Cyber-Enabled Influence Operations

Suzanne Waldman	Susan Watson	Natalie Nakhla	Farid Pesteh
DRDC	*DRDC*	*DRDC*	*DRDC*
suzanne.waldman@gc.forces.ca	*susan.watson@forces.gc.ca*	natalie.nakhla@forces.gc.ca	faridoddin.pesteh@forces.gc.ca

Abstract

The domain of Psychological Operations, otherwise known as Influence Operations, is now transacted almost wholly in cyberspace: that is into networks of online media, social media and other web applications [1]. Basic online influence operations in cyberspace, going back to the mid-2000s, consist of using online applications in a deceptive way--for example creating social media accounts that appear to belong to real, relatable and/or credible individuals, and using them to circulate persuasive content among online social networks [2].

Increasingly, adversarial online influence operations are additionally leveraging cyber-capabilities to push influence operations beyond the limits of what they can achieve using the customary affordances of social media platforms [3]. Cyber capabilities can provide botnets capable of introducing or amplifying social media content on a larger scale and/or at a faster rate than human operators can do [4]. Generative AI can likewise significantly reduce the requirements and expand the reach of Psychological Operations by automating and streamlining the process [5][6].

There is a case for the tactical use of cyber-enabled influence operations targeting adversaries in named military operations. Yet facilitating joint cyber-influence activities raises distinctive challenges for Allied militaries, which typically house cyber and influence capabilities in separate institutions and attributed with different degrees of status [7]. This paper first looks at the tactics, techniques, and procedures (TTPs) of recent major Influence Operation campaigns—in general and then in particular--to establish the degree to which they are already being enabled by cyber capabilities. It subsequently looks at some examples of doctrine to elicit some obstacles for allied militaries to create competitive joint cyber-influence functions and provides some recommendations.

1 Cyber-Enabled Influence Operations - a Military Problem

1.1 What makes a cyber-enabled influence operation?

In influence operations, the objective is to affect people's attitudes, beliefs and behaviour. Cyber capabilities, in turn, are intended to create effects in cyberspace by taking advantage of flaws or weaknesses in software or hardware systems, altering these systems to achieve objectives, such as obtaining root access to a computer system and exfiltrating data [8]. In keeping with conventional understanding of the Information Environment as a series of layers, the use of cyber capabilities used for influence directs cyber capabilities in the virtual domain towards affecting human audiences in the cognitive domain [9].

For example, some cyber-enabled influence operations use offensive cyber techniques to access, modify, manipulate or expose information to support desired narratives. Other cyber-enabled influence operations use social media and online platforms in an automated way, generating fake personas, synthetic content, and artificial networks to bolster messaging.

We consider all these techniques as deploying cyber capabilities with an influence effect. Drawing on technical skills that are likely to be housed in cyber-capabilities amidst contemporarily militaries, they go beyond the more straightforward activity of 'executing influence operations in cyberspace,' which an influence operator can do simply using a social media or web-site construction platform in an authorized, albeit deceptive way.

1.2 Process of Undertaking Cyber-Enabled Influence Activities

Existing research on the underlying process (or "kill chain") of cyber-enabled information operations indicates that these operations typically involve four phases; these phases are, however, somewhat interchangeable and reiterative in sequence and do not map onto a traditional cyber kill chain [10][11][12]. These phases are rooted in basic PSYOPS planning, but also integrate cyber capabilities for sophisticated technical operations on potentially lengthier timelines.

- The first phase is *Planning*, where reconnaissance is undertaken to find issues or tensions that can

be exploited in the influence campaign. For instance, Internet Research Agency's (IRA) tactics during the 2016 U.S. elections involved polarizing the U.S. public around key wedge issues (e.g. racial tensions, LGBTQ+ rights, gun rights, etc.), knowledge of which required an in-depth understanding of the U.S. social milieu [13].

- Planning is followed by a *Preparation* stage, where the infrastructure and online assets are acquired and set up to carry out their operations, and cyber capabilities are brought to bear. Setting up online assets can be sped up by creating botnets that can become "followers" of a sock-puppet account, as a means of increasing the account's legitimacy. Using Generative AI, threat actors can create legitimate-looking news websites or Twitter posts at a fraction of the cost. Any cyber capability used for influence is directed towards a human audience--though sometimes indirectly, as is the case with deterrence activities in cyberspace. We say that influence effects achieved using online tools or social media platforms are effects delivered "via cyberspace" rather than in cyberspace.
- Next comes a *Targeting* stage, where audiences are studied to learn how narratives can be tailored to them, thus making them more susceptible to messaging. Audiences can also be segmented into various sub-groups who are presented with different narratives.
- Having identified key issues and key audiences, the *Execution* stage begins where content is created to engage a target audience and is delivered as surgically and stealthily as possible. Cyber capabilities involved in Execution can include attribution management to evade detection and geo-fencing of target IP addresses to focus targeting efforts and evade wider detection.
- Operators can then undertake an *Amplification* and *Supporting* phase. Amplification can potentially leverage cyber-capabilities such as botnets that engage in coordinated inauthentic behaviour. Supporting the operation can entail commenting on others' posts, engaging in trolling behavior, or stirring up polarized conversations. The Amplification and Supporting phase is where the automation of traditional IO tactics allows a campaign to fully scale up its reach and impact.
- Finally, continuous *Assessment* is required of which aspects of the operation are successful and which are not. Based on the results of this iterative process, additional resources can be put into the former.

Notably, Cyber-enabled influence kill chains tend to be "modular", with operators initiating multiple phases simultaneously, or following the kill chain in different orders [14]. For example, while assessment is often depicted as the last phase of an operation, operators can engage in A/B testing during their execution phase and modify content based on reactions from their targeted audience. This iterative process, combined with cyber-enabled tactics, allows for reductions in costs and delays, evasion of detection, and saturation of targeted social networks with desired narratives.

2 Cyber-Influence Operations - Examples

We studied several examples from a list of publicly available cyber incidents that occurred between 2022 and 2024 [15]. Our goal is to better understand and taxonomize the concept of cyber-enabled influence.

- The most infamous case is the interference by the Internet Research Agency (IRA) in the 2016 U.S. elections using Facebook, Twitter, Instagram, and YouTube to misinform and polarize users. This campaign relied on three broad cyber tactics: hacks of online voting systems, hacks of DNC databases that led to leaks of Hilary Clinton's email, and launching a DDOS attack on the online voting platforms [13]. Influence effects included amplifying polarizing narratives, sowing divisions between groups, spreading disinformation, and suppressing voting in specific demographics [16]
- The CCP's Spamouflage campaign (also known as Dragonbridge and Spamouflage Dragon), active since 2017, which targets North American audiences with narratives to undermine the legitimacy of democratic institutions and politicians and to sow public divisions. The campaign now uses generative AI botnets to generate and botnets to widely amplify seemingly organic content aligned with the CCP's strategic narratives across social media platforms [17][18]. For example, in August 2023, presumed proxies of the PRC used generative AI to amplify misleading information on WeChat about a Canadian politician who had taken positions adverse to the PRC [19].
- Russia's "Doppelganger" activities – beginning in the summer of 2022 – to spread disinformation

using Gen-AI to create clones of reputable European news sources and publish pro-Kremlin narratives and stories and amplify hybrid operations. This campaign also used troll accounts and sock puppets (fake social media accounts) to place content on comment section of established Facebook pages that included spoofed news links; fake accounts (likely bot networks) on X/Twitter, to share, re-tweet, and reply to Tweets; Facebook adware to segment audiences based on demographics and interests and push targeted stories; obfuscation techniques such as geofencing content based on users' IP address to evade detection; and multiple redirection URLs to circumvent social media platform restrictions on certain domain names [20].

- In March 2023, Russian hackers targeted US and European politicians who denounced Russia's invasion of Ukraine to participate in phone and video calls, giving them misleading prompts to provide pro-Russia soundbites. They then published these clips to discredit previous statements [15].
- In December 2023, Russian hackers disabled the access of 24 million Ukranian customers to Kyivstar, Ukraine's largest mobile phone provider, and destroyed more than 14,000 computers and servers, hours before President Zelensky met with President Biden [21].
- In April 2024, Ukraine's military intelligence agency launched a flood of DDoS against the United Russia party's servers and domains, rendering them inaccessible on the same day that Russia was hosting a patriotic online initiative [15].
- In January 2024, before Taiwan's general election, the "Dragonbridge" campaign linked with the PRC circulated AI-synthesized audio recordings of a false history of Taiwan's outgoing President via thousands of Youtube accounts registered to AI-generated avatars and populated with fake comments. [22]

2.1 Discussion of Examples

The preceding cases of cyber-enabled influence campaigns show how cyber-techniques have been employed by a variety of actors to achieve strategic influence effects and advance influence objectives. The incidents reviewed can be broadly categorized into two rough groups:

- Social engineering campaigns, impersonation and infiltration [6] campaigns enabled with generative AI, bots, trolls and other automated systems, intended to negatively impact victims and influence audiences [7]. In the case of the social engineering campaigns, the cyber-enabled influence nexus is overt.
- DDoS, ransomware, and other cyber-attacks against government/party websites and critical infrastructure, apparently intended to influence populations and strategic actors [15]. It is impossible to know the intent of these examples in every example, but many of them evidently had objectives to create influence effects. Some of these cyber incidents were clearly in response to or prior to significant events [4][5]. Others seemed carefully timed to create influence effects of warning, deterring, fearmongering, and destabilizing the target.

Table 2 provides additional detail on how specific cyber techniques can be used to enable specific influence effects. Considered at a high level, the cyber techniques employed were interruption, modification, degradation, fabrication, automation, interception and obfuscation techniques, as seen in Column 2 [3] [8]. Each of cyber-these techniques were in turn exploited to achieve a range of influence effects, as can be seen in Column 3.

Cyber Tactics used in Recent Cyber-Enabled Influence-Operations	**Cyber Technique**	**Influence**
Creating "newsbots" that automate sharing of fake news (RU)	Automation	Amplification
Disabling customer access to cell network (RU)	Denial of Service Attack	Intimidation, obstruction of communication
Denial of service attack on government websites (UKR)	Denial of Service Attack	Demoralization, obstruction of information
Multiplying Top-Level Domains (RU)	Fabrication	Masking, Infiltration
Botnetting new/ hijacked accounts to amplify disinfomation (PRC)	Fabrication	Amplification

GAN-generated personas (PRC)	Fabrication	Deception
AI-synthesized voice recording (PRC)	Fabrication	Deception
Cyber Espionage and data leaking [1]. (RU)	Infiltration	Discrediting
Creation or cloning/ of seemingly legitimate websites (RU)	Manipulation	Infiltration
IP address and phone carrier location masking (RU)	Obfuscation (of Identity)	Masking
Registration of accounts in areas of interest through proxy services (RU)	Obfuscation	OpSec
Geo-fencing content (RU)	Obfuscation (of Location)	Masking
Rotating hosting services (RU)	Obfuscation	Masking
Websites hosted on reverse proxy infrastructure (RU)	Obfuscation	Masking, Infiltration
Multiple redirection URLs (RU)	Obfuscation	Masking

Table 1 – Cybertechniques Used and their Influence Effects

3 Challenges Integrating Cyber and Influence Capabilities in the West

The above examples are meant to illustrate the technical range of influence operations conducted by all actors today. Evidently from the examples described and taxonomized above, adversaries are clearly innovating automated ways to accelerate and speed up their influence operations.

For Western militaries conducting military operations, there may be opportunities to have their own toolkit of cyber capabilities to enhance their influence operations [23]. To this point, however, it has been assessed that "technology's role in the cognitive and information space is one of the largest gaps ... between adversaries and our (i.e. the US's) partners" [24].

One obvious challenge for Western governments is legal and normative. For authoritarian governments acting in the cognitive space, "the only rule is that there are no rules" [25]. In contrast, laws and norms inhibit allied militaries from experimenting and developing the same level of efficacy in cyberspace. Allied military practices demand that all operations—including influence operations—be surgically targeted at approved audiences, as well as risk-managed so they do not create unproportionate harms [26]. Allied militaries are also prohibited from practicing influence in a way that might impact their own citizenships [27], although separating domestic from foreign audiences may be near to impossible to assure when acting on transnational social media platforms.

Further, given difficulties of assessing performance and effectiveness of cyber operations and influence operations alike, estimating and measuring impacts of cyber-enabled influence operations are likely to remain significant challenges, obstructing Western militaries from performing these operations in a way that breeds accountability and confidence [28][29].

Yet nother challenge for Western governments in building up cyber-enabled influence capability is related to the demanding skillsets of both domains. Cyberspace is extremely dynamic, with many and diverse potential targets and capabilities with short shelf lives [30]. The conditions of cyber operations increase the technical skills, workload, and need for secrecy, such that many countries struggle to find staff [31][32]. Influence in turn requires an immensely different skill set, consisting of psychological, cultural, and technological understanding of people, cultures and societies. A cyber force that could also support influence is thus unlikely to emerge on its own and would also be difficult to build without concerted effort.

The ultimate challenge for the West in conducting cyber-influence operations may stem from how our militaries are historically structured and governed. Multi-domain operations are a current buzzword reflecting the need of Western militaries to coordinate better across their military services and capabilities [33]. However, Western military organizations are traditionally built on principles of division and compartmentalization of labour, thus tending to group people with similar skills in distinct chains of commands and locations, especially below the threshold of armed conflict [34]. It is known that militaries already face difficulty integrating cyber and information warfare with traditional kinetic operations in a joint sense [35]. Stovepipe capabilities are bound to additionally inhibit cyber- and information-related warfare -- also known as 'intangible warfare' [36] -- in "creating cognitive impacts in a planned manner" [24].

3.1 Highlights of Western Cyber and Influence Doctrine

A spectrum of doctrine approaches to coordinating cyber and influence is illustrated in Table 2, which describes several pieces of new doctrine concerning information to observe how Western militaries are addressing the coordination across information capabilities.

Doctrine	Schema for Cyber and Influence
NATO's AJP 3.20 Cyberspace Operations (2020) [37]	● Contemporary influence operations are typically conducted in cyberspace, they benefit from integration with COs, which target the logical layer of cyberspace (software, data and protocols) but can achieve substantial effects on the cyber-persona layer where people virtually interact and encounter information (2.27). ● Recommends operational commands run integrated Joint Targeting Cycles and (JTC) operational planning process (OPP) with representatives of cyber and PSYOPS capabilities maintaining a common operating picture of cyberspace and planning and executing activities on targets in tandem (3.18, 3.21) (3.40).
France's Ministere Des Armees (MdA)'s Lutte Informatique (2021)[38]	● Has developed an integrated "Lutte Informatique D'Influence" (computer influence warfare) function (L2I) under the Cyber Defence Command. ● In peacetime can counter adversarial disinformation and support Strategic Communication. In wartime can conduct military deception against adversaries as well as operations to attack their legitimacy. ● Additionally empowers operational commands to build specialized L2I units capable of supporting military operations by disrupting adversarial propaganda and amplifying and mobilizing sabotage actors.
US Army ADP 3-13 Information (2024)[39]	● Divides Information Activities into "Inform," "Influence" and "Attack" pillars, with Influence in its own pillar and Cyberspace operations under the "Attack" pillar (7-19). ● It is unclear whether Cyber and Influence units will be able to consistently coordinate within this structure.
Canada's Defence Policy Update (2024)[40]	● Canada's DND/CAF has been charged to develop a Cyber Command (DND, 2024) in conjunction with the Communications Security Establishment [37]. ● There is no current doctrine establishing coordination between cyber and influence units.

Table 2 – Some Examples of Doctrine Bearing on Cyber-Enabled Influence

As seen in this table, NATO--and by implication the UK who have adopted their doctrine, conceive of cyber and influence as functioning smoothly in integration with kinetic warfare. To achieve this outcome, France initiated the computer-influence concept to integrate cyber and influence into single units. The US and Canada, on the other hand, are building up their cyber-capabilities in ways that could--in theory at least--silo them away from influence as well as other joint activities. US Cyber Command has already been accused of not being well-set up to support joint capabilities, or to delegate its own capability to joint operational commands [41].

4 Conclusion

The examples reviewed and discussed above demonstrate how the incorporation of cyber tactics into influence operations holds potential to increase their scale and impact, while helping them evade detection and attribution. The examples further show that cyber-enabled influence activities become more sophisticated with time and iteration.

A lesson to be taken is that if Western militaries intend to competitively engage in cognitive warfare against adversaries in their operations, influence units will require sophisticated and consistent cyber support. The solution innovated by the French has been to develop a dedicated cyber-enabled influence function. Yet, on the surface at least, some western militaries appear to be preparing only for sporadic and ad hoc coordination between influence and cyber teams, which may be insufficient to build momentum in this domain.

Solutions for integrating cyber and influence capabilities thus urgently need to be devleoped, notwithstanding challenges in combining and sustaining the required skillsets and in justifying these functions to the public. All in all, cyber-enabled influence is likely to present ongoing challenges to the West with regards to norms, skills, and organizational structure; these challenges should be anticipated and faced head on, rather than encountered as they arise.

References

[1] P. Paganini. (2013), Social Media Use in the Military Sector. Infosec Institute. Accessed at Social Media

[2] T. Seaboyer, (2017), Influence Techniques Using Social Media, Defence Research and Development Canada, DRDC-RDDC-2018-C1

[3] M. Bernier (2013), Military Activities and Cyber Effects (MACE) Taxonomy, Defence R&D Canada Technical Memorandum TM 2013-226.

[4] Maj. M. Johns (2019), #WAR: The Weaponization of Bots for Online Influence Activities, Canadian Forces College JCSP 45.

[5] D. Tayouri (2020), The Secret War of Cyber Influence Operations and How to Identify Them, Cyber, Intelligence, and Security, 4(1).

[6] D. Bazarkina & D. Matyashova (2022) "Smart" Psychological Operations in Social Media: Security Challenges in China and Germany, European Conference on Social Media 9(1): 14-20.

[7] H. Lin and A. Zegart, eds. (2019), Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, Brookings Institution Press.

[8] S. Cordey (2019). Cyber Influence Operations: An Overview and Comparative Analysis, Center for Security Studies, Zurich SW.

[9] P. A. L. Ducheine, J. van Haaster, and R. van Harskamp (2017), "Manoeuvring and Generating Effects in the Information Environment," ACIL Research Paper 2017-25, 6.

[10] Bergh, A. (2020). Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach. Journal of Information Warfare, 19(4), 110–131. https://www.jstor.org/stable/27033648

[11] Watts, C. (2019). Advanced Persistent Manipulators, Part Three: Social Media Kill Chain. German Marshall Fund Alliance for Securing Democracy. Advanced Persistent Manipulators, Part Three: https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-three-social-media-kill-chain/

[12] Schneier, B. (2019). Towards an Information Operations Kill Chain. https://www.lawfaremedia.org/article/toward-information-operations-kill-chain#site-main

[13] DiResta, R. et al. (2019). The Tactics and Tropes of the Internet Research Agency. United States Senate Documents. https://digitalcommons.unl.edu/senatedocs/2/

[14] Nimmo, B. & Hutchins, E. (2023). Phased-Based Tactical Analysis of Online Operations. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations?lang=en&center=global

[15] Significant Cyber Incidents. (2024). Center for Strategic and International Studies (CSIS), Washington, D.C., https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[16] Howard, P. N. et al. (2019) The IRA, Social Media and Political Polarization in the United States, 2012-2018. United States Senate Documents. https://digitalcommons.unl.edu/senatedocs/1/

[17] Thomas, E. (2024). Pro-CCP 'Spamouflage' network pivoting to focus on US Presidential Election. Institute for Strategic Dialogue. https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election/

[18] Rapid Response Mechanism Canada. (2023). Probable PRC "Spamouflage" campaign targets dozens of Canadian Members of Parliament in disinformation campaign. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2023-spamouflage.aspx?lang=eng

[19] Raycraft, R. (2023). Global Affairs says disinformation operation targeted MP Michael Chong on WeChat. CBC News, https://www.cbc.ca/news/politics/wechat-disinformation-operation-chong-1.6931377

[20] EU Disinfo Lab. Doppelganger Operation. https://www.disinfo.eu/doppelganger-operation/

[21] Antoniuk, D. (2024). Russian hackers infiltrated Ukrainian telecom giant months before cyberattack. Recorded Future News, https://therecord.media/russians-infiltrated-kyivstar-months-before

[22] Google Threat Analysis Group, June 26, 2024, "Google disrupted over 10,000 instances of DRAGONBRIDGE activity in Q1 2024", Google Blog. Google TAG: New efforts to disrupt DRAGONBRIDGE spam activity (blog.google)

[23] LCol. R. Moll (2020), Cyber-Enabled Influence Wafare, Canadian Forces College JCSP 46.

[24] J. Whiteaker & S. Valkonen (2022), "Cognitive Warfare: Complexity and Simplicity," in B. Claverie; B. Prébot; N. Buchler & F. du Cluzel, Cognitive Warfare: The Future of Cognitive Dominance, NATO Collaboration Support Office, 11, 1-5.

[25] K. Orinx, T. Struye de Swielande (2022), "China and Cognitive Warfare: Why Is the West Losing?" in B. Claverie; B. Prébot; N. Buchler & F. du Cluzel, Cognitive Warfare: The Future of Cognitive Dominance, NATO Collaboration Support Office, 8: 1-6.

[26] NATO (2021), NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting, Edition B, version 1, November 2021.

[27] US DOD (1984), Directive S-3321.1, Overt Psychological Operations Conducted by the Military Services in Peacetime and in Contigencies Short of Declared War.

[28] E. Orye & O. Maennel (2019), Recommendations for Enhancing the Results of Cyber Effects, 2019 11th International Conference on Cyber Conflict:

Silent Battle, T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (Eds.). NATO CCD COE.

[29] J. Vićić & R. Harknett (2024), Identification-imitation-amplification: understanding divisive influence campaigns through cyberspace, Intelligence and National Security 39 (5), 897-914.

[30] H. Lin and A. Zegart, eds. (2019), Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, Brookings Institution Press.

[31] S. Carberry, August 3 2023, Pentagon desperately seeking cyber workers, National Defence Magazine, https://www.nationaldefensemagazine.org/articles/2023/8/3/pentagon-desperately-seeking-cyber-workers

[32] D. Pugliese, February 20, 2024, DND Cyber Force Hindered by Lack of Staff and Training Assessment Team, Ottawa Citizen, https://ottawacitizen.com/news/national/defence-watch/dnd-cyber-force-hindered-by-lack-of-staff-and-training-assessment-team-warns

[33] R. Walden (September 13, 2023), quoted in "Embracing the Future of Warfare: US and Allies Forge Ahead with Multi-Domain Operations," Shephard Media. Blog accessed at Embracing the Future of Warfare: US and Allies Forge Ahead with Multi-Domain Operations (Studio) | Shephard (shephardmedia.com)

[34] R. Stelmack and D. Gomez (July 12, 2021), Breaking out or our Silos: How to Strengthen Relationships between Service-Specific Information Operations Communities, and Why we Need to, *Modern War Institute,* accessed at Breaking Out of Our Silos: How to Strengthen Relationships Between Service-Specific Information Operations Communities, and Why We Need To - Modern War Institute (westpoint.edu).

[35] T. Grant and H. Kantola (2021), Targeting in All-Domain Operations: Choosing Between Cyber and Kinetic Action, European Conference on Cyber Warfare and Security.

[36] D. Moore (2022), Offensive Cyber Operations: Understanding Intangible Warfare, Hurst Publishers.

[37] [7] NATO, AJP-3.20: Allied Joint Doctrine for Cyberspace Operations (January 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

[38] Ministere des Armees (France), Elements Publics de Doctrine Militaire de Lutte Informatique D'Influence (L2I), 2021.

[39] United States Army, 2024, Army Doctrine Publication 3-13: Information.

[40] Department of National Defence (2024), Our North, Strong and Free: A Renewed Vision for Canada's Defence, Accessed at Our North, Strong and Free: A Renewed Vision for Canada's Defence - Canada.ca

[41] Capt. J. M. Black, (February 3, 2020, Integrating Cyber Effects into the Joint Targeting Cycle, Air University, Integrating Cyber Effects into the Joint Targeting Cycle > Air University (AU) > Wild Blue Yonder (af.edu)