THE PERSISTENCE OF VIOLENCE IN THE CYBER AGE

By **MAJ Jeffrey Ng Zhaohong**

ABSTRACT

According to the author, with the advance of technology, cyber space has become the new battleground for war. It has provided huge opportunities for many countries to further their political agendas without resorting to violent conflicts. In fact, similar to the threat of nuclear destruction, cyber attacks' threat of widespread devastation can deter and compel against violent escalations. Furthermore, cyber space's high cost-effectiveness and difficulty in attribution provide a viable non-violent avenue to achieve political gains. Besides manipulating rational calculations, cyber information operations can subvert people's passions and soften the psychological battlefield, thereby reducing the violence involved in achieving one's political goals. However, the author highlights that historical examples have shown that in a clash for survival and critical interests, man will exhaust all means, including physical violence and destruction, to exploit vulnerabilities in all dimensions to preserve his interests. He concludes that violence will continue to persist as part of the nature of war.

Keywords: *Cyber, Passion, Violence, Threat, Manipulate*

With the dawn of the cyber age, many established militaries and thinkers have pondered the implications of cyber operations for both the nature and character of war.[1] Clausewitz defined war as serving political goals, and as a 'paradoxical trinity' comprising violence, chance and rationality.[2] An elimination of any of the three elements would indicate a fundamental shift in the nature of war. On the other hand, the character of war can vary according to the interactive relationship between the three elements. Rationality, associated with political leadership, dictates the boundaries and direction for military strategies. The execution of these strategies then involve chance and probability. Violence and its accompanying passions influence the balance between chance and rationality according to the stakes involved—the higher the stakes, the more likely that passions will favor chance over rationality and push the character of war to violent extremes. Conversely, limited political aims may favor rationality over chance to minimise the use of violence. With cyber space touted as a war-fighting dimension, the time has come to contemplate if cyber operations have truly augured a revolution by eliminating violence from the trinity of war. While the character of war may become less violent as states exploit cyber space to pursue political gains through the manipulation of rationality and passions, violence will continue to persist in clashes of high political stakes as effective cyber countermeasures and strong passions will ultimately force a resolution through physical violence.

Through its threat of widespread destruction and disruption, cyber operations are similar to nuclear weapons in manipulating rational cost-benefit-risk calculations and creating deterrence against violent conflicts. According to Schelling, the threat of large scale destruction is more effective than its actual use.[3] Schelling further explained that the mere possession of nuclear weapons, coupled with a credible reputation for using them, is sufficient to deter violent escalation of political competition.[4] In addition, the threat of mutual annihilation allows nuclear states to manipulate shared risks, using brinksmanship to compel each other to back down from his political position.[5] This was seen in the Cuban Missile Crisis when the Union of Soviet Socialist Republics (USSR) was compelled to de-escalate and withdraw its missiles from Cuba given that the anticipated cost of nuclear strikes on Moscow dwarfed the limited political gains in a tit-for-tat strategy against the United States' (US) deployment of ballistic missiles in Turkey and Italy.[6]

Russians hackers wanted by the Federal Bureau of Investigation (FBI) for interference during the 2016 US Presidential Elections.

In a similar vein of manipulating rational cost-benefit calculations, cyber operations can deter violent escalations by its threat of widespread disruption while providing an attractive non-violent alternative for furthering one's goals. Similar to a nuclear threat, cyber operations can wreak large-scale disruption through co-ordinated and simultaneous targeting of critical computer networks supporting key national infrastructure such as energy, water supply, electrical grid, communication nodes and financial institutions.[7] The ability to shut down normal functions of all instruments of power can exert the same deterrence effects as the threat of a nuclear attack. In addition, the magnitude and severity of attacks can be more rapidly

scaled up than traditional military capabilities. Hence, a demonstration of limited use, such as Russia's involvement in the Distributed Denial of Service (DDoS) attacks on Estonia and Georgia, is sufficient to build up the credibility and reputation needed to exert deterrent effects.[8] Similar to Brodie's advocacy of nuclear weapons as a highly cost-effective capability, cyber operations can yield great political pay-offs with little investment in resources.[9] This was demonstrated when Russian 'patriotic hackers' and 'hacktivists' ran primitive cyber attack codes on their home computers to attack Georgian websites, resulting in widespread denial-of-service in Georgia's public and private sectors, including Georgia's largest commercial bank.[10] Besides, difficulty in attribution provides insurance against violent retaliation due to the lack of legitimacy and timeliness for reprisals. Hence, cyber operations' threat of widespread damage provides deterrence against violent escalation, while its high cost-effectiveness and low risk of attribution provide an attractive avenue for rational actors to further their political goals without resorting to violence.

Besides manipulating a government's rational calculations, cyberspace, through its widespread usage and ease of access, provides opportunities for insidious undermining and subversion of public opinions to reduce moral resistance. In accordance with Clausewitz's recognition of 'the spirit and other moral qualities' in influencing the outcome of war, military strategists have often contemplated undermining strategic leadership and the people's collective will to reduce moral resistance and facilitate swift victories.[11] For example, Fuller saw potential in the tanks' speed and mobility to strike directly and unexpectedly at the Army's leadership to 'render inoperative the command of the enemy's forces,' thereby reducing moral and physical resistance in subsequent battles through strategic paralysis.[12] Similarly, Douhet advocated capitalising on airpower's speed and reach to conduct strategic bombing on civilian population centres to break the public's will and cause them to 'rise up and demand an end to the war.'[13]

The ability to shut down normal functions of all instruments of power can exert the same deterrence effects as the threat of a nuclear attack.

The simultaneity, speed and penetration of cyber operations far exceed that of tanks and airpower. Besides, cyber information warfare can undermine leadership and the people's will without incurring high costs and violence, and hence provides an attractive

Pro-Russian encampment outside the Trade Unions House, Ukraine, 6th April, 2014.

avenue for state and non-state actors to insidiously manipulate its target audience's perceptions. For example, Russia conducted a comprehensive cyber information campaign to achieve the annexation of Crimea with minimal violence.[14] Through the use of fake social media posts and fake news sites, coupled with cyber attacks disrupting communications and government functions in Crimea, Russia successfully orchestrated a 'blizzard of denial, deception and disinformation' to paralyse the Ukrainian government while creating the perception of an indigenous Crimean grassroots movement to join the Russian Federation.[15] Hence, through its unprecedented speed, reach and parallel effects, cyber information operations can be more effective than tanks and airplanes in breaking its adversary's collective will while stoking its people's nationalistic feelings to bolster its moral spirits. By manipulating the people's passions, states can shape the psychological battlefield to their advantage and achieve political goals with much less violence and bloodshed.

Despite the allure of cyberspace as a beacon of hope for eliminating violence, clashes involving high stakes and strong passions will ultimately resort to violence for resolution. As Clausewitz explained, a war's outcome is transitory and the defeated will soon adapt and exploit vulnerabilities to restore the equilibrium.[16] Hence, ingenious development of effective countermeasures and strategies will eventually erode the competitive edge afforded by technological advances. This is especially so when the consequences of losing are deemed unacceptable and strong passions demand resistance at all costs, as demonstrated in Japan's willingness to adopt kamikaze tactics and field manned torpedoes against the American aircraft carriers in a last ditch effort to prevent a homeland attack.[17] In World War I (WWI), the water-cooled machine guns were highly effective in overwhelming advancing armies, but were soon pounded by accurate indirect artillery fires.[18] At sea, German ocean-going submarines effectively challenged British naval surface dominance, but were countered with depth charges and sonar detection.[19] In the air, British's fast and agile interceptor monoplanes and radar interception techniques successfully thwarted Germany's bombing raids.[20] In addition, as witnessed in the Vietnam War, materially inferior forces such as the Viet Cong could adopt asymmetric strategies and exploit vulnerabilities to defeat the technologically superior US forces.[21]

Ingenious development of effective countermeasures and strategies will eventually erode the competitive edge afforded by technological advances.

Donald Trump tweets on twitter suggesting that he won the election. The tweets are marked as disputed.

Cyber information operations can subvert the people's passions and soften the psychological battlefield, thereby reducing the violence involved in achieving one's political goals.

Therefore, it is expected that states will pursue effective countermeasures and strategies to erode the advantages of cyber offensive capabilities. Recognising the strategic threat of cyber attacks, the US has stated its focus in accelerating cyber capability development to counter malicious activities and strengthen the cyber-security of key government networks through partnership with private sector and allies.[22] To defend against subversive social media posts and fake news, governments stepped up social awareness on the threat of malicious cyber misinformation through high visibility campaigns, such as the publicised grilling sessions of Facebook and Twitter for their failings in regulating the spread of mistruths.[23] In addition, in clashes concerning national survival and sacrosanct interests, cyber propaganda can quickly inflame nationalistic sentiments, leading to a stronger push for the employment of all instruments beyond cyberspace, including physical military capabilities. Hence, even in the cyber age, as long as stakes are high and passions are stoked, violence will still erupt.

CONCLUSION

Through its widespread use, cyberspace has become an integral dimension of most of the world's functions and this created huge opportunities for furthering political agendas without resorting to violent conflicts. Similar to the threat of nuclear destruction, cyber attacks' threat of widespread devastation can deter and compel against violent escalations. In addition, cyberspace's high cost-effectiveness and difficulty in attribution provide a viable non-violent avenue to achieve political gains. Besides manipulating rational calculations, cyber information operations can subvert the people's passions and soften the psychological battlefield, thereby reducing the violence involved in achieving one's political goals. However, historical examples show that in a clash for survival and critical interests, man will exhaust all means, including physical violence and destruction, to exploit vulnerabilities in all dimensions to preserve his interests. Realistically then, violence will continue to persist as part of the nature of war. Beyond academic discussion, taking a Hobbesian view on the persistence of violence compels the state and its people to continue their support for a credible military that is ready to win the nation's wars and secure the peace in both physical and cyber dimensions with the dawn of the cyber age.

ENDNOTES

1. Thomas Rid,"Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no.1 (2012): 5-6, http://dx.doi.org/10/1080/01402390.2011.608939.
2. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 87-89.
3. Thomas C. Schelling, *Arms and Influence*, (New Haven, CT: Yale University, 2008), 10.
4. Ibid., 36-38.
5. Ibid., 99-105.
6. Schelling, *Arms and Influence*, 40-41.
7. Matthew R. Schwonek, "The Cyber Age and Russian Information Warfare" (lecture, Air Command and Staff College, Maxwell AFB, AL, 25 September, 2018), 10.
8. Thomas Rid, "Cyber War Will Not Take Place," 11-14.
9. Bernard Brodie, "The Weapon: War in the Atomic Age," in Bernard Brodie et al., eds., *The Absolute Weapon: Atomic Power and World Order* (Book draft, 1946), 33.
10. Thomas Rid, "Cyber War Will Not Take Place," 25.
11. Clausewitz, *On War*, 184.
12. John Frederick C. Fuller, "Strategic Paralysis as the Objective of Decisive Attack," in *On Future Warfare* (London: Sifton Praed, 1928), 93.
13. Giulo Douhet, The Command of the Air (Washington DC: U.S. Government Printing Office, 1983), 58.
14. Schwonek, "The Cyber Age and Russian Information Warfare," 18-19.
15. Ibid.
16. Clausewitz, *On War*, 79-80.
17. Lynn Vincent and Sara Vladic, *Indianapolis* (New York, NY: Simon & Schuster, 2018).
18. James D. Campbell, "World War I and the Evolution of Combined Arms Maneuver Warfare" (lecture, Air Command and Staff College, Maxwell AFB, AL, 28 August 2018), 25.
19. Michael Howard, War in Euro History (Oxford: Oxford University Press, 2009), 125. John T. LaSaine, "The Struggles for Mastery of the Sea, 1898-1918" (lecture, Air Command and Staff College, Maxwell AFB, AL, 7 September, 2018).
20. Howard, War in Euro History, 130.
21. Ivan Arreguin-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," International Security, Vol. 26, No. 1 (Summer 2001), 93-128.
22. Department of Defense, "Department of Defense Cyber Strategy 2018 Summary," Department of Defense, accessed 28 September 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf .
23. Tim Mak, "Senate Committee vents about hijacking of Big Tech for Information War," NPR, accessed 1 October 2018, https://www.npr.org/2018/09/05/644607908/facebook-twitter-heavies-set-to-appear-at-senate-hearing-google-may-be-mia.

MAJ Jeffrey Ng is a qualified Heron 1 UAV Command Pilot and is currently the Squadron Commander of 119 SQN in UAV Command. Prior to this, he was serving as a Senior Force Transformation Officer in Joint Plans & Transformation Department, contributing to the strategising of future warfighting concepts. MAJ Ng holds a Bachelor in Psychology from University College London (UCL) and a Master in Performance Psychology from the University of Edinburgh. MAJ Ng also graduated from the United States Air Command and Staff College in 2019 as a Distinguished Graduate and is a recipient of the Commandant's International Officer Academic Award.