OF THE THREE ALLIES CANADA, THE UK AND THE US, WHICH NATION'S DEFENCE POLICIES BEST POSITION THE NATION FOR THE FUTURE SECURITY ENVIRONMENT (FSE)?

Maj Mick Bioletti

JCSP 43 DL

Exercise *Solo Flight*

PCEMI 43 AD

Exercice *Solo Flight*

Canada

OF THE THREE ALLIES CANADA, THE UK AND THE US, WHICH NATION'S DEFENCE POLICIES BEST POSITION THE NATION FOR THE FUTURE SECURITY ENVIRONMENT (FSE)?

Maj Mick Bioletti

**OF THE THREE ALLIES CANADA, THE UK AND THE US,
WHICH NATION'S DEFENCE POLICIES BEST POSITION
THE NATION FOR THE FUTURE SECURITY ENVIRONMENT (FSE)?**

INTRODUCTION

One would be hard-pressed to find strategic level defence publications from western nations, which do not present *hybrid warfare* as one of their greatest security challenges. Given that militaries do not necessarily have a good track record for predicting the nature of the next war, the challenge is, therefore, to simultaneously prepare for hybrid and conventional threats. The defence policies of Canada, the UK and the US will be compared for the purpose of determining which of the three allies has been best positioned for the future security environment (FSE). Analysis will commence using an assumption of a FSE marked by hybrid threats, in which the capabilities of cyber, information operations and capacity building will be particularly important to operational effectiveness. The evaluation will then continue taking the assumption of a FSE encompassing conventional threats, in which the application of technological advances will be examined along with complimentary structural and doctrinal changes. Since the US is a superpower, the examples and arguments will be made without consideration to size and focus instead on relative capabilities, innovation, application of technology and both structural and doctrinal design. By presenting examples from recent defence policies, the reader will be led to conclude that the US is the best positioned for both cases of hybrid and conventional warfare, followed by the UK and lastly, by Canada. The discussion will commence by discussing the degree of relevance of hybrid warfare to the FSE.

Is Hybrid War Certain

As illustrated in figure 1, Hybrid warfare is simultaneous employment of conventional weapons, irregular forces, criminal elements, cyber and information operations, to achieve political objectives. Canada's defence policy, "Strong, Secure and Engaged" (SSE), defines a key trend of the changing nature of conflict and draws particular attention to hybrid warfare.[1] The UK's Strategic Defence and Security Review (SDSR) goes further by identifying hybrid tactics as part of six *tier one threats* over the next five years.[2] The US, however, shies away from classifying hybrid warfare as a distinct type of war, and maintains that "traditional and irregular warfare is sufficient to describe the current and future operational environment."[3]
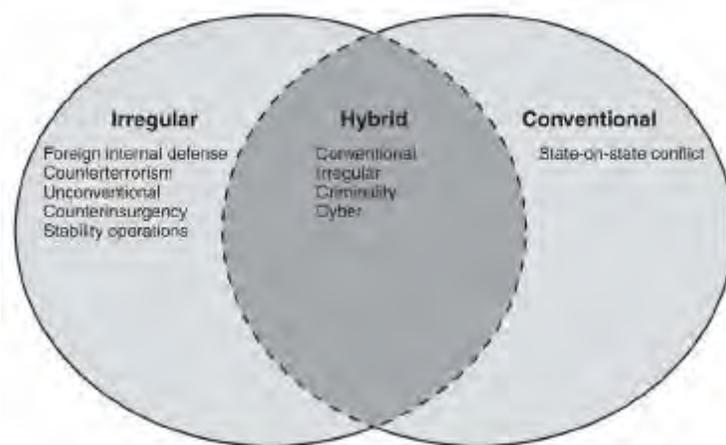
Figure 1 – Hybrid Warfare

Source: US GOA, 2010 Brief on Hybrid Warfare, 16.

---

[1] Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy, (Ottawa: Department of National Defence, 2017), 53.

[2] Ministry of Defence, *National Security Strategy and Strategic Defence and Security Review 2015*, (London: HM Government, 2015), 85.

[3] Government Accountability Office, *Hybrid Warfare - Briefing to the Committee on Armed Services, House of Representatives*, (Washington: U.S. Government Printing Office, 2010), 2. Last accessed 21 May, https://www.gao.gov/assets/100/97053.pdf

It is difficult to determine which one of the three has got it right as to the extent that hybrid warfare will be prevalent in the FSE. Many find it difficult to envision high intensity interstate conventional conflict due to the interconnectedness of international economic systems. Robert Johnson posits that since US conventional capability is so dominant and a nuclear exchange is so unthinkable, future western adversaries will wage irregular or unconventional warfare and therefore, *proxy wars* will be ever more common.[4] Andrew Mumford also states that proxy wars are the "logical replacement for states seeking to further their own strategic goals yet at the same time avoid engaging in direct, costly and bloody warfare."[5] Syria and the Ukraine are often cited as examples of hybrid war, and yet they are also proxy wars. The absence of direct conflict, whether by irregular or conventional forces, between US (or NATO) and Russia, combined with stated political objectives and overt military support, clearly makes them fitting examples of proxy wars. Be that as it may, the task at hand therefore will be to evaluate how well positioned the three allies are for hybrid scenarios. The comparison will now focus on the design of capabilities and structures in cyber operations, information operations and capacity building.

THE HYBRID WAR CASE

Canada's SSE uses the pretext of hybrid war and criminal activities to inform strategic decision making and increase resource allocation to cyber capabilities. Canada is increasing Regular Force personnel by 5.1% in order to invest in cyber, space, intelligence, and health

---

[4] Dr Robert A. Johnson, "Predicting Future War" in *Parameters (The US Army War College Quarterly),* Vol. 44, No. 1, Spring 2014, pp. 71.

[5] Andrew Mumford, "Proxy Warfare and the Future of Conflict" in *The RUSI Journal,* 158:2, 40. Last accessed 21 May 2018, https://www.tandfonline.com/doi/abs/10.1080/03071847.2013.787733

capabilities.[6] Furthermore, Canada will increase investment in research and development in cyber and create full-time capability through part-time service, by designating several reserve units with cyber roles.[7] Much of Canada's capability will be defensive in nature, and the SSE suggests that Canada will develop preventive and offensive cyber capabilities operations from within National Defences' Communications Security Establishment (CSE).[8] The UK SDSR also commits to increase staff by 1,900 in order to respond to and deter "increasing international terrorist, cyber and other global threats."[9] The SDSR outlines an investment of £1.9 billion over five years to protect the UK from cyber-attacks and also provides joint forces with offensive cyber capabilities through the National Offensive Cyber Programme, a partnership between the Ministry of Defence (MOD) and the Government Communications Headquarters (GCHQ). [10] The UK will also invest significantly in non-military departments such as establishing the National Cyber Crime Unit within the National Crime Agency (NCA) and also a new intelligence unit dedicated to tackling the criminal use of the *dark web*.[11] The US raises the status of its cyber capabilities by elevating USCYBERCOM to the status of a full and independent Unified Combatant Command.[12] The secretary of Defense, Jim Matis, intends to seperate the Command from the National Security Agency, a move which will further militarise cyber capabilities. The assistant secretary of homeland defense and global security, Kenneth Rapuano,

---

[6] Ministry of Defence, *National Security Strategy and Strategic Defence and Security Review 2015*, (London: HM Government, 2015), 13.

[7] *Ibid*., 69.

[8] Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy, (Ottawa: Department of National Defence, 2017), 72.

[9] Ministry of Defence, *National Security Strategy and Strategic Defence and Security Review 2015*, (London: HM Government, 2015), 24.

[10] *Ibid*., 41.

[11] *Ibid*., 41.

[12] Jim Garamone and Lisa Ferdinando, *DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command*, (Washington: US Department of Defense, August 2017), 1. Last accessed 21 May 2018, https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/

stated that the move signals US resolve to "embrace the changing nature of warfare and maintain U.S. military superiority across all domains and phases of conflict."[13] CSE and CCHQ are civilian organisations and are very good at conducting cyber activities in isolation, however military commanders will require deeper integration and timely synchronisation of cyber capabilities against adversaries, which themselves integrate cyber, conventional and irregular military capabilities. USCYBERCOM is evolving its structure to be further integrated within the military, and in doing so, capabilities will be more readily synchronised with military operations allowing for greater adaptation and more timely decision making in the event of a FSE marked by hybrid war.

Canada's SSE and UK's SDSR use the backdrop of hybrid warfare to build the case for increased information operations (IO) capabilities, while the US Defense Posture Statement (DPS) 2017 offers little new direction on IO. The SSE states that the reserve force will be used to create full time operational capability through part time service by designating several reserve units to generate and sustain information capabilities.[14] In 2018, the Canadian Army stood up the Canadian Combat Support Brigade (CCSB), which regroups key battle enablers including targeting, intelligence, electronic warfare and IO. The CCSB commands an Influence Activities Task Force (IATF) which will enable Canada to develop IO expertise and specialised capabilities.[15] The UK's SDSR announced the establishment of a Counter Hybrid Warfare formation, 77th Brigade, which specialises in IO and institutional development. [16] The UK

[13] *Ibid.*, 1.
[14] Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy, (Ottawa: Department of National Defence, 2017), 68.
[15] The Canadian Army, "Canadian Combat Support Brigade," last accessed 21 May 2018, http://www.army.forces.gc.ca/en/5-canadian-division/canadian-combat-support-brigade/index.page
[16] Ministry of Defence, *National Security Strategy and Strategic Defence and Security Review 2015*, (London: HM Government, 2015), 28.

created 77th Brigade with 440 personnel including a mix of reserve and regular force.[17] The US

Army has a similar approach with the 1st IO Command, which is a formation based on two

regular force battalions supported by reserve personnel.[18] In the US model, each command has

an IO component supported by the Joint Information Operations Warfare Center (JIOWC).[19]

This is an element missing from the UK and Canadian models, since although both SSE and

SDSR speak about information operations in terms of joint capability, their IO structures are

very much land centric. Overall, the UK is best positioning IO capabilities to meet the hybrid

threat followed by Canada and the US.

Canada has less specialised capacity building than the US and UK, which have both

recently rerolled former conventional units into security sector reform and capacity building.

UK's SDSR outlined major changes to defence engagement. Firstly, defence engagement

became a core Defence task, meaning that it will be adequately funded as a priority. Secondly,

new regional British Defence Staffs for defence engagement are established in the Gulf, Asia

Pacific and West Africa, and lastly, four light infantry battalions are rerolled as capacity building

battalions.[20] The US has also designed a specialisation in capacity building, by rerolling two

infantry brigades as Security Force Assistance Brigades (SFAB), with another three planned. The

1st SFAB, with its six battalions, commenced operations in Afghanistan in March 2018.[21]

---

[17] The British Army, "77th Brigade – Influence and Outreach," last accessed 21 May 2018, https://www.army.mod.uk/who-we-are/formations-divisions-brigades/77-brigade/

[18] The US Army, "1st Information Operations Command (Land)", last accessed 21 May 2018, http://www.1stiocmd.army.mil/Home/brigadestaff

[19] Department of Defense, *Joint Publication 3-13: Information Operations*, (Washington: Joint Chief of Staff, 2014), III-2.

[20] Ministry of Defence, *Defence engagement and national resilience*, (London: Parliament Publications and Records, 2015), last accessed 21 May 2018, https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/108/10807.htm

[21] Maj. Matthew Fontaine, *1st SFAB uncases colors, begins train, advise, assist mission in Afghanistan*, (Fort Eustis: Tradoc News Center, 2018), last accessed 21 May 2018, http://tradocnews.org/tag/1st-security-force-assistance-brigade/

Canada's SSE acknowledges the important history of capacity building, however avoids specialisation and presents no indication of force structure design. This resistance to design is in the face of ongoing capacity building missions in Afghanistan, Iraq, Niger, and the Ukraine. Both the US and the UK are relatively better positioned than Canada to conduct capacity building in the event of a hybrid war, due to the design of specialised capabilities through structural changes.

After examining capabilities and structures in cyber, IO and capacity building the US has been found to be the best positioned to face hybrid threats. The US upgraded the status of its cyber command and is moving to further integrate civilian cyber capabilities within the military, it has a Joint Information Operations Warfare Center and it has designed and deployed specialised capacity building organisations. The UK comes in second, by having increased cyber capabilities, particularly within the home office, by designing specialised IO structures for hybrid war and by designing specialised capacity building organisations and increasing defence engagement. Canada is improving capabilities mostly within CSE without significant changes to organisational structure and also continuing capacity building operations without any design for specialisation. IO is a source of encouragement for Canada due to its design approach in creating new full time capabilities through part time service and the creation of the IATF structure.

THE CONVENTIONAL WAR CASE

David Kilcullen used the analogy of *dragons* (states) and *snakes* (Non State Actors) to describe how after the cold war western militaries turned their attention from dragons to snakes. In irregular and hybrid conflicts, nations will continue to face the threat of snakes, however as

David Kilcullen cautions us, the dragons are coming back.[22] More importantly, the dragons have watched from the sidelines as the west fought prolonged wars against snakes. Dragons have observed how the west leveraged technology and the combined arms approach, while also noting the best practices of snakes' irregular tactics. Russia, China, Iran and North Korea should not be expected to fight with obsolete dragon techniques, as the Iraqi military did in the first Gulf War, since they are adapting their tactics, capabilities and structures. For some perspective, consider how the transformed Russian motorised brigade groups now employ a combined arms approach with integral assets that the west often allocates to divisions or corps.

The new Russian Brigades groups will be based on the leading edge Armata platform of T-14 tanks and Infantry Fighting Vehicles (IFV) (currently in field trials), supported by heavy artillery, roughly equivalent to a western regiment, two assault bridges, three mechanised bridges, a company of Spetsnaz, as well as air defence (AD), electromagnetic pulse systems and electronic warfare assets usually found at western divisions.[23] Russia's modernisation of capabilities, structures and tactics compliments its numerical superiority. Russia announced that up to 6000 stocked soviet era T80 tanks will be reactivated and modernised. [24] A silver lining is that this tank modernisation project is likely the result of production delays for Armata T-14, which could potentially limit Russia's numerical and technological advantage in tanks for the next five years. Nevertheless, Russia is moving forward with drastic increases in SOF and assault

---

[22] David Kilcullen, *The Dragon and the Snakes: Emerging and Future Security Threats in the Post-Cold War Order*, (London: Royal United Services Institute (RUSI), 2016), 5.

[23] Dr Igor Sutyagin, *Land Warfare Conference 2017 – Session 7*, (London: RUSI Conference, 2017), Last accessed 21 May 2018, https://www.youtube.com/watch?v=_EcrrD1dBhg

[24] Dr Igor Sutyagin, Russian Appreciation of Security in Europe: Background and "Zapad-2017"in the *Air and Missile Defence Conference*, (Hamburg: RUSI, 26 September 2017), 20. Last accessed 21 May 2018, https://www.ccsbamd.org/competence-centre/wp-content/uploads/2017/10/109_RUSI.pdf

pioneer capability and production of new anti- access and area denial (A2/AD) platforms such as the S400V4s.[25]

Given that Dragons such as Russia, China, Iran, North Korea are modernising equipment and increasing the span of their areas of influence, it is necessary to reflect on how well western nations are preparing for conventional warfare, whether through proxy or interstate conflict. In order to analyse how well Canada, the UK and the US are designing capabilities and structures to face conventional threats, it is helpful to review some theory on the future of conventional warfare.

Thomas Donnelly posited that the end of the cold war, combined with the long series of small wars in the 1990s and 2000s, led to reduced research and development for conventional capabilities. He added that "failure to build and field in important numbers the weapons designs of the 1990s has all but deprived US forces of conventional-force superiority."[26] Proliferation of fielded applied technology has diffused western military power and several emerging disruptive technological applications are in experimentation. These disruptive technologies include autonomous robotic systems, drones, anti-satellite weapons, active protection systems (APS), smart missiles and torpedoes, and advanced manufacturing, to name a few. When Harry S. Truman said that *the size of the Army matters but it is the technology that wins war*, he was only half right. The tactics employed by militaries and structures used to optimise the application of capabilities are essential to winning wars. In the book *War and Technology,* Jeremy Black reasoned that *synergy* is imperative, saying that:

[25] Richard Connolly and Mathieu Boulègue, *Russia's New State Armament Programme Implications for the Russian Armed Forces and Military Capabilities to 2027*, (London: Chatham House, 2018), 23. Last accessed 21 May 2018, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf

[26] Thomas Donnelly, "You Say You Want a Revolution?", in *Strategika - New Military Technologies* Issue 39, March 2017, 1. Last accessed 21 May 2018, https://www.hoover.org/research/you-say-you-want-revolution-2

synergy suggests that, in any future conflict, success will hinge on the ability to

achieve a successful combination of land, air, sea, cyber, and space forces, an

ability that requires the development of new organizational structures.[27]

The comparison of the three allies will now resume, commencing with a review of equipment modernisation and the application of new technologies followed by an examination of synergies created through structural and doctrinal changes.

Modernisation and Application of Technology

Canada's SSE confirms funding for the modernisation of the Army's light armoured vehicles, the replacement of support vehicles and the acquisition of air defence, anti-tank weapons and bridging equipment.[28] The CAF will replace the outdated fleet of CF-18, invest in medium altitude remotely piloted aircraft and modernise maritime patrol aircraft. Canada will also invest in the Royal Canadian Navy's ability to meet evolving undersea threats and acquire 15 Canadian Surface Combatants.[29] Canada will also increase warfighting capability against conventional threats by increasing SOF personnel by 605.[30] With the notable exception of investment in SOF capabilities and in countering emerging undersea threats, most of the investments identified in SSE address existing critical gaps in warfighting capabilities. As such, SSE conveys a message of modernising to catch up, rather than innovating to achieve and sustain competitive advantage.

---

[27] Jeremy Black, "Into the Future", in *War and Technology*, (Bloomington: Indiana University Press, 2013), 247.

[28] Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy, (Ottawa: Department of National Defence Canada, 2017), 36.

[29] *Ibid.*, 102.

[30] *Ibid.*, 109.

The UK's SDSR confirms investments in new platforms such as the Ajax (tracked light armour platform with first squadron to be operational in 2019) and continued investment in fourth plus and fifth generation aircraft, including 160 Typhoons, 135 F-35 and 20 new Protectors (armed remotely piloted aircraft).[31] The national shipbuilding strategy, published in 2017, ensures that the Royal Navy will remain a technologically advanced world class navy. Investments include two Queen Elizabeth Class carriers (2018), at least five Type 31 Frigates (2023), eight Type 26 Global Combat Ships (2026), as well as four next generation Dreadnought Class submarines, (2028).[32] The UK will balance current operations with the ability to modernise and improve its equipment since the SDSR committed 20% of defence budgets to research, development and procurement.[33]

The US Department of Defense (DOD) Posture Statement (DPS) 2017 outlines major investments in existing capabilities but also in emerging capabilities. Investments in existing land capabilities include next-generation shoulder-launched weapons, a life extension program as well as a replacement for the Army Tactical Missile System (ATACMS), increased firepower for Stryker armoured vehicles, and 327 new Apache AH-64E.[34] In response to emerging A2/AD threats, ground based interceptors (GBI) missile defence and terminal High-Altitude Area Defense (THAAD) systems are receiving funding increases. The Airforce is introducing new variants of the fifth generation F-35 and investing in Unmanned Carrier-Launched Air Surveillance and Strike (UCLASS), program thereby "setting the stage for a future unmanned

---

[31] Ministry of Defence, *National Security Strategy and Strategic Defence and Security Review 2015*, (London: HM Government, 2015), 31.
[32] *Ibid*., 24.
[33] *Ibid*., 27.
[34] Department of Defense, *2017 Defense Posture Statement: Taking the Long View, Investing for the Future*, (Washington: Department of Defence, 2017), 34.

carrier air wing."[35] The navy's fleet will grow from 280 ships to 308 over five years (FYDP) and make considerable investments in the undersea battlespace. This includes nine new attack submarines, P8-A Poseidon anti-submarine maritime patrol aircraft and unmanned undersea vehicles (UUV).[36]

The defence policies of Canada, the UK and the US have all stated the need for modernisation and outlined investments in order to address concerns. Canada addresses existing gaps in conventional warfighting capability, while the UK improves platforms to ensure technological relevance. The US is the most innovative of the three, not only improving existing platforms, but also innovating and applying new technologies to generate new capabilities.

Despite the significant investment announced in the DPS, the US Army's Training and Doctrine Command (TRADOC) G2 writes that even the US "may find itself with the very real potential of being out-gunned, out-ranged, out-protected, outdated, out of position, and out of balance against adversaries."[37] This is not just due to the proliferation and convergence of technology but also due to the ability of adversaries to adapt and "present an array of threats that will be lethal and will be presented across multiple domains."[38] Canada's Chief of Force Development acknowledges that "proper consideration and integration of science and technology into overall capabilities has often proven more important than having the most advanced equipment."[39] It is now fitting to examine the complimentary structural and doctrinal changes which will be necessary to create synergies and prepare forces for conventional threats.

---

[35] *Ibid.*, 37.
[36] *Ibid.*, 33.
[37] TRADOC G-2, *The Operational Environment and the Changing Character of Future Warfare*, (Fort Eustis: Army Capabilities Integration Center, 2017), 4.
[38] *Ibid.*, 5.
[39] Department of National Defence Canada, *The Future Security Environment 2013-2040*, (Ottawa: Chief of Force Development, 2014), 64.

Changes to Structure and Doctrine

Canada's SSE announces very little in terms of structural and doctrinal changes aside from the previously mentioned creation of full time capability through part time service. Fortunately, Canada already has an integrated joint command structure since 2012, in the form of the Canadian Joint Operations Command (CJOC) and the deployable 1st Canadian Division Headquarters. There are several important warfighting capabilities such as CSE cyber capabilities, CANSOFCOM SOF capabilities, and CFINTCOM capabilities which are not normally employed by CJOC. Further structural and doctrinal changes are required in order to better integrate Canada's joint capabilities for conventional near-peer threats in the FSE.

The UK's SDSR announced the return to a deployable heavy division and two strike brigades rather than five independent brigades. It also confirmed the validity of the joint force command structure that was established in 2012. Joint Force Command encompasses cyber, SOF, space, special reconnaissance, communications, intelligence and medical capabilities along with permanent and deployable joint headquarters. [40] Canada's first commander of CJOC, LGen (Ret'd) Stuart Beare, wrote that the "UK had invested in joint capabilities, structure and leadership to drive integration and joint behaviour across the Force" which created an enhanced joint culture.[41] Doctrinally, SDSR announced an investment in a ground-based ballistic missile defence (BMD) radar which will integrate Type 45 Destroyers to create a joint BMD capability.[42]

---

[40] United Kingdom, Ministry Of Defence, "*Joint Forces Command - About Us*" last accessed 26 May 2018, https://www.gov.uk/government/organisations/joint-forces-command/about

[41] LGen (Ret'd) Stuart Beare, Championing the Joint Force: A Job for the Public and Our Political Leaders – Not Just Military Professionals Alone, (Calgary: Canadian Global Affairs Institute, November 2015), 7.

[42] Ministry of Defence, *National Security Strategy and Strategic Defence and Security Review 2015*, (London: HM Government UK, 2015), 25.

The US DPS makes significant investments to expand war gaming efforts which will allow the US to experiment with nascent operational concepts and test new capabilities. The results of future wargames will be integrated into DoD's new war gaming repository and inform doctrinal changes.[43] The US is currently evolving doctrine to position itself for the Multi-Domain Battle (MDB). In May 2016, the Commander of US Pacific Command, Admiral Harry Harris, told pacific army leaders that land forces must "be able to sink ships, neutralize satellites, shoot down missiles, and damage the enemy's C2" and that the US "needs systems that enable the Army to project power over water, from shore."[44] In February 2018, Admiral Harris told the House Armed Service Committee that Pacific Command was progressing from experimentation to validation of concepts, and the Army's new Multi-Domain Task Force would be validated during the RIMPAC 20 exercise.[45] Structural improvements include the aforementioned changes in Cyber Command and the establishment of the Joint Interagency Combined Space Operations Center (JICSpOC), which will better align joint operations in space across the U.S. government.[46]

CONCLUSION

The comparison of the defence policies of Canada, the UK and the US has revealed that the US is the best positioned for the FSE since it has aggressively designed capabilities,

---

[43] Department of Defense, *2017 Defense Posture Statement: Taking the Long View, Investing for the Future*, (Washington: Department of Defence, 2017), 27.

[44] Admiral Harry B. Harris, *LANPAC Symposium 2016: Role of Land Forces In Ensuring Access To Shared Domains*, (Waikiki: Institute of Land Warfare, 25 May 2016), 1. Last accessed 25 May 2018, http://www.pacom.mil/Media/Speeches-Testimony/Article/781889/lanpac-symposium-2016-role-of-land-forces-in-ensuring-access-to-shared-domains/

[45] Admiral Harry B. Harris, *Statement Before the House Armed Services Committee*, (Washington: http://docs.house.gov/meetings/AS/AS00/20180214/106847/HHRG-115-AS00-Wstate-HarrisJrH-20180214.pdf

[46] Department of Defense, *2017 Defense Posture Statement: Taking the Long View, Investing for the Future*, (Washington: Department of Defence, 2017), 39.

advanced platforms, structures and doctrine. The UK has demonstrated innovation in designing structures and capabilities for hybrid threats while ensuring technological relevance in conventional capabilities through consistent levels of investment and optimising joint command structures. In the case of hybrid war, Canada has improved IO but lacks specialisation in capacity building and faces organisational friction in integrating CSE cyber capabilities for military operations. In the case of conventional warfare, Canada is not a technological leader, has existing gaps in critical warfighting capabilities and has yet to shape full integration of its emerging joint capabilities. The optimistic reader can find hope in the fact that Canada collaborates very closely with the UK and the US and further study of allied capabilities, structures and doctrine will likely inform Canada's future policy decisions, which should better prepare Canada for the FSE.

BIBLIOGRAPHY

Bartels, Clay; Tormey, Tim; Hendrickson, Jon. "Multi-domain Operations and Close Air Support: A Fresh Perspective" in Military Review. Fort Leavenworth, Mar/Apr 2017.

Beare, LGen (Ret'd) Stuart. Championing the Joint Force: A Job for the Public and Our Political Leaders – Not Just Military Professionals Alone. Calgary: Canadian Global Affairs Institute, November 2015.

Black, Jeremy. "Into the Future." Chapter 7 in War and Technology. Bloomington: Indiana University Press, 2013.

Canada. Canadian Army. "Canadian Combat Support Brigade." Last accessed 21 May 2018, http://www.army.forces.gc.ca/en/5-canadian-division/canadian-combat-support-brigade/index.page

Canada. Department of National Defence. Defence Acquisition Guide 2016. Ottawa: Department of National Defence, 2016. Last accessed 17 March 2018. http://www.forces.gc.ca/en/business-defence-acquisition-guide-2016/joint-and-other-systems-405.page

Canada. Department of National Defence. Strong, Secure, Engaged: Canada's Defence Policy. Ottawa: Department of National Defence, 2017.

Canada. Department of National Defence. The Future Security Environment 2013-2040. Ottawa: Chief of Force Development, 2014.

Canada. Government of Canada. Foreign Cyber Operations. Ottawa: Communications Security Establishment, June 2017. Last accessed 17 March 2018. https://www.cse-cst.gc.ca/en/cse-act-loi-cst/cyberop

Connolly, Richard and Mathieu Boulègue. Russia's New State Armament Programme Implications for the Russian Armed Forces and Military Capabilities to 2027. London: Chatham House, 2018. Last accessed 21 May 2018, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf

Donnelly, Thomas. "You Say You Want a Revolution?", in Strategika - New Military Technologies Issue 39, March 2017. Last accessed 21 May 2018, https://www.hoover.org/research/you-say-you-want-revolution-2

Fontaine, Maj. Matthew. 1st SFAB uncases colors, begins train, advise, assist mission in Afghanistan. Fort Eustis: Tradoc News Center, 2018. Last accessed 21 May 2018, http://tradocnews.org/tag/1st-security-force-assistance-brigade/

Freier, Nathan and Berteau, David. "Beyond the Last War - Balancing Ground Forces and Future Challenges Risk" in USCENTCOM and USPACOM. Washington: Centre For Strategic & International Studies (CSIS), April 2013.

Garamone, Jim and Lisa Ferdinando. DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command. Washington: US Department of Defense, August 2017. Last accessed 21 May 2018, https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/

Harris, Admiral Harry B. LANPAC Symposium 2016: Role of Land Forces In Ensuring Access To Shared Domains. Waikiki: Institute of Land Warfare, 25 May 2016. Last accessed 25 May 2018, http://www.pacom.mil/Media/Speeches-Testimony/Article/781889/lanpac-symposium-2016-role-of-land-forces-in-ensuring-access-to-shared-domains/

Harris, Admiral Harry B. Speech to the House Armed Services Committee on U.S. PACOM Posture. Washington: DoD, 14 February 2018. Last Accessed 18 March 2018. http://docs.house.gov/meetings/AS/AS00/20180214/106847/HHRG-115-AS00-Wstate-HarrisJrH-20180214.pdf

Johnson, Dr Robert A. "Predicting Future War" in Parameters - The US Army War College Quarterly. Vol. 44, No. 1, Spring 2014.

Kilcullen, David. The Dragon and the Snakes: Emerging and Future Security Threats in the Post-Cold War Order. London: Royal United Services Institute (RUSI), 2016.

Mumford, Andrew. "Proxy Warfare and the Future of Conflict" in The RUSI Journal, 158:2. Last accessed 21 May 2018, https://www.tandfonline.com/doi/abs/10.1080/03071847.2013.787733

Sutyagin, Dr Igor. Land Warfare Conference 2017 – Session 7. London: RUSI Conference, 2017. Last accessed 21 May 2018, https://www.youtube.com/watch?v=_EcrrD1dBhg

Sutyagin, Dr Igor. "Russian Appreciation of Security in Europe: Background and Zapad-2017" in the Air and Missile Defence Conference. Hamburg: RUSI, 26 September 2017. Last accessed 21 May 2018, https://www.ccsbamd.org/competence-centre/wp-content/uploads/2017/10/109_RUSI.pdf

Trenin, Dmitri. Avoiding US-Russia Military Escalation During the Hybrid War. Washington: Carnegie Endowment for International Peace, January 2018.

United Kingdom. British Army. "77th Brigade – Influence and Outreach." Last accessed 21 May 2018, https://www.army.mod.uk/who-we-are/formations-divisions-brigades/77-brigade/

United Kingdom. Cabinet Office. National Security Strategy and Strategic Defence and Security Review 2015. London: HM Government, 2015.

United Kingdom. Ministry of Defence. Defence engagement and national resilience. London: Parliament Publications and Records, 2015. Last accessed 21 May 2018, https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/108/10807.htm

United Kingdom. Ministry of Defence. "Joint Forces Command - About Us." Last accessed 17 March 2018. https://www.gov.uk/government/organisations/joint-forces-command/about

United States. Department of Defense. 2017 Defense Posture Statement: Taking the Long View, Investing for the Future. Washington: Department of Defence, 2017.

United States. Department of Defense. Joint Publication 3-13: Information Operations. Washington: Joint Chief of Staff, 2014.

United States. Joint Chief Staff. Joint Operating Environment (JOE) 2035: The Joint Force in a Contested and Disordered World. Washington: DOD, 14 July 2016.

United States. Joint Force Development (J7). Cross-Domain Synergy in Joint Operations. Washington: DoD, 14 January 2016.

United States. Secretary of Defense. Quadrennial Defense Review 2014. Washington: Department of Defense, 2014.

United States. US Army. "1st Information Operations Command (Land)." Last accessed 21 May 2018, http://www.1stiocmd.army.mil/Home/brigadestaff

United States. US Army Training and Doctrine Command. Combat Vehicle Modernisation Strategy. Fort Eutis: Army Capabilities Integration Center, 15 September 2015.

United States. US Army Training and Doctrine Command. MultiDomain Battle: Evolution of Combined Arms for the 21st Century. Fort Eustis: Army Capabilities Integration Center. 7 October 2017). Last Accessed 17 March 2018. https://www.youtube.com/watch?v=nfOgPayfATo

United States. US Army Training and Doctrine Command G-2. The Operational Environment and the Changing Character of Future Warfare. Fort Eustis: Army Capabilities Integration Center, 2017.