence in a cyber-intensive environment and hinders the development of effective strategies.

Literature Review:

Deterrence in Digital Age:

Discussing deterrence in the 21st century evokes memories of a different era, notably the Cold War, where deterrence held significant societal influence across diverse political spectrums. However, its prominence has waned with the reduction of nuclear arsenals. Today, deterrence remains a potent governmental tool rather than an overriding force, amidst a shifting international landscape characterized by evolving conflict paradigms and the utilization of non-military tactics such as propaganda and cyber warfare. Despite its continued relevance in the cyber age, deterrence faces novel challenges and opportunities. Yet, our comprehension of cyber deterrence is often hindered by antiquated Cold War ideologies, inhibiting the development of effective strategies necessitated by the intricate dynamics of the digital realm (Joseph S. Nye, January 01 2017).

Can nations prevent or discourage cyber aggression from other countries? This question has been a pressing concern, as former Estonian President Toomas Ilves noted, 'The biggest challenge in cyber is deterrence.'[1] Since the turn of the century, the Internet has become a vital technology, contributing significantly to the global economy and connecting nearly half of the world's population. However, this increased dependence on the Internet has also created new vulnerabilities, leading to a new dimension of international insecurity. With the projected growth of the 'Internet of Things' to over 20 billion devices in the next five years, and cyberattacks potentially targeting a wide range of sectors, accounting for up to 3.4% of GDP in major economies, the need for effective cyber deterrence strategies has become increasingly urgent. (Roxburgh, 2011)

Cyber Threat in Nuclear Domain:

Today, more people realize that cyber-attacks can harm nuclear weapons. This includes spoofing, hacking, manipulating data, poisoning it, and digital jamming. These attacks could compromise the integrity of their communications and take control of their dual-use command and control (C2) systems without the target's knowledge. For example, someone else could get into nuclear power plants, stop warning systems, or start a nuclear explosion or launch. China, the US, and Russia all worry about the threats of AI-augmented cyber warfare. This may make states think about taking launch-on-warning nuclear positions or taking preventive measures during crises. The rise of drone swarming technology further complicates the nuclear landscape. In a world with nuclear multipolarity, long-standing assumptions about nuclear deterrence are being challenged. This makes it hard for states to manage escalation and interpret signaling effectively, which could lead to misperception and miscalculation among nuclear-armed countries. With weak de-escalation mechanisms and doctrinal opacity, nuclear use is more likely in strategic alliances like India-Pakistan, US-Russia, US-North Korea, and US-China. A report from the House of Lords in 2019 says that nuclear weapons use is more likely now that there is more competition between countries, a more multipolar world, and advances in technology. The advent of AI-augmented drones and hypersonic weapons raises more concerns. While AI's impact on tactical and operational aspects of warfare is clear, its strategic implications remain unclear. Some people think that AI's use at the tactical level could affect deterrence policy, escalation mechanisms, and strategic stability among great powers. AI and autonomy may decrease stability in nuclear multipolarity and increase the risk of inadvertent escalation to nuclear use. Additionally, the use of drones, especially in swarms, poses a significant threat. Conceptually suited for pre-emptive attacks and nuclear ISR missions, drones can target an adversary's nuclear mobile missile launchers and submarines, along with their enabling facilities, using advanced AI-ML technology and drone swarming techniques.

Comparative study of cyber warfare and nuclear deterrence:

In the realm of cyber warfare, identifying the precise source of an attack can pose a challenge, as third-party intrusions can obscure the genuine perpetrators behind the operation. In contrast, in nuclear deterrence, the source of an attack is usually identifiable, especially if it involves a state actor. Even terrorist attacks involving nuclear materials may be traceable. Nuclear deterrence and cyber warfare have distinct intellectual foundations, as nuclear weapons possess unparalleled destructive capacity, whereas cyber weapons primarily aim to sow confusion and disruption. However, the

intersection of cyber and nuclear domains poses potential challenges to nuclear deterrence. Cyber attacks could exacerbate nuclear crisis management, while information attacks on command and control systems may lead to erroneous nuclear launches, misinterpreted data, or panic induced by feared information blackout. Moreover, future nuclear strike planning may incorporate preliminary cyber-attacks or prolonged "preparation of the battlefield" through enemy network infiltration to plant malware or identify vulnerabilities. (Cimbala, 2014).

Cyber -attacks typically target information systems, networks, and messaging content, with the potential to impact military operations, the economy, and social infrastructure. Nuclear deterrence can cause unprecedented and socially catastrophic damage even in a scenario considered limited by Cold War standards. The possibility of thwarting an adversary's goals in online combat depends on the strength of safeguards and the ability to swiftly address flaws. Advances in missile defenses aim to change the dynamic of deterrence in nuclear contexts.

Cyberattacks often aim to cause disruption or confusion, allowing them to go unnoticed or unreported for a long time. The fundamental tenet of nuclear deterrence hinges on the verifiable apprehension of extensive and prompt destruction of assets and populations.

Cyber warfare presents a low barrier to entry, with actors ranging from individual hackers to state entities participating. Similarly, establishing and maintaining a second-strike nuclear deterrent requires substantial state-supported infrastructure, scientific and technical expertise, and long-term financial commitments.

Potential Overlap - Cyber and nuclear?

What happens if we use cyber warfare and nuclear deterrence together? Cyber warfare and nuclear weapons may seem very different, depending on who supports using non-nuclear or post-nuclear weapons. Cyber warfare offers the possibility of destroying enemy assets without having to use kinetic assaults. This contrasts sharply with the mass destruction that nuclear weapons often cause. But these two areas can't exist alone in policy frameworks, so they need to be part of systems that govern command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) Nuclear weapons require protection against both physical and digital threats. Decision-makers responsible for managing nuclear forces during a crisis necessitate precise and timely information regarding their own nuclear and cyber capabilities, as well as those of potential adversaries. (Cimbala, 2014).This includes knowledge of enemy intentions and risk tolerance, as well as C4ISR systems. Effective nuclear crisis management depends on clear thinking and good information. Nonetheless, the utilization of cyber weapons at an early stage of a crisis has the potential to disrupt networks and decision-making channels, resulting in confusion and compromised crisis management. The temptation to launch early cyberattacks may eventually weaken nuclear crisis management capabilities. Also, a nuclear crisis requires a lot of situational awareness and decision-making, which could be hampered by early cyber interventions that cause network disruptions and operational confusion. The downsizing of US and Russian nuclear arsenals post-Cold War is good for arms control, but it also raises concerns about the coalescence of cyber and nuclear capabilities, making nuclear forces less flexible and resilient against cyber-enabled attacks. Both offensive and defensive cyber activities are on the agendas of US and Russian military establishments, highlighting the importance of cybersecurity concerns. Even though there is a need for cybersecurity cooperation, it is still a difficult task to achieve cyber arms control. Also, the cyber domain's relative novelty and lack of historical scrutiny add layers of uncertainty to the cyber-nuclear intersection. Experts agree that nuclear deterrence and cyber warfare are different, but their inevitable interaction shows how difficult it is to navigate the convergence between these domains in practice.

Evolution of Cybersecurity Risks in Nuclear Environments

The cyber domain encompasses the other geostrategic domains for warfare as well: land, sea, air, and space. However, the cyber domain, compared to the others, suffers from lack of a historical perspective: the cyber domain has been created in a short time and has not had the same level of scrutiny as other battle domains. (J.Cimbala, 17 Jul 2017).The cyber threat in the nuclear industry has changed from small incidents to sophisticated attacks. As nuclear power plants rely more on computers, they are more likely to be attacked, which can have serious consequences. Criminals and governments are targeting nuclear facilities to disrupt operations, steal important information, or cause serious problems. In 2015, Russia attacked Ukraine's power grid and caused many people to lose power. In January 2017, a cyberattack hit two Saudi petrochemical companies, Tasnee and

Sadara Chemical Company, causing widespread disruption. Computers went black and hard drives were destroyed, wiping out important data. The attack, which took months to recover, was meant to stop operations and cause a catastrophic explosion. Johnson says that this incident shows how cyber threats are getting worse. Organizations need strong access controls and continuous monitoring to prevent potentially disastrous consequences. The nuclear industry must adapt to this new reality by taking strong cybersecurity measures, sharing threat intelligence, and working together internationally to prevent cyber incidents from affecting global security and safety. The Stuxnet attack on Iran's Natanz nuclear facility showed how cyber weapons can be used in the real world. A report by Chatham House, "Cyber Security at Civil Nuclear Facilities: Understanding the Risks," says that the nuclear industry is not doing enough to address cyber threats. The report says that the likelihood of a significant cyberattack remains constant as cybercriminals, state-sponsored hackers, and terrorists increase their online activities. Even if the cyberattack is small or unlikely, it still poses a serious threat because radiation could be released.

Modern nuclear facilities rely on technology, such as SCADA systems and industrial control systems, which can be easily hacked. Many experts think that air-gapped critical components are safe from a major cyberattack. But the Chatham House report says that Stuxnet virus infected Iran's nuclear facilities using a flash drive, breaking the supposed "air gap." The report shows that nuclear facilities have different levels of physical and computer security. Some facilities are very safe, but others are not. It shows how important it is to have a strong security posture to reduce risks and prevent disasters. (Paganini, 2015).

Missile Defense, Cyber, and Nuclear Deterrence: A Complex Web of Challenges

Increasing numbers of major powers are allocating significant political and financial resources to develop autonomous weapons systems, aiming to tap into their full military potential at all levels - tactical, operational, and strategic.Cyber security, missile defense, and nuclear deterrence share numerous connections. A robust missile defense system can help deter attackers by making it harder for them to succeed. The technical and political complexities of missile defense are present. The controversy surrounding the European Phased Adaptive Approach (EPAA) proposed by the US and NATO, and the technical limitations of proposed missile defense components, adds to the complexity of the discussion. Furthermore, the political dimension of missile defense, including the linkage between US and NATO missile defense plans and advancements in US-Russia strategic arms reductions, presents a contentious relationship.

Cyber warfare could disrupt network communications, distract operators, or interfere with launch commands and software performance. This could make crisis management and response strategies more difficult. The complexity of cyber warfare suggests that attackers may exploit vulnerabilities in missile defense systems, posing challenges to effective defense strategies. The New START agreement aims to reduce deployed strategic weapons by a modest amount. Questions about deterrence effectiveness and arms control stability are raised about the possibility of further reductions. The effects of missile defense capabilities on deterrence dynamics and strategic stability in the new START environment are explored through simulation models.

Challenges and Rewards -In Cyber & Nuclear Realms:

Cyber is a complex landscape that needs careful consideration. Cyber capabilities can be used to improve the security and resilience of nuclear systems. During most of the time when nuclear weapons were used, bombers and missiles didn't work well enough to destroy hard-to-kill targets. But as technology got better, they became more accurate. Breakthroughs in navigation and guidance, such as advanced inertial sensors and celestial updates, improved missiles' ability to pinpoint their location during flight and make necessary course corrections, thereby making them more precise and effective. (Keir A. Lieber, 2017) .Cyber technologies can help protect critical infrastructure, improve early warning systems, and improve command and control mechanisms, which would make nuclear arsenals more deterrent overall.

But cyber also brings challenges and risks to nuclear deterrence. One of the biggest challenges is the vulnerability of nuclear systems to cyber-attacks. As nuclear weapons use computers to control and communicate, they become more vulnerable to cyber threats like hackers, viruses, and manipulating data. A successful cyber-attack on nuclear infrastructure could undermine the credibility of deterrence, disrupt decision-making processes, or even give people access to or control over nuclear weapons. Furthermore, it is difficult to attribute cyber-attacks to nuclear deterrence.

Cyberspace makes it challenging to identify those responsible for cyber-attacks on nuclear facilities. Lack of attribution can lead to misinterpretation of intentions and escalation of tensions between nuclear-armed states.

The rapid pace of technological advances in both the cyber and nuclear domains is another challenge. People use to attack computers as they get better. Keeping up with new cyber threats and keeping nuclear deterrence tactics effective is a constant challenge in this dynamic environment. Nuclear deterrence is even more complicated because of the increased cyber capabilities of both countries and non-countries. Non-state actors with sophisticated online abilities could pose a serious threat to nuclear safety by gaining access to confidential nuclear data or disrupting vital nuclear facilities.

Because of these issues, we need to ensure that nuclear systems are safe from cyber threats. This means using strong security measures, learning more about threats, checking for weaknesses regularly, and working with other countries to share information about cyber threats that could harm nuclear weapons. Cyber technologies offer fresh ways to boost nuclear dissuasion, but they also introduce new weaknesses and dangers that require careful oversight to safeguard the global nuclear order.

Future command-and-control support tools may overcome many of the shortcomings inherent to human strategic decision making during wartime with potentially stabilizing effects. The faster and more reliable cyber applications could also enable commanders to make better decisions in a crisis, enhance the safety and reliability of nuclear support systems, bolster the cyber defenses of command-and-control networks, enhance battlefield awareness, and diminish the risk of human error caused by fatigue and repetitive tasks. AI systems that allow commanders to predict the potential production, commissioning, deployment, and ultimately launch of nuclear weapons by adversaries will likely lead to unpredictable system behavior and outcomes, which in extremis could undermine first-strike stability, the premise of mutual assured destruction. (Johnson, 01.28.21)

Research methodology:

The integration of qualitative designs enables a deeper exploration of nuclear deterrence in the cyber age. I will analyze existing data and scholarly literature using an extended nuclear deterrence theory framework. The research methodology follows a positivist approach, emphasizing the objective analysis of empirical evidence to uncover causal relationships and patterns. The paper examines the challenges and opportunities presented by the convergence of the cyber and nuclear realms by synthesizing insights from various scholarly sources. The researcher uses deductive reasoning to examine the information and make conclusions that either support or challenge their initial ideas or theories. The researcher aims to understand how cyber warfare and nuclear deterrence work together using deductive reasoning.

Theoretical Framework:

This paper uses a theory called extended nuclear deterrence that has been modified for the internet age to explain extended nuclear deterrence. This framework demonstrates how conventional notions of deterrence, primarily centered on nuclear capabilities, must adapt to address online threats. Adding cyber warfare to nuclear deterrence requires a re-examination of existing theories and the development of new strategies that account for the unique characteristics of cyber threats. This theory extends traditional nuclear deterrence by adding cyber capabilities to it. It involves denial, retribution, toughness, and repetition.

Discussion:

The amalgamation of nuclear deterrence and cyber warfare signifies a pivotal moment in contemporary strategic analysis. This intersection challenges conventional notions of security and requires a re-evaluation of established deterrence theories. Cyber threats introduce new weaknesses to nuclear systems, such as the potential for spoofing, hacking, and data manipulation. This could compromise the credibility of nuclear deterrence. The rapid evolution of technology, particularly in cyber capabilities, has exacerbated these vulnerabilities, which require continuous adaptation and innovation in defensive strategies. One crucial aspect of this convergence is the incorporation of cyber warfare into the framework of nuclear deterrence. Cyber weapons are capable of achieving strategic objectives with minimal physical damage, in contrast to nuclear weapons, which are specifically designed for mass destruction and serve as a deterrent through the threat of catastrophic retaliation.

This disparity in impact requires a nuanced approach to deterrence that integrates both the traditional elements of nuclear strategy and the unique characteristics of cyber threats.

The rise of artificial intelligence-augmented cyber warfare and drone swarming technology complicates the nuclear landscape. Cyber-attacks are more precise and effective with these tools, increasing the chance of wrong assumptions and accidental escalation among nuclear-armed nations. Another layer of complexity is added to deterrence strategies by the opaque nature of cyber operations. Uncertainty can lead to misunderstandings of actions and intentions, escalating tensions and potentially triggering conflict. Additionally, the increasing dependence on digital technologies for command, control, communications, computers, intelligence, surveillance, and reconnaissance systems in nuclear operations introduces significant cybersecurity risks. Cyber-attacks could potentially disrupt these vital systems, highlighting the need for robust security protocols and enhanced resilience in nuclear facilities. Strategic stability and the prevention of the un-authorized or accidental deployment of nuclear weapons are dependent on the integrity and reliability of C4ISR systems. Cyber and nuclear capabilities have dual-use nature, which presents policy challenges. Policymakers must navigate the delicate balance between using cyber technologies to enhance nuclear security and mitigating the risks they pose. This encompasses the creation of comprehensive cyber frameworks, fostering international cooperation, and promoting transparency and confidence-building measures to mitigate the potential for cyber conflicts to escalate to nuclear crises. In conclusion, the incorporation of cyber warfare into nuclear deterrence tactics highlights the interconnectedness of current disputes. Policymakers and military strategists can develop more effective and resilient deterrence frameworks by recognizing and adapting to the changing technological landscape .

Conclusion:

The advancement of cyber weapons or cyber warfare is not the sole factor determining nuclear modernization and deterrence, but they are also subject to the influence of evolving defense technologies. There have already been significant changes in the environment for strategic planning, nuclear dissuasion, arms control, and disarmament analysis, and there are more on the way. Technological advancements are the most obvious, but their effects go beyond the realm of technology. It's possible that the evolution of offensive strike platforms, the improvement of antimissile and anti-air defenses, and the growing importance of cyber, including offensive and defensive information warfare, will result in a paradigm shift in how advanced nations approach major conflict and nuclear deterrence. This discussion is only beginning to explore this potentially significant change.

Cyber tools won't eliminate the need for nuclear deterrence, and models designed to study nuclear deterrence can't be directly applied to cyber conflict without causing significant disruptions in strategic thinking. However, military strategists and decision-makers will spot connections between nuclear and online concerns. A truly strategic cyber conflict, distinct from physical attacks, is less pressing than cyber's role as an enabler (or disabler) of success in conventional warfare or nuclear deterrence. The future of digital technology in military affairs is uncertain. Future nuclear command, control, and communications systems, while benefiting from digital advancements, will still need to meet the strategic and policy requirements for prompt response to authorized commands.

References:

Cimbala, Dr. Stephen J. "Nuclear Deterrence and Cyber:The Quest for Concept." *Air & Space Power Journal* , March–April 2014.

Cimbala, Dr. Stephen J. "Nuclear Deterrence in Cyber-ia:Challenges and Controversies." *Air & Space Power Journal*, Fall 2016.

Cimbala, Stephen J. "Nuclear deterrence and cyber warfare: coexistence or competition?" *Defence& Security Analysis*, 17 Jul 2017: Vol-33,Issue-3,193-208.

Fischer, Manuel. " The Concept of Deterrence and Its Applicability in the Cyber Domain ." *The Quarterly Journal:Connections*, 2019: Connections QJ 18, no. 1-2 : 69-92 .

Freedman, Lawrence. "Introduction—The Evolution of Deterrence Strategy and Research." *SpringerLink*, 04 December 2020: pp 1–10.

Geist, Edward. "Deterrence Stability in the Cyber Age ." *Strategic Studies Quarterly*, winter 2015: Vol. 9, No. 4 , pp. 44-61.

Johnson, James. "Nuclear deterrence:New challenges for deterrence theory and practices." In *AI and the Bomb*, by James Johnson, 98-148. UK: Oxford univeristy press, 2023.

Joseph S. Nye, Jr. "Deterrence and Dissuasion in Cyberspace." *International Security* , (2017) : 41 (3): 44–71.

Joseph S. Nye, J. (January 01 2017). Deterrence and Dissuasion in Cyberspace. *MIT press journalVolume 41, Issue 3*, Volume 41, Issue 3,Pg 44–71.

Keir A. Lieber, D. G. (2017). The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. *MIT Press Direct*, Volume 41, Issue 4,Pg 9–49.

Libicki, Martin C. "Expectations of Cyber Deterrence." *Strategic Studies Quarterly* , 01 May 2018: Vol. 12, No. 4 pp. 44-57 Air university Press .

Lupovic, Amir. "Cyber Warfare and Deterrence:." *Military and Strategic Affairs*, december 2011: Vol.3,No.3.

Paganini, P. (2015). *Cyber-Attack on Worldwide Nuclear Facilities.*

Roxburgh, J. M. (2011). The great Transformer and the impact of the Internet on economic growth and prosperity. *McKinsey Global institute*.