National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Space and Cyber Capabilities in a Changing Modern Operational Environment

Major Woong Kim

JCSP 48

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 48

Étude Militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 48 – PCEMI 48
2021 – 2022

Service Paper – Étude militaire

Space and Cyber Capabilities in a Changing Modern Operational Environment

Major Woong Kim

SPACE AND CYBER CAPABILITIES IN A CHANGING MODERN OPERATIONAL ENVIRONMENT

INTRODUCTION

1. Kodak, Sony, Motorola and Nokia, what do these companies have in common? Kodak, a camera film company founded in the 1880s, was once a rapidly growing company in the film field to the point where the film was called Kodak. However, despite the spread of digital cameras since the 2000s, Kodak has led to a decline in companies by focusing only on product development to strengthen existing analogue films rather than strengthening the digital camera business[1].

2. Sony, once called the world's strongest electronics industry, was also complacent about the technology of TV, but the release of digital panel TV products was delayed, and major products such as smartphones, PCs, and cameras failed to show synergy in the combination of content and hardware[2].

3. The science and technology industry, which has developed with mankind, is facing a period of upheaval. In particular, the recent development of information and communication technologies such as computers and networks, which have brought decisive changes to human life, has progressed day by day, adding to the pace of upheaval across the science and technology industry. One interesting fact is that the future of a company is determined by how companies respond innovatively in times of such upheaval.

4. Earlier, both camera film company Kodak and electronics industry Sony failed to actively cope with the advent of the digital era, failing to read the trend of times from analogue to digital and being immersed in the technology they have developed. On the other hand, companies leading IT products and technologies in the current era, such as Samsung, Google, and Apple, have been judging and preparing for the turbulent flow of science and technology in advance.

5. The development of information and communication technology is also a key factor in the development of military weapons systems, strategies, operations and tactics[3]. The reliability of the information collected from the battlefield continues to improve, and rapid information sharing, and situational awareness allow all combatants on the battlefield to carry out operations in line with common goals. Modern and future weapon systems can also strike enemies in a short time while increasing precision and striking power, and commanders can get the information required anytime, anywhere and make timely decisions.

---

[1] Forbes. “How Kodak Failed.” 2012. Accessed on 17 January 2022 at: How Kodak Failed (forbes.com).
[2] The New York Times. “How the Tech Parade Passed Sony By.” 2012. Accessed on 17 January 2022 at: How Sony Fell Behind in the Tech Parade - The New York Times (nytimes.com)https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.
[3] Canadian Department of National Defence. “Strong, Secure, Engaged: Defence Policy”. 2017. 55-57.

6. The logic that applied to the above companies can be applied equally to the military that prepares for war to protect the security of the country. The rapidly changing science and technology are bound to be projected into military power in a direct or indirect form. The question is how much innovative you read the flow of science and technology and prepare for the future war than the other parties.

7. This paper will first address how important capabilities in space, cyber, and information domains are today as times change and subsequent war paradigm shift. In addition, from a threat-based point of view, I will discuss what kinds of capabilities adversaries are developing to gain an edge in these domains and how much it will pose as a threat to us, then emphasize how important capabilities in space, cyber, and information domains play in competition and armed conflict with them. Finally, as this paper concludes, it is inevitable to have capabilities in space, cyber, and information domains, depending on the changing operational environment and threats, and to this end, we could expect that countries find ways to build and operate military forces tailored to their characteristics.

CHANGES IN CIVILIZATION AND WAR PARADIGM

8. The 4th Industrial Revolution, which first appeared at the 2016 World Economic Forum, is a technological revolution in which fused technologies in three fields, digital, bio, and physics, based on the 3rd industrial revolution called the information revolution, rapidly change the economic system and social structure. It is predicted that the scale, scope, and complexity of the changes caused by this new technological revolution will be completely different from those previously experienced by mankind. In particular, the 4th Industrial Revolution is expected to develop human civilization into a hyper-connected and super-intelligent society. This means that people and things are connected regardless of space and place, and beyond the ability of science and technology to simply calculate better than humans, the intelligence of machines beyond human brains arrives in creativity and general knowledge[4].

9. These new advances in science and technology shift the paradigm of civilization, and further change the war paradigm. The battlefield has expanded from three-dimensional domains of the land, sea, and air to five-dimensional domains including space, cyber/electromagnetic spectrum (EMS), and the development of artificial intelligence (AI) weapon systems is spreading within a hyper-connected network battlefield environment. In the past, combatants centred on human and manned platforms have been transformed into unmanned and autonomous weapon systems such as drones, robots, ultra-precision and supersonic weapon systems, and intelligence, surveillance and reconnaissance (ISR) by satellites and cyber and electronic warfare (CEW) activities are frequent from normal times before armed conflicts[5].

---

[4] World Economic Forum. "The Fourth Industrial Revolution: what it means, how to respond." 2016. Accessed on 17 January 2022 at: The Fourth Industrial Revolution: what it means and how to respond | World Economic Forum (weforum.org)https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.

[5] Seokjoo Doo et al., *Next War and Information Operations*. (Golden Pine Tree, 2017). 1-21.

10. This change in the war paradigm in the era of the 4th Industrial Revolution causes innovative competition over emerging technologies and potential changes in future national power balance, and the success of militarization of the emerging technologies in the future is emerging as a key variable. Recognizing this, countries are scrambling to promote military innovation.

11. For example, the U.S. established the Space Force in 2019 to pre-emptively occupy and strengthen space capabilities, and the U.S. Army established the Army Future Command (AFC) and pursued the U.S. Army future force modernization enterprise (FFME). In this plan, the U.S. Army is striving to have operational capabilities in multiple domains by selecting six priorities - long range precision fires, combat vehicle, network, vertical lift, soldier lethality and air/missile defence. At the same time, nine military science and technologies - disruptive energetics, radio frequency (RF) electronic materials, quantum, hypersonic flight, AI, autonomy, synthetic biology, material by design, and science of additive manufacturing - are selected and conducting prior research to have the ability to overwhelm adversaries in the future operational environment[6]. In addition, the multi-domain task force (MDTF) consisting of aviation, multiple rocket launcher, air defence and I2CEWS – information, intelligence, cyber, electronic warfare, and space/signal - is being formed to conduct combat experiments on what synergy can be created by combining cyber/EMS, space, and information capabilities with other functions and components[7].

12. Japan is pushing for the construction of military forces through the 2019-2023 medium term defence program (MTDP), focusing on cross-domain defence in the land, sea, air, space, and cyber domains and EMS. In other words, Japan is promoting the establishment of cyber defence units, electronic warfare departments, and space specialists to secure capabilities in the multiple domains, as well as the introduction of ballistic missile defence, amphibious maneuverer groups, and F-35B[8].

13. Since 2018, the Republic of Korea (R.O.K.) Army has also been pushing for the Himalaya project to apply and develop advanced science and technology in the military sector in line with this global trend. This is a policy related to the high-tech force to transform into an army that meets the future operational environment. The high-tech force is a concept that maximizes the survival and efficiency of the combatants by applying new technologies of the 4th Industrial Revolution to all combat platforms in the R.O.K. Army, and the overall concept of the research and development (R&D) project is the Himalaya project. The Himalaya project is a project that divides the high-tech R&D field into fourteen categories – nuclear/weapons of mass destruction (WMD), drone/robot, warrior platform, hyper-connected/mobile, modelling, virtual

[6] U.S. Army. "Army Modernization Stratety: Investing in the Future". 2019. 1-12.
[7] Kyle Borne. "Targeting in Multi-Domain Operations." *Military Review*, May-June 2019. 60-67.
[8] The Diplomat. "Japan's Emerging 'Multi-Domain Defense Force'." 2020. Accessed on 18 January 2022 at: Japan's Emerging 'Multi-Domain Defense Force' – The Diplomathttps://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.

environments & simulation (MOVES), advanced sensor, cyber, energy, high-manoeuvre, biomedical/brain science, AI/quantum, intelligent stack processing, materials/stealth, and unmanned vehicle, such as fourteen sites in the Himalayas. And to lead the project, the R.O.K. Army operates the Science and Technology Committee. The committee's fourteen groups in each technology field are composed of military, industry, academia, and research, and play a role in reviewing and developing the Army's technology development, combat power, and combat experiments to develop the future operational concept and requirement in the change of operational environment[9].

14. In this paradigm of a new war in the era of the 4th Industrial Revolution, many countries are establishing new policies and strategies on how to secure and utilize the latest military technologies in pan-domain. Countries lagging in this competition cannot overwhelm adversaries in future operational environments, and the level of national power will fall behind.

THREAT-BASED APPROACH

15. China's rise threatens global security based on international order and is the biggest issue for democratic countries, including the U.S. China has set a goal of fostering world-class forces by the middle of the 21st century and is building the anti-access/area denial (A2/AD) system to compete strategically with the U.S. while striving to strengthen its arms. Currently, the A2/AD strategy and capabilities aim for the concept of multi-domain battlefields, strengthening its ability to destroy the other country's systems in case of a contingency through aggressive enhancement of cyber and space capabilities and strong ballistic missile power[10]. In addition, China emphasizes efforts to secure world-class technologies in core technologies of the 4th Industrial Revolution such as AI, drones, and autonomous systems[11].

16. Russia boldly implemented military and non-military measures to expand its influence through the 2009 Georgia War and the 2014 Ukraine crisis, explicitly expressing its intention to reject the U.S.-centred international order and expand Russia's influence in Ukraine. In the two wars, Russia launched attacks on the other country's government, military networks, and democratic society through covert measures such as offensive cyber operations and information/psychological warfare before overt military intervention. And after that, Russia was able to easily achieve political and strategic goals through overt and conventional military intervention[12].

---

[9] R.O.K. Army. “Army’s Himalaya Project.” 2019. Accessed on 18 January 2022 at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.

[10] U.S. Army Training and Doctrine Command. “The Operational Environment and the Changing Character of Warfare”. 2019. 5-17.

[11] U.S. Chamber of Commerce. “Made in China 2025: Global Ambitious Built on Local Protections”. 2017. 9-17.

[12] Cristopher Chivvis. “Understanding Russian "Hybrid Warfare" And What Can Be Done About it.” RAND Corporation. 2017. 1-7.

17. This means that the dichotomy of war or peace is no longer valid understanding the continuity of dispute, and competition with adversaries in space, cyber/EMS and information domains, which is the previous stage of conventional armed conflict, is important[13].

18. In this context, the importance of space and cyber capabilities is rapidly increasing from the stage of competition before armed conflict, which leads to rapid militarization of space and cyber domains. Great powers, including China and Russia, have already made the great efforts to achieve an edge in competition in space and cyber domains. They are developing a variety of physical/non-physical anti-satellite (ASAT) weapons such as cyber hacking, missiles, jamming, high-power lasers, electromagnetic pulse (EMP), and Kamikaze and kidnapper satellites[14], and apply innovative AI technologies to platforms and software in cyber domain.

19. Based on these capabilities, adversaries will attempt to constantly influence the other party's political leaders, government, military, and people by collecting critical information and using psychological warfare in competition. In transition to armed conflict, considering the capabilities of space, cyber/EMS first, they will attempt to disrupt or deny the other party's key data access by degrading, paralysing, or destroying its command/control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities, which causes serious obstacles to the other party's manoeuvre and defensive/offensive operations since adversaries attempt to paralysis its systems.

20. As a result, capabilities, and operations in cyber, space, and information domains have become more important for the areas beyond the scope of the manoeuvre and projection of conventional military forces from competition. On the contrary, if friendly forces secure superior capabilities to adversaries in space, cyber and information domains, they can create synergy and secures the flexibility through selective multiple options by simultaneously integrating all capabilities in land, sea, air, space and cyber domains, and EMS, not in any single domain. An effective combination of capabilities in multiple domains gives friendly forces flexibility by providing them with various options, while imposing uncertainty and complexity on adversaries, making them unable to respond effectively in multiple domains[15].

21. Capabilities in cyber and space domains are very important in considering multiple options to create an effective combination in pan-domain because it overcomes various limitations in the land, sea and air domains, and has a very significant effect on the employment of land, sea and air assets. Communication satellites, for example, allow effective command and control of all components beyond the limitations of terrain and distance, the global positioning

[13] Canadian Department of National Defence. "Pan-Domain Force Employment Concept: Prevailing in an Uncertain World". 2020. 12, 34-36.
[14] CNN. "War in space: Kamikazes, kidnapper satellites and lasers." 2016. Accessed on 18 January 2022 at: War in space: Kamikazes, kidnapper satellites and lasers | CNN Politicshttps://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.
[15] U.S. Army Training and Doctrine Command. "The U.S. Army in Multi-Domain Operations 2028". 2018. 17-24.

system (GPS) helps to effectively manoeuvre all components, and gives precision to their munitions. Moreover, reconnaissance satellites provide ISR on areas where cannot be observed by land, sea and air assets to improve situational awareness (SA) and target information to project joint fires[16].

22. All modern actors such as nations, government/military, social and private companies always have vulnerability because they live in an open-networked environment. The adversaries' capabilities in cyber domain and EMS can not only target physical components that make up the network, but also non-physical networks and data. Furthermore, it can be effectively operated to achieve cognitively desired effects and goals to audiences in the information domain, which aims to lead political, strategic, and operational situations to advantages.

23. As such, in modern operations, cyber and space/EMS capabilities do not only affect in cyber and space domains, but also play a pivotal role in pan-domain that supports and influences all activities and actions in multiple domains.

CONCLUSION

24. The development of hyper-connected and super-intelligent war paradigms is weakening the boundaries between domains that have been fixed in the past due to mutual overlap and influence across domains, and the dominance in space and cyber domains is very likely to determine the initiative in the future operational environment. As the advanced science and technology of the 4th Industrial Revolution further develops, the hyper-connectivity and intellectualization of the weapon system will intensify, and based on this, the data-based decision-making cycle of observation-orientation-determination-action will be shorter. After all, with the development of the network-centric warfare (NCW), innovation in military forces, especially in space and cyber domains, is an inevitable fate and essential to national security to maximize cross-domain synergy[17] in pan-domain.

25. From the threat-based point of view, efforts are required to develop capabilities in space and cyber domains to obtain the upper position in the era of pan-domain from the competition in response to threats such as adversaries A2/AD, hybrid warfare, and grey zone strategy because space and cyber capabilities that support and influence activities in all domains are essential conditions in order to create the synergy and flexibility against the threats.

26. The multi-territorialisation of the operational domain in modern operations has already become a reality which is an inevitable general trend. There is an opportunity for a state and military to accurately recognize the changes and characteristics of the threats and operational environment, and immediately start various efforts tailored to each country's situation and characteristics to protect its national interest and security in the competition.

---

[16] Alberts Harris. "Preparing for Multi-Domain Warfare: Lessons from Space/Cyber Operations." *Air & Space Power Journal* 32, no. 3 (Fall 2018): 50-53.
[17] U.S. Joint Chiefs of Staff. "Cross-Domain Synergy in Joint Operations Planner's Guide". 2016. 1-5.

BIBLIOGRAPHY

Forbes. “How Kodak Failed.” 2012. Accessed on 17 January 2022 at: How Kodak Failed (forbes.com).

The New York Times. “How the Tech Parade Passed Sony By.” 2012. Accessed on 17 January 2022 at: https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/.

Canadian Department of National Defence. “Strong, Secure, Engaged: Defence Policy.” 2017. 55-57.

World Economic Forum. “The Fourth Industrial Revolution: what it means, how to respond.” 2016. Accessed on 17 January 2022 at: https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.

Doo, Seokjoo *et al., Next War and Information Operations*. (Golden Pine Tree, 2017). 1-21.

U.S. Army. “Army Modernization Strategy: Investing in the Future.” 2019. 1-12.

Kyle Borne. “Targeting in Multi-Domain Operations.” *Military Review*, May-June 2019. 60-67.

The Diplomat. “Japan’s Emerging ‘Multi-Domain Defense Force’.” 2020. Accessed on 18 January 2022 at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.

R.O.K. Army. “Army’s Himalaya Project.” 2019. Accessed on 18 January 2022 at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

U.S. Army Training and Doctrine Command. “The Operational Environment and the Changing Character of Warfare.” 2019. 5-17.

U.S. Chamber of Commerce. “Made in China 2025: Global Ambitious Built on Local Protections.” 2017. 9-17.

Chivvis, Cristopher. “Understanding Russian ‘Hybrid Warfare’ and What Can Be Done About it.” RAND Corporation. 2017. 1-7.

Canada. Department of National Defence. “Pan-Domain Force Employment Concept: Prevailing in an Uncertain World.”. 2020. 12, 34-36.

CNN. “War in space: Kamikazes, kidnapper satellites and lasers.” 2016. Accessed on 18 January 2022 at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-

it-means-and-how-to-respond/https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/?sh=755f4f1d6f27.

U.S. Army Training and Doctrine Command. “The U.S. Army in Multi-Domain Operations 2028.” 2018. 17-24.

Harris, Alberts. "Preparing for Multi-Domain Warfare: Lessons from Space/Cyber Operations." *Air & Space Power Journal* 32, no. 3 (Fall 2018): 50-53.

U.S. Joint Chiefs of Staff. “Cross-Domain Synergy in Joint Operations Planner's Guide”. 2016. 1-5. https://www.army.mil/article/243754/the_u_s_army_in_multi_domain_operations_2028