This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

The Potential Impact of Cyber Capabilities on Future Strategy

https://www.e-ir.info/2021/05/05/the-potential-impact-of-cyber-capabilities-on-future-strategy/

NITIN MENON, MAY 5 2021

Strategy has always been a consequential idea, as it represents the pursuit of goals set against limited resources available at disposal. Across the history of humankind, technological advancements have redefined the way we address hostilities and the fashion in which we fight wars. The 21st century has seen a spectacular rise in cyber capabilities. In just over three decades since the World Wide Web entered human lives, now there are more than four billion active internet users with cyberspace penetrating every walk of our lives. This article aims to shed light on the real impact of cyber potency on strategy in our present world and future controlled by data.

Cyberspace – A New Paradigm

Traditional conflicts and wars saw confronting states or their proxies strategizing to overpower their adversary in the domains of air, sea, land, and space. Now cyberspace has quickly become the fifth domain of warfare, with the keyboard and mouse appearing to be the modern arms of choice. In 2010, the US acknowledged cyberspace as an operational domain stating that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[1] Former CIA Director Leon Panetta, in 2011, even warned that "the next Pearl Harbour could very well be a cyberattack."[2]

Cyberspace, a unique man-made construct, has given a new meaning to war as anyone can attack almost everyone from anywhere at any time. Owing to its virtual nature, the threat landscape has expanded immeasurably, where security concerns engender from faceless and indistinguishable adversaries. Digital technologies have also accelerated the rise of non-state actors as significant entities in world politics. All this has led to questions regarding adequacy of the past and present strategic thought. Remarking on this, Colin Gray says, "the immaturity of strategic theory for cyber typically is accepted as an inevitable and none-too-troubling consequence of the novelty of cyberspace."[3]

Should there be a Cyber Strategy?

Many strategists have downplayed cyber capabilities as just a tool and not a new means of war.[4] Colin Gray believes "cyber power should be understood as just another category of weapon"[5] and doesn't consider cyber to be vastly different from hitherto operational domains with regards to tactical application and strategy.[6] On the same lines, Thomas Rid claims that "there was no and there is no Pearl Harbour of cyberwar"[7]. According to him, the word 'war' in 'cyber war' has "more metaphoric than descriptive value.[8] He contends that cyberattacks are different from conventional warfare because they don't satisfy the Clausewitzian definition of war as a violent, instrumental, and political use of force.[9] He observed that the colossal distributed denial of service (DDoS) attacks on Estonia in 2007 cannot be called an act of war as "the mere 'blockade' of websites is not violent."[10]

Despite rejecting the war capabilities of cyberspace, Rid admits that "cyberspace turns the offense/defence balance on its head by making attacking easier and more cost-effective while making defending harder and more resource-intense." [11] Even though Rid showed a disdain for a brand-new cyber strategy, this final observation of Rid does make one think about a novel strategic thought for cyberspace.

New Future, New Conflicts

According to Sun Tzu, victory can be accomplished by subduing the enemy without even fighting.[12] Such a pursuit of triumph without sending a soldier across the border happens the best in cyberspace. Remarking upon another uncanny nature of cyber capabilities, Larry May admitted that the objective of cyber-attacks is never to kill or wound soldiers but to destroy property.[13] Speaking about the *ends* these attacks aim for, he says, "the destruction of the computer programs that control centrifuges in a nuclear power plant or the electric power grid that supplies power to military installations, certainly can have as their foreseeable secondary effects that civilians and perhaps also soldiers will suffer."[14]

Cyberattacks, without causing direct injury to humans, have ensured harm to physical infrastructure worth billions, which eventually affect human lives. The notorious Shamoon attack on Saudi Aramco[15] and the 2015 cyber-attack targeting Ukrainian power distribution[16] are few instances of adversaries exploiting cyber fragility around the world. Besides the damage to physical infrastructure, cyber-attacks have resulted in enormous data breaches at MNCs and government agencies causing financial loss and leaking confidential information and intellectual property. Much below this institutional level of destruction, the lives of individuals have been afflicted due to cybercrimes. Millions of LinkedIn log-in details were up for grab on the dark web courtesy of a massive cyber-attack, costing many their privacy and virtual lives.[17]

Globally, the USA, China, and Russia are said to have the most formidable cyber offensive capabilities, which they have been using to stifle their nemeses. While the USA has employed the Stuxnet to quell the nuclear program of Iran, China has been accused of cyber espionage campaigns and hacking information from military networks of the USA, Japan, and India.[18] In 2020, British Intelligence and Security Committee claimed that Russia was incessantly targeting countries around the world with malicious cyber-attacks and also influencing democratic elections.[19] Another intriguing aspect of cyberspace is how it has levelled the playing field. Now, lower-tier rogue states are capable of vicious attacks like Iran launching denial-of-service attacks on American financial institutions after the Stuxnet attack and North Korea disrupting South Korean networks.

Cyberspace has not only subverted political boundaries but also shaken the roots of the Westphalian system that gave precedence to states. The absence of geographical borders and the apparent opacity in this fifth domain of warfare have allowed a surfeit of malicious non-state actors to come up as security threats. Georgian cyber-attacks before the 2008 Georgia-Russia War started and Anonymous group's Operation Israel demonstrate the fervid rise of cyber non-state actors. The perplex modus operandi of non-state actors, their unusual anatomy, confusing allegiances, and diverse motivations have drastically affected strategy in the cyber world and made extenuating their impact onerous.

New Challenges, New Mitigations

We are witnessing a "cybersecurity dilemma" reshaping state strategies in the wake of the rising cyber capabilities of various countries.[20] The nefarious 2007 cyber-attacks on Estonia had far-reaching effects around the world. Estonia quickly cultivated tremendous cyber capabilities and became the host of NATO's Cooperative Cyber Defence Centre of Excellence in 2008. The United States mooted the creation of a Cyber Command in 2009 and established it in 2010 that "operates globally in real-time against determined and capable adversaries."[21] Soon China formed the "Information Security Base," under its PLA General Staff Department, which functions as its cyber command.[22]

Despite variegated state efforts, any cyberspace strategy will be debilitated by some unique challenges. Deterrence, the ability to prevent an attack from one's adversary, becomes baffling considering the cyber enemy's identity, capabilities and motives are almost always uncertain. Deterrence is also worsened by the "very limited or no situational awareness" in cyberspace.[23] Moreover, policy makers wonder how traditional nuclear strategy concepts like pre-emptive first-strike or mutually assured destruction be useful in today's reality. Another question that bewilders strategists is how a government would respond to issues in cyberspace when most of that realm is with the private sector. In America, around 85% of critical infrastructure is owned or operated by the private sector and not

monitored directly by federal agencies.[24] Furthermore, there are a host of cyber threats like espionage, sabotage, and disruption,[25] yet there is an ambiguity regarding their status and definition and there exists no effective international governance model to help shape state strategy.

Trying to solve some of these dilemmas, Joseph Nye suggests deterrence by denial in cyberspace; deterring an attack by fortifying own defensive capabilities to make the cost of the adversary's gains prohibitive.[26] It means. He says building good cyber-defences will ensure "chewing up attacker's resources and time" and "disrupts the cost-benefit model that creates an incentive for attack."[27] Even the 2018 U.S. Cyber Strategy with the motto "Defend Forward" emphasised enhancing the resilience of critical infrastructure.[28] Ben Buchanan says in this unsure world, countries should "solidify their bilateral relationships" which will help "interpreting the intentions of potentially hostile actors" better and advancing one's security.[29] The work done by liberal democracies in forming alliances like QUAD and focus on cyber capabilities show their inclination towards a united stance against China and its proxies.

Conclusion

Though the pace of innovation in the cybersphere has been greater than any other domain of warfare, strategy has always had an enduring nature. Concerning this, Gray says, "there is an essential unity to all strategic experience in all periods of history because nothing vital to the nature and function of war and strategy changes."[30] But future wars or conflicts would never resemble past or present ones. We are living in times when we do not even know when a cyber-attack starts and when it ends, whether there is peace or a virtual war. The goal of any strategy must be to anticipate the profound changes in the conflict environment, evolve, and prepare efficiently to get a decisive advantage. Thus, for cyberspace, we need to reanalyse our long-held beliefs of what is violence, and what is war. The future of strategy in the 21st century would be in understanding conflicts, in the light of the technological changes, as a "continuous interaction of opposites"[31] and then making use of centuries worth of strategic thought.

[1] White House, *National Security Strategy* (Washington, DC: White House, 2010), 27, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[2] Jason Ryan, 'Leon Panetta Warns of Possible Cyber-Pearl Harbor', *ABC News*, accessed 26 February 2021, https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905.

[3] Colin S. Gray, *Making Strategic Sense of Cyber Power* (Strategic Studies Institute, US Army War College, 2013), 3.

[4] Gray, "Making Strategic Sense of Cyber Power", 12.

[5] Ibid, 12.

[6] Ibid, 13.

[7] Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35, no. 1 (2012): 29.

[8] Ibid, 15.

[9] Ibid, 7.

[10] Ibid, 13

[11] Ibid, 28.

[12] Sun Tzu, *The Art of War* (Dover: Dover Publication, 2002), 40.

[13] Larry May, 'The Nature of War and the Idea of "Cyberwar"', in *Cyber War* (Oxford: Oxford University Press,

2015), 5.

[14] May, 'The Nature of War and the Idea of "Cyberwar", 5.

[15] Nicole Perlroth, 'Cyberattack on Saudi Firm, U.S. Sees Iran Firing-Back', *The New York Times*, accessed 25 February 2021, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[16] 'Ukraine Power Cut "was Cyber-Attack', *BBC*, accessed 25 February 2021, https://www.bbc.com/news/technology-38573074.

[17] 'LinkedIn Users' Log-in Details "for Sale on Dark-Web"', *Independent*, accessed 26 February 2021, https://www.independent.ie/business/technology/millions-of-linkedin-users-log-in-details-for-sale-on-dark-web-34727328.html.

[18] Brandon Valeriano and Ryan C. Maness, 'Cyber Power, Cyber Weapons, and Cyber Operations', in*Cyber War versus Cyber Realities* (New York: Oxford University Press, 2015), 26.

[19] 'Report Reveals Cyber-Warfare Campaign against UK', *ComputerWeekly.Com*, accessed 26 February 2021, https://www.computerweekly.com/news/252486422/Russia-Report-reveals-long-running-cyber-warfare-campaign-against-UK.

[20] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (New York: Oxford University Press, 2017), 3.

[21] "About the U.S. Cyber Command," U.S. Cyber Command, accessed 25th February 2021, https://www.cybercom.mil/About/History/

[22] 'China's Cyber Command?', *Jamestown*, accessed 27 February 2021, https://jamestown.org/program/chinas-cyber-command/.

[23] 'DoD Has Limited Cyber Situational Awareness', *Federal News Network*, accessed 26th February 2021, https://federalnewsnetwork.com/defense/2010/06/dod-has-limited-cyber-situational-awareness/.

[24] 'Critical Infrastructure Protection and Cyber-Security', *U.S. Chamber of Commerce*, accessed 26th February 2021, https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security.

[25] Rid, 'Cyber War Will Not Take Place', 28.

[26] Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security* 41, no. 3 (2017): 56.

[27] Ibid, 56.

[28] U.S. Cyber Command, "About the U.S. Cyber Command"

[29] Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, 163*.

[30] Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 1.

[31] Carl Von Clausewitz, *On War* (New Jersey: Princeton University Press, 1989), 136.