SPOTLIGHT
ON REGIONAL AFFAIRS

December 2023, Vol.41, No.12 (2)

Quantum Supremacy: Assessing Nuclear Deterrence Dynamics in Cyberspace

Sidra Shahid*

Introduction

The advent of nuclear weapons in the 20th century had a transformative impact on global politics, introducing the concept of Mutually Assured Destruction (MAD) and reshaping the dynamics of International Relations. In this era of nuclear politics, the ability to possess and control nuclear weapons provided a strategic advantage and created the deterrence discourse among states. However, the 21st century is characterised by the digital revolution and the widespread integration of Information Technology (IT) into every aspect of the society. This increasing reliance on digital systems has given rise to sophisticated cyber threats and opened a whole new domain of warfare. With the rapid and extensive transformation of cyberspace from ARPAnet to the Internet and now into a sphere of military interactions, and national and economic security, debates on fostering deterrence in the domain have intensified. The traditional nuclear deterrence was challenged regarding its application in cyberspace and it seems that Quantum technologies can be the nuclear equivalent in cyberspace. Quantum technology mainly referring to quantum computers, harnesses the principles of quantum mechanics to perform computations in ways fundamentally different from classical computers. Utilising quantum bits or qubits, quantum computers can process vast amounts of information in parallel. This enables them to solve certain problems considerably faster than classical computers, offering transformative potential for fields such as cryptography, optimisation, and complex simulations.[1] The capability of quantum computers to break widely used cryptographic systems could offer a similar advantage in achieving deterrence in cyberspace as nuclear did in kinetic space.

Cyberspace deterrence is a vague concept. Some experts argue against the unbreakable constraints of nuclear deterrence in this field. Arguably, as complete prevention of attacks is unachievable, understanding deterrence in cyberspace on nuclear foundations is difficult.[2] The concept of deterrence followed in nuclear politics, i.e., "Dissuading threats from a state by installing the fear of retaliation or denial of objectives" [3] cannot fully address the security challenges emerging from cyberspace. The nuclear dynamics of mutually assured destruction, second strike capability, and credibility of threats fall short in achieving cyber deterrence. It is suggested that deterrence in the cyber world would be achieved through indigenous technologies of the field. Quantum is one such technology that potentially can prove to be decisive among cyberwarfare strategies of states just like nuclear weapons were after WW2.

The international race for quantum supremacy mirrors the nuclear arms race during the Cold War, with states competing for technological superiority in the quantum domain. This global competition for quantum capabilities reframes the geopolitical competition, potentially resulting in a quantum arms race with countries seeking to achieve deterrence and dominance in cyberspace. US-China competition in the realm of quantum supremacy is a reflection of the strategic importance that both powers attribute to advancing quantum technologies. The competition for achieving quantum supremacy and advancing quantum technologies has significant implications for deterrence in cyberspace. The possession of quantum capabilities for codebreaking enhances a state's deterrence posture by signaling the ability to neutralise or respond effectively to cyber threats relying on conventional encryption methods. Additionally, secure communication channels resistant to quantum attacks can deter adversaries from engaging in communications interception or manipulation. In short, the concept of traditional nuclear deterrence falls short in the cyber domain and quantum computing bears the potential to attain deterrence in cyberwarfare. Before exploring quantum potential as a deterrent in cyberspace, this study highlights the areas where nuclear deterrence applicability falls short in the cyber domain.

[*] Sidra Shahid is working as an Intern with the Cybersecurity Program at the Institute of Regional Studies (IRS) Islamabad.

Constraints of Nuclear Deterrence Applicability in Cyberspace

The enduring legacy of the Cold War makes deterrence in cyberspace quite difficult to comprehend. In the context of a nuclear attack, there is the threat of massive retaliation using nuclear means. The aim is total prevention in the case of nuclear warfare which is contradictory to the nature of cyberspace. Much like crime prevention, governments can only do so much in terms of cyberspace deterrence.

The difficulty in achieving deterrence in cyberspace stems from its inability to establish credibility both, in terms of denial and punishment. Unlike nuclear deterrence, cyberspace is not able to establish deterring measures in the broader aspect. Many experts debate the applicability of nuclear deterrence determinants in cyberspace. The 3Cs, i.e., Capability, Communication, and Credibility are the essential components that influence a deterrence strategy's efficacy when it comes to nuclear weapons. Nevertheless, specific difficulties and distinctions exist in the context of cyber deterrence, which might restrict how these ideas can be optimally applied.

Capability

In the realm of nuclear deterrence, the capability is mainly estimated in terms of weapons of mass destruction and second-strike capability. Comparatively, in the domain of cyber, capability is determined by technical proficiency, dexterity, and flexibility in addition to destructive potential. Cyber capabilities can be developed and implemented more quickly than nuclear capabilities, which makes it difficult to identify and neutralise threats that are always changing. Secondly, as the domain is steeped in ambiguity, the attribution of the attack to a specific actor is incredibly difficult.[4] Even though computers have a unique Internet Protocol (IP) address, hackers can still identify computers that they have unintentionally taken over by using botnet attacks. Rouge packets can conceal the source of aggression by bouncing between computers as they travel to the target. This particular challenge of attribution undermines the effectiveness of demonstrating capability in the cyber deterrence context, as attackers can operate with relative anonymity. The state’s retaliatory capability is rendered useless if the identification of ‘who’ to retaliate against is not clear. According to Bob Gourley, one cannot deter without punishment and one cannot punish without having an attribution.[5] In cyberspace making the right attribution is not always possible. The structural complexity of the internet, undeveloped political and legal policies, and its borderless global nature make attackers operate anonymously resulting in the process of attribution quite time-consuming and difficult.

Credibility

The reliable intent to use the capabilities is what forms the credibility in nuclear deterrence. Along with retaliation, credibility in cyber deterrence requires demonstration of a strong defense. This shows that traditional nuclear deterrence focuses mainly on the threat of punishment, and the shift in emphasis complicates the dynamic in the cyber realm. In comparison to nuclear deterrence, the reliability of deterrence in cyberspace is tilted more toward denial of objectives, i.e., a strong defense. This dependency on strong defense poses further challenges in the acquisition of fully achieved deterrence. The persistent and dynamic nature of threats in cyberspace makes effective defense difficult. In cyberspace, adversaries are often swift to circumvent defensive measures, as no system is entirely invulnerable to all types of cyber-attacks. The constant evolution and sophistication of tactics, techniques, and procedures make achieving absolute defense practically impossible. Furthermore, with the asymmetry, and the involvement of non-state stakeholders, i.e., private actors, hacktivists, or terrorist/criminal organisations, the phenomenon of maintaining deterrence becomes more complex as it is challenging to control and guarantee the actions of all entities within their borders. Also, the cost and benefit analysis of the attack differs for states with less dependability.

Communication

Communication is another important aspect in achieving nuclear deterrence. There are well-established communication channels and norms to convey any intentions in case of conflict and its resolutions. In contrast, the nature of norms in cyberspace is undefined and lacking which compromises the communication aspect of deterrence. States subjectively interpret the activities in cyberspace can result in misunderstanding leading towards further escalation. Another point to notice is that in traditional deterrence, a clear red line establishes the limits of acceptable behaviour, and crossing that red line triggers a retaliatory response. Whereas, in cyberspace, the absence of well-defined redlines hinders deterrence. This can happen mainly due to two aspects; the uncertainty leading to miscalculation of risk and consequences, as the adversary cannot understand what can trigger a retaliatory response and secondly, from the defensive perspective, cyberspace faces challenges in determining when a cyber threat warrants a retaliatory response. The absence of well-defined redlines complicates decision-making processes in this regard. This issue is of extreme concern when it comes to maintaining deterrence in cyberspace. No state until now has taken a measure that has effectively deterred the adversary from taking an offense because of undefined thresholds. The US identifies key areas to be considered threshold and even retains the option to retaliate by all means kinetic and non-kinetic. This however, has not stopped cyberattacks from the adversaries. Hence without communicating clear red lines either, there is a risk of immature escalation or compromised deterrent capabilities.

Another key aspect regarding communication is the real-time communication challenges. Threats in cyberspace unfold rapidly and require real-time communication for effective deterrence. In the existing time, the communication structures may not be agile enough to keep pace with the speed of cyber operations and hence limits the ability to send and receive timely messages to deter potential adversaries.

Deterrence by Entanglement and Dynamics of Cyberspace

Besides the traditional nuclear deterrence implacability in cyberspace, deterrence by entanglement is a concept advocated to attain deterrence by various scholars including Joseph Nye. Parallel to denial and punishment, the attribution and involvement of non-state actors challenge the deterrence through entanglement. The concept of interdependence and increasing the cost of an attack for the adversary can be neutralised if the state refuses to accept the responsibility or use a third party as a resource for launching a cyberattack. As far as economic interdependencies are concerned, they can create entanglement along with risks. In this case a state may be more vulnerable in the case of a cyber conflict if it depends too heavily on one country for vital resources or services, as disruptions could have dire economic consequences. Also, if the perceived reciprocal harm is less vis a vis the possible gains from the attack, a highly skilled cyber actor may be less discouraged by entanglement. Furthermore, Nye's idea of imposing economic sanctions as a deterrent against offensive cyber operations has its limitations in this realist world. From a realist lens, economic sanctions may not be fruitful in the case of economic power contributing to the global economy. For instance, the US economic and trade sanctions on Russia in the recent Russia-Ukraine conflict did not achieve the desired results partially due to the dependency of multiple states on Russian energy supplies, including Europe.

In summary, while deterrence concepts like denial, punishment, and entanglement seem to be theoretically applicable to cyberspace, practical implementation faces formidable challenges. Achieving deterrence in cyberspace on the parameters of nuclear concepts is not very practical. The unique attributes of cyberspace, including its asymmetric nature, attribution difficulties, and the complex interconnectedness of systems, necessitate a nuanced and evolving approach to cyber deterrence. These challenges can be addressed to a limit through international cooperation, the development of norms and rules of engagement, and ongoing efforts to enhance cyber resilience and defense capabilities. However, it can be argued that near-complete deterrence in cyberspace can be acquired through any such technological advancement that will be indigenous to the domain such as quantum computing.

Quantum Computing; A Nuclear Equivalent in Cyberspace

Quantum Computing and Strategic Warfare

A crucial part of the United States and China's larger geopolitical conflict is their strategic competition in cyberspace. Both states now battle in cyberspace for political influence, intelligence collection, and possibly even military superiority in addition to economic and technological advantages. Achieving quantum supremacy is seen as a critical milestone in achieving supremacy and deterrence in the cyber domain by both states. The country that attains this capability first gains a strategic technological advantage, potentially influencing the balance of power in global affairs. Quantum capabilities will potentially be a strategic imperative for national security. Possessing advanced quantum technologies enhances a state's geopolitical influence and its cyber warfare strategies similar to nuclear weapons.

Quantum Computing and Cyber Deterrence

One can suggest that cyber deterrence will eventually come from the flow of data and quantum technologies. The ability of the quantum computer to swiftly break encryption codes, search data at high speed, and function with greater power than contemporary supercomputers breaks the blockades to cyber transparency.[6] The ability to search data quickly and solve differential data along with appropriate software will be able to depict graphically real-time happenings in cyberspace, creating situational awareness resulting in the possibility of clear attribution. Hence resulting in the credibility to retaliate effectively. Quantum computers can even enhance denial strategies, the state possessing the technology will be unlikely to get an attack as protecting networks and information through quantum encryption will prevent the adversary from achieving its objectives.[7] Besides that, same as in the nuclear realm, the conflict between two quantum powers will also be unlikely, as the benefit of a first strike will be reduced due to better retaliatory powers. Another aspect of denial can be drawn from the limitation over the physical distribution of quantum computers so that responsible governments only possess the fastest and best ones. In that regard, one must treat quantum computers as regulated objects, similar to nuclear material. This notion of maintaining strict control over quantum computers would be difficult, it would be simpler to make sure the state possessed the newest and most advanced quantum computers. All these characteristics make quantum technologies able to achieve deterrence in the cyber world. Nevertheless, in navigating the complex landscape of quantum computing and its implications for cyberspace deterrence, states must balance competition with cooperation. The development of global norms, collaborative research efforts, and responsible governance frameworks will play a pivotal role in ensuring that quantum technologies contribute to a secure and stable cyberspace environment. The race for quantum supremacy underscores the need for strategic foresight, ethical governance, and international collaboration to harness the full potential of quantum computing for the collective benefit of global cybersecurity and deterrence efforts.

Conclusion

Deterrence in cyberspace is not fully achievable on existing parameters, however, with a multi-dimensional approach incorporating all methods of punishment, denial, entanglement, and international norms and regulation, a workable framework for the prevention of attacks can be formulated. Additionally, as suggested, the advent of quantum computing signaled a new era in which the realisation of quantum technologies holds the potential of fortifying cyber deterrence. The ability to manipulate quantum bits, harness superposition, and leverage entanglement presents unprecedented opportunities to strengthen the security of digital communication and prevent malicious cyber activities. As states contest for quantum supremacy, the potential to break and secure cryptographic systems reshapes the dynamics of cyber deterrence, offering a transformative advantage. As we stand on the brink of this quantum revolution, it becomes increasingly evident that the mastery of quantum computing technologies is intricately linked to the attainment of robust cyber deterrence capabilities, laying the foundation for a more secure and resilient digital future.

Notes and References

[1] Wang, Yazhen, "Quantum Computation and Quantum Information," *Statistical Science* 27, no. 3 (2012): 373–94, http://www.jstor.org/stable/41714771.

[2] Joseph S. Nye, "Deterrence in Cyberspace," *The Strategist*, 7 June 2019, https://www.aspistrategist.org.au/deterrence-in-cyberspace/.

[3] Richard Harknett, "Deterrence by Lawrence Freedman," *Political Science Quarterly*, 2005, https://www.researchgate.net/publication/259814555_Deterrence_by_Lawrence_Freedman

[4] Erica Lonergan, and Mark R. Montgomery, "What Is the Future of Cyber Deterrence?" *The SAIS Review of International Affairs* 41, no. 2 (2015): 61–73, https://www.fdd.org/wp-content/uploads/2022/04/Lonergan_Montgomery_The-Future-of-Cyber-Deterrence.pdf

[5] Timothy M. McKenzie, "Is Cyber Deterrence Possible," *Air Force Research Institute Perspectives on Cyber Power* (January 2017), https://apps.dtic.mil/sti/pdfs/AD1122446.pdf.

[6] James G. Sturgeon, *Taking a Quantum Leap in Cyber-Deterrence*, 2012, https://apps.dtic.mil/dtic/tr/fulltext/u2/1018576.pdf.

[7] Ibid.