Information Warfare – The Challenges and Opportunities for Militaries in the Information Age

by **CPT Jeffrey Ng Zhaohong**

Abstract:

This essay argues that owing to the globalisation of information technology, conflicts today will not only see an increase in the use of information in warfare as an operational and strategic imperative, but also in the use of information as warfare to provide non-kinetic capabilities for achieving strategic outcomes. It then briefly examines the implications for modern militaries and concludes that the information domain will bring game-changing strategic value to militaries that can master both information in warfare and information as warfare.

Keywords: Technology; Information Age; Information Barrage; Availability; Ease of Access

INTRODUCTION

While humans have interacted over long distances for thousands of years, the speed and scale of transnational human interaction around the world has seen an unprecedented surge, enabled by increasingly rapid forms of transportation and communication. This has greatly compressed the time and space needed for the exchange of goods, ideas, knowledge and technology. This increasing interconnectedness, branded as 'globalisation' towards the turn of the millennium, was further amplified by the prolific use of the Internet following the introduction of the World Wide Web.[1] The concomitant revolution in the information technology and communications landscape, touted as the information age, has shaped politics, demolished regimes, given rise to new markets, and offered a bigger voice to the individual. Unsurprisingly, the information age has also heralded transformations in the conduct of present-day military conflicts. This essay argues that owing to the globalisation of information technology, conflicts today will not only see an increase in the use of information in warfare as an operational and strategic imperative, but also in the use of information as warfare to provide non-kinetic capabilities for achieving strategic outcomes. It then briefly examines the implications for modern militaries and concludes that the information domain will bring game-changing strategic value to militaries that can master both information in warfare and information as warfare.

NEW NORMS IN THE INFORMATION AGE

The globalisation of information technology has enabled individuals and organisations to interact at an unprecedented scale and speed. For example, access to the Internet has grown from just 5% in 2000 to over 42% in 2014.[2] With an increasing ease of instantaneous information access, traditional state-driven censorship and media control as a means to regulate and shape public opinions are fast becoming obsolete and counter-productive because individuals have become empowered to scrutinise and challenge

Celebrations in Egypt's Tahrir Square after Vice President Omar Suleiman's statement concerning President Hosni Mubarak's resignation.

the actions of well-established social and government institutions. In parallel, the proliferation of mobile communications, and the rising participation rate in social media over the past decade have enabled individuals to share and shape public opinions, garner support from like-minded individuals, and rapidly self-mobilise for a common cause against governments, as witnessed in the Arab Spring and the various Occupy Movements in 2011.[3] Taken together, societies in the information age possess heightened awareness of the diverse opinions and portrayals of world events, and are less likely to rely solely on the government's interpretation of events. To deal with the increased public demand for accountability and transparency, governments are now compelled to actively engage and convince the public of its legitimacy in order to engender continued support for its actions and policies.

The use of information in warfare to achieve operational objectives has always been an integral arm of military warfare, be it in the forms of covert intelligence or overt domestic propaganda.

The information age has not only altered the social compact within individual states; it has also interwoven states, corporations, and organisations into interdependent networks due to the growing reliance on the use of computers and information systems. In the civilian and commercial domains, the explosive growth of information technology, especially in terms of online storage and network traffic capacity, has accelerated the adoption of electronic systems, as well as vastly increased the dependency on wireless communications to digitise and automate daily tasks. Modern militaries have also

leveraged on the available technology to transform their operations using networked concepts.[4] Such network-centric warfare heavily hinges upon a robust and resilient network infrastructure to link together various sensors and shooters with computer systems to vastly speed up the kill cycle. The widespread reliance on networked information systems in state and non-state organisations has also increased the inter-dependency between these entities for functional integrity. Such national-level vulnerabilities, arising from the growing dependence on networked systems, present militaries with both challenges and opportunities in the present-day conflicts.

INFORMATION IN WARFARE - AN OPERATIONAL AND STRATEGIC IMPERATIVE

The use of information in warfare to achieve operational objectives has always been an integral arm of military warfare, be it in the forms of covert intelligence or overt domestic propaganda. However, with the increase in speed and reach of information, any newsworthy conflict will be immediately thrust into the consciousness of the international community, and subjected to scrutiny, debates, and opinions which will shape the portrayal of the parties involved in the conflict. Moreover, traditionally weaker adversaries can leverage on cheap and readily available information technology such as social media platforms and video hosting websites, to wield disproportionate influence over domestic and international masses to systematically undermine the legitimacy and morality of the military and also mobilise local populations to rise up against the invading military. Hence, carefully crafted multi-faceted information operations, as an essential element of an overall military strategy, will become an increasingly pivotal operational and strategic imperative for winning the battle of perceptions, securing operational battle-space, and achieving strategic victory in present-day conflicts.

The centrality of information operations to the strategic success of present-day conflicts is exemplified by contrasting the outcomes of the 2006 Second Lebanon War and the 2009 Operation Cast Lead. Despite the Israeli Defense Force (IDF)'s tactical successes in the Second Lebanon War, Israel was unable to achieve strategic victory against the Hezbollah. In fact, the organisation's charismatic leader, Hassan Nasrallah, was able to emerge from the conflict with his reputation intact.[5] Post-mortem analysis of the conflict indicated that the strategic failure was largely attributed to Israel's inability to paint a coherent narrative to blunt Hezbollah's portrayal of the IDF's disproportionate use of force against civilian victims.[6] For example, the destruction wrought by the IDF's use of air power against civilian buildings provided copious material for Hezbollah's civilian-victim narrative. On the other hand, Hezbollah was able to coerce and manage the international press in Lebanon to ensure the non-existence of Hezbollah's combat imagery, further reinforcing the perception that defenceless Lebanese civilians were being bullied by the IDF.[7] The theme of 'disproportionality' resonated with the international audience, and mounted political pressures on Israel, ultimately forcing the IDF to halt its operation before it could achieve its operational objectives.[8]

Learning the strategic significance of a coherent information effort, Israel established the Directorate of National Information in 2007 to coordinate and develop inter-ministerial plans and strategies for a whole-of-government approach in information operations during national emergencies.[9] The increased emphasis on the information battle was evident in Operation Cast Lead in 2009, during which the Israeli government was able to consistently portray an overarching narrative against the Hamas through a coordinated inter-ministerial approach.[10]

Smoke rising from a bombed building in Lebanon during the Second Lebanon War.

This was further complemented by the innovative use of social media sites to disseminate imagery from the soldiers' cameras to the international audience in a timely manner. The real life ground and Unmanned Aerial Vehicle (UAV) footages enhanced the IDF's emotive connection with the audience and authenticated claims of its relentless efforts in minimising collateral damage and civilian casualties. Consequently, Israel was able to secure the operational battle-space necessary for the IDF to achieve its operational objectives without overwhelming political incrimination.

The strategic failure of the Second Lebanon War and the relative success in Operation Cast Lead illustrated that in the information age, a coherent and proactive information campaign waged on traditional and online media must complement traditional operations in order to dominate the international mindshare with favourable portrayals and secure strategic political legitimacy. Winning the battle of perceptions is not only important for freedom of operations, but also pivotal to the strategic outcome of the conflict.

INFORMATION AS WARFARE – CYBER WARFARE

Beyond the use of information to shape strategic narratives, the proliferation and near-universal accessibility of information technology can potentially supplant the Clausewitzian industrial-era model of destruction-driven warfare with an information age model of disruption-based operations waged through the use of smart technologies in the cyberspace.[11] The exploitation of national-level vulnerabilities in information networks opens up

possibilities for non-lethal cyber attacks to disrupt, incapacitate, defeat or deter an adversary, thereby attaining strategic objectives without resorting to resource-intensive conventional kinetic operations. As both society and militaries become more networked and reliant on computers and information systems, the cyber domain will likely become the predominant battle-space for conflicts in the information age because of the strategic strengths conferred by cyber warfare.

As both society and militaries become more networked and reliant on computers and information systems, the cyber domain will likely become the predominant battle-space for conflicts in the information age because of the strategic strengths conferred by cyber warfare.

Firstly, the rapid growth in worldwide interconnectedness of online systems allows operations in cyberspace to provide global reach, even to areas where access is denied to other domains. This is unlike traditional military operations, which are often confined by geographic limitations. Compared to the projection of troops into contested areas, cyber operations can also provide access without physical risks to the operators. Another alluring advantage of cyber operations is its ability to strike with speed and precision. Computer virus dissemination through online networks can occur literally at the speed of light through fibre optic cables, and can be selective in targeting specific networks to achieve intended effects with minimal collateral damage. These strengths were well demonstrated in the employment of the malware 'Stuxnet' to disrupt the Iranian nuclear centrifuges by targeting the industrial control systems.[12] The malware attack, allegedly a joint US-Israel endeavour, damaged over a thousand centrifuges at the Natanz uranium enrichment facility, and successfully delayed Iran's acquisition of a nuclear device without any forward deployment of troops, breach of Iranian airspace, loss of life, or physical damage to the nuclear facility.[13] The 'Stuxnet' attack also demonstrated another strategic advantage of warfare in the cyber domain – anonymity. The high degree of decentralisation and peer-to-peer networks characterising the cyber domain makes it challenging to trace the evidentiary trail to originators of the cyber attacks.[14] This confers great latitudes of action with limited attribution and hence, minimises potential social and political backlash on the perpetrators.

The strengths offered by cyberspace favours offensive operations over defence. Moreover, unlike traditional weapons, the tools needed to wage cyber warfare may be freely accessible on the Internet or traded in underground markets.[15] This creates greater asymmetry in a conflict by allowing state and non-state actors that have limited resources and are weaker in traditional domains of warfare to exploit the cyber domain for strategic effects of disruption, and even destruction of system capabilities. For example, in 2013, a small group of hackers named 'the Anonymous Collective' or 'the Messiah' allegedly managed to disrupt the normal functioning of 19 Singapore governmental websites.[16] Paradoxically, the more sophisticated the fighting force, the higher the likelihood of suffering from cyber attacks. The consequences of a successful attack are also greater due to the systemic dependency of routine operations on the integrity of networks and computer systems. In light of the strategic threats and opportunities offered by the use of the information domain, leading militaries such as the United States (US) Air Force

have stepped up on their efforts in building up cyber warfare capabilities.[17] Singapore has also recognised the importance of a co-ordinated national approach against cyber threats to its national infrastructure, and in response, has established the Cyber Security Agency to strengthen cyber security in sectors critical to the nation's survivability.[18]

IMPLICATIONS FOR MODERN MILITARIES

With the growing strategic importance of the information domain for present-day conflicts, modern militaries will be increasingly compelled to focus on information operations and cyber warfare capabilities in order to maintain their strategic edge over other state and non-state actors. To truly harness the strategic value of information operations, modern militaries would need to restructure themselves to be centralised and dedicate focus on planning and orchestrating a coherent strategic narrative. Military operations should also be planned and coordinated to support the strategic campaign message. This is because in today's conflicts, conducting military operations in isolation of a central narrative will run the risk of adversaries using these operations to reinforce their own narratives. In contrast, a unified message stemming from complementary operational effects would serve to solidify the military's legitimacy, and allow the military to quickly translate operational success into strategic victories. For example, during Operation Cast Lead, in a bid to maintain its moral standing and to erode the Hamas' civilian-victim narrative, the IDF deliberately deployed Combat Camera teams to provide footages demonstrating the Hamas using mosques as weapon caches, and also flew dedicated sorties to drop leaflets asking civilians to vacate the area before each air strike.[19]

Paradoxically, the more sophisticated the fighting force, the higher the likelihood of suffering from cyber attacks.

Similarly, the strategic importance of cyber operations would compel modern militaries to develop

A screenshot of a Singapore website that was being hacked into by the group known as 'Anonymous'.

cyber warfare capabilities in a coherent approach as a strategic capability, instead of ad-hoc enhancements to existing capabilities. Militaries pursuing cyber operations as an individual military domain should also aim to fulfil the full range of military objectives, including physical destruction in order to harness the strategic gains of cyber warfare. Advanced militaries facing manpower and budgetary constraints would likely spearhead the development and employment of cyber attack capabilities given the high resource efficiency of cyber operations. Consequently, robust cyber defence capabilities would become staple operational requirements for undisrupted military operations in the present day. Given the convergence between defence against military cyber attacks and commercial cyber crime, militaries could explore synergistic inter-ministerial developments, leverage creatively on commercially available technology, and adopt established commercial cyber defence protocols in order to quickly develop sustainable cyber defence capabilities.

CONCLUSION

Globalisation of information access has exponentially increased the interconnectedness of human consciousness and computer systems through worldwide proliferation of networked information technology. Consequently, present-day conflicts are waged under the scrutiny of the international audience. Hence, information operations in warfare will play an increasingly pivotal role as an operational and strategic imperative to cultivate favourable political atmospherics for continued freedom of action. The growing dependence on the cyber space in the information age offers cyber warfare as an alternative realm for waging present-day conflicts. The widespread accessibility of information technology provides state and non-state actors with the necessary tools for both information operations and cyber attacks, tilting the balance against traditionally superior fighting forces. To ensure strategic success in the information age, militaries and their governments must rapidly re-examine their organising principles and adopt current technologies to develop comprehensive information warfare capabilities in line with a coherent national strategy.

BIBLIOGRAPHY

Albright, David, and Andrea Stricker. "Stuxnet Worm Targets Automated Systems for Frequency Converters: Are Iranian Centrifuges the Target?" Institute for Science and International Security, November 17, 2010.

http://isis-online.org/isis-reports/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-is-irans-ce/8.

Allagui, Ilhem, and Johanne Kuebler. "The Arab Spring and the Role of ICTs." International Journal of Communication 5 (2011): 1435-1442.

Bishop, Matt, and Emily Goldman. "The Strategy and Tactics of Information Warfare." Contemporary Security Policy 24 (2003): 113-139.

Catignani, Sergio. "Variation on a Theme: Israel's Operation Cast Lead and the Gaza Strip Missile Conundrum, " The Rusi Journal, 154 (2009): 66-73.

Cebrowski, Arthur K, and John H. Garstka. "Network-Centric Warfare: Its Origin and Future." US Naval Institute Proceedings Magazine 124 (1998), 28-35.

Greenberg, Andy. "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits." Forbes, March 23, 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-forzero-days-an-price-list-for-hackers-secret-software-exploits.

International Monetary Fund. "Issues Brief - Globalization: A Brief Overview." Accessed February 1, 2015. http://www.imf.org/external/np/exr/ib/2008/053008.htm.

Internet World Stats. "World Internet Users Statistics and 2014 Population Stats." Accessed February 1, 2015. http://www.internetworldstats.com/stats.htm.

Kalb, Marvin, and Carol Saivetz. "The Israeli—Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." The International Journal of Press/Politics 12 (2007): 43-66.

Lee, Terence. “19 Singapore Government Websites Taken Down Simultaneously for “Planned Maintenance”.” Tech in Asia, November 2, 2013.

https://www.techinasia.com/16-singapore-government-websites-simultaneously-planned-maintenance.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” Security Studies 22 (2013): 365-404.

Nakashima, Ellen. "Pentagon to Fast-Track Cyberweapon Development." The Washington Post, March 18, 2012.

http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html.

Snyder, Michael D. “Information Strategies Against a Hybrid Threat: What the Recent Experience of Israel Versus Hezbollah/Hamas Tell The US Army.” In Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD, edited by Scott C. Farquhar, 103-146. Fort Leavenworth, Kansas: Combat Studies Institute Press, 2009.

Stewart, Frances. "Global Economic Influences and Policies towards Violent Self-Determination Movements: An Overview.” In Globalization, Violent Conflict and Self-Determination, edited by Valpy FitzGerald, Frances Stewart and Rajesh Venugopal, 20-47. New York: Palgrave Macmillan, 2006.

Tham, Irene. “New Cyber Security Agency to be set up in April, Yaacob Ibrahim to be Minister in Charge of Cyber Security.” The Straits Times, January 18, 2015. http://www.straitstimes.com/news/singapore/more-singapore-stories/story/national-cyber-security-efforts-fall-under-new-cyber-sec.

The Statistics Portal. "Number of Global Social Network Users 2010-2018.” Accessed February 5, 2015. http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

Wilson, Clay. “Cyber Crime.” In Cyberpower and National Security, edited by Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, 415-436. Washington, DC: National Defense University Press, 2009.

ENDNOTES

1. IMF Staff, Globalization: A Brief Overview, (International Monetary Fund, 2008) http://www.imf.org/external/np/exr/ib/2008/053008.htm.
2. "World Internet Users Statistics and 2014 Population Stats," Internet World Stats, accessed February 1, 2015, http://www.internetworldstats.com/stats.htm.
3. Ibid.
4. Number of Global Social Network Users 2010-2019 (in billions), (statista, The Statistics Portal) http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

   Stewart, Frances, Global Economic Influences and Policies towards Violent Self-Determination Movements: An Overview, (New York: Palgrave Macmillan, 2006).

   Allagui, Ilhem and Kuebler, Johanne, The Arab Spring and the Role of ICTs, (International Journal of Communication 5, 2011)
6. Arthur K. Cebrowski and John H. Garstka, Network-Centric Warfare: Its Origin and Future, (*US Naval Institute Proceedings Magazine*, 1998), v._124
7. Michael D. Snyder, Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD, (*DIANE Publishing*, 2010), 115.
8. Ibid., 120.
9. Kalb, Marvin and Saivetz, Carol, THE ISRAELI-HEZBOLLAH WAR OF 2006: The Media As A Weapon In Asymmetrical Conflict, (Harvard University, 2007), 43-66.
10. Ibid., 55.
11. Snyder, Information Strategies, 126.
12. Ibid.
13. Bishop, Matt and Goldman, Emily, The Strategy and Tactics of Information Warfare, (*Contemporary Security Policy* 24, 2003), 113.

14. Albright, David and Andrea Stricker, Andrea, Stuxnet Worm Targets Automated Systems for Frequency Converters: *Are Iranian Centrifuges the Target?, Institute for Science and International Security*, 2010) http://isis-online.org/isis-reports/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-is-irans-ce/8.

15. Jon R. Lindsay, Stuxnet and the Limits of Cyber Warfare, (*Security Studies* 22, 2013)

16. Wilson, Clay, Cyber Crime, Cyberpower and National Security, (*Washington*, DC: NDU Press, 2009)

17. Greenberg, Andy, Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits, (Forbes, 2012) http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-forzero-days-an-price-list-for-hackers-secret-software-exploits.

18. Lee, Terence, 19 Singapore Government Websites Taken Down Simultaneously for "Planned Maintenance", (*Tech in Asia*, 2013) https://www.techinasia.com/16-singapore-government-websites-simultaneously-planned-maintenance.

17. Nakashima, Ellen, Pentagon to Fast-Track Cyberweapon Development, (*The Washington Post*, 2012) http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html.

18. Tham, Irene, New Cyber Security Agency to be set up in April, Yaacob Ibrahim to be Minister in Charge of Cyber Security, (*The Straits Times*, 2015) http://www.straitstimes.com/news/singapore/more-singapore-stories/story/national-cyber-security-efforts-fall-under-new-cyber-sec.

19. Catignani, Sergio, Variation on a Theme: Israel's Operation Cast Lead and the Gaza Strip Missile Conundrum, (*The Rusi Journal* 154, 2009), 71.

CPT Jeffrey Ng Zhaohong is currently serving as an Officer Commanding in 119 SQN, UAV Command. He is a UAV Pilot by vocation and is a Command Pilot of the Heron 1 UAV. A recipient of the SAF Merit Scholarship in 2008, he graduated from University College London with a Bachelors of Science Psychology with Honours in 2011, and subsequently from the University of Edinburgh with a Masters of Science in Performance Psychology.