National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

BIG DATA AND RELATED CONCEPTS: NEW ASSETS IN CAF OPERATIONS

Lieutenant-Colonel Bryan Blyth

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

BIG DATA AND RELATED CONCEPTS: NEW ASSETS IN CAF OPERATIONS

Lieutenant-Colonel Bryan Blyth

AIM

1. This paper will inform interested parties within the Canadian Joint Operations Command (CJOC) on the upside potential of Big Data concepts and the associated areas of best application within Canadian Armed Forces (CAF) operations.

2. An in-depth analysis of aspects associated with resourcing, education and training, structure, etc. is not in scope of this paper, but may be broadly included as part of the activities the CAF would need to consider in order to employ Big Data into operations. These aspects are areas of supplementary study if Big Data concepts are endorsed to ensure a comprehensive foundation and strategy for implementation.

INTRODUCTION

3. As the CAF continues to evolve into a more digital force leveraging technology to support operations[1], newer concepts such as Big Data, Blockchain, and the internet-of-things (IoT) seem attractive as options to increase the CAF's value proposition[2]: operational excellence. These concepts have been driven and successfully adopted by private industry to gain competitive advantage[3], however, adaptability of these concepts to a military context of operational advantage (rather than business competitive advantage) is yet to be assessed.

4. This paper will highlight the potential of Big Data concepts first by discussing Big Data at a macro level followed by some of its forms of analysis in practical application. Secondly, it will outline basic Blockchain functionality and its suitability for maintaining awareness and integrity of information regarding resource stewardship. The last discussion point will be regarding the potential of integrating IoT enabled devices to enhance our common operating picture (COP) across the operational functions.[4]

DISCUSSION

Big Data

5. Big Data lacks a ratified definition[5], but Bagiwa provides a succinct explanation: "Big Data is a broad term for data sets so large or complex that traditional data processing application are inadequate."[6] Boyd and Crawford, as quoted within Landon-

---

[1] 'Close Engagement : Land Power in an Age of Uncertainty : Evolving Adaptive Dispersed Operations', 33–41, accessed 17 January 2022.
[2] Şahin Çetin and Kerim Goztepe, *International Conference on Military and Security Studies 2015 ICMSS Proceedings*, 2015, 55.
[3] Kefa Rabah and Mara Research, 'Convergence of AI, IoT, Big Data and Blockchain: A Review' 1, no. 1 (2018): 1–5.
[4] 'Canadian Military Doctrine.', 2–7, accessed 18 January 2022.
[5] Çetin and Goztepe, *International Conference on Military and Security Studies 2015 ICMSS Proceedings*, 55.
[6] Lawal Bagiwa, 'Big Data: Concepts, Approaches and Challenges - ProQuest', 182, accessed 15 January 2022.

Murray, provide a great working description: "Big Data is less about data that is big than it is about a capacity to search, aggregate, and cross-reference large data sets…as a cultural, technological, and scholarly phenomenon on the interplay of: Technology, Analysis, and Mythology."[7]

6. Chen et al. outline Big Data characteristics that are accepted within the community of practitioners as "the three Vs"[8] identified in Figure 1. Still debated are the additional Vs of veracity (reliability) and value[9] included by some scholars or businesses with specific focal points (not depicted).

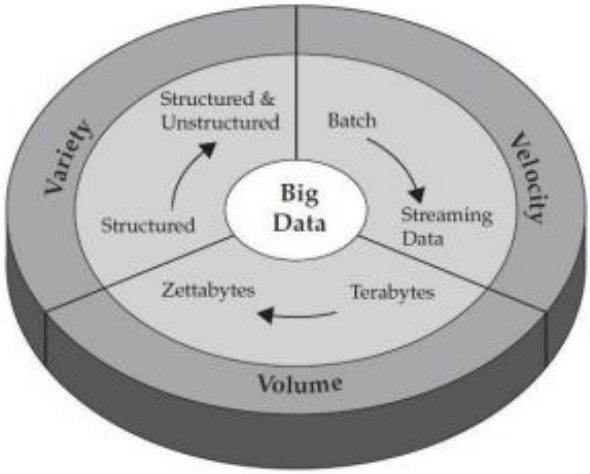

Figure 1 – Big Data Characteristics
Source: Bagiwa, *Big Data: Concepts, Approaches and Challenges*, 182

7. Big Data seeks to enrich business intelligence by producing insights not by trial-and-error, but through accessible data. This provides value in a more timely manner by delivering clarity to uncertainty, predictability for the volatile, stability for the dynamic, and useful trends for the complexity of the future land (as well as other components) operating environment (FLOE).[10] This is not resource neutral, or light, as investment in infrastructure and education would be required to appropriately harness Big Data; however, the return on investment (ROI) may be worth the short-term strain, and it may be mitigated through hybrid options of vertical integration (internal to CAF/DND), outsourcing, or both through feedback from trialing the capabilities.

8. The Intelligence (Int) Community (IntCom), supporting the sense function, is best suited to leverage Big Data for two distinct reasons: first, the benefits, in order of value, from the analytic processes of Big Data: Prescriptive (precision with additional

[7] Michael Landon-Murray, 'Big Data and Intelligence: Applications, Human Capital, and Education', *Journal of Strategic Security* 9, no. 2 (Summer 2016): 95, http://dx.doi.org/10.5038/1944-0472.9.2.1514.
[8] Yong Chen et al., 'Big Data Analytics and Big Data Science: A Survey', *Journal of Management Analytics*, 26 February 2016. https://www.tandfonline.com/doi/abs/10.1080/23270012.2016.1141332?
[9] Bagiwa, 'Big Data', 182.
[10] 'Close Engagement : Land Power in an Age of Uncertainty : Evolving Adaptive Dispersed Operations', 11.

layer of proposed actions from predictive), Predictive (past trends to predict future behaviour), Diagnostic (fault-finding), and Descriptive (past activity to indicate performance)[11] are best applied early to inform commanders and staff through indications and warnings (I&W), Int preparation of the operational environment (IPOE), or more tactically, Int preparation of the battlefield (IPB) as part of the CAF Operational Planning Process (OPP).[12] Second, the skillsets of Int Officers/Operators align with those of data scientists and would assist in operationalization of Big Data for the military. As Landon-Murray states "data scientists must be good at communicating and storytelling, verbally and visually"[13], in addition, Rachel Schutt, as quoted within the same document, outlines the "habits of mind[*, sic*] that good data scientists have, noting storytelling, data intuition, and curiosity, as well as an ability to interpret."[14] Although the IntCom may not have the same scientific backgrounds as data scientists, they could receive introductory education and training on this in order to animate Big Data outputs into more CAF understandable lexicon and applied intelligence.

9. The following is a fictitious scenario highlighting the potential of Big Data. The CAF is ordered to deploy as part of a coalition to the Indo-Pacific region to counter Chinese aggression towards, including the invasion of, Taiwan. Notwithstanding that Int derived between allied partners and by the CAF IntCom would support this mission, Big Data could enhance the CAF success rate via the following (as only some examples):

a. Prescriptive analysis could support all operational tiers of war-gaming throughout the spectrum of conflict (pre-to-post conflict) by analyzing historical and current actions of our allies and adversaries to better inform/develop friendly courses of action (COAs) as well as derive and counter our adversaries' most likely or most dangerous COAs. This analysis could distill Fr/En Strength, Weakness, Opportunities, Threats (SWOT) coupled with historical information to even suggest certain mission objectives and campaign design;

b. Predictive analysis can support activities such as information operations (IO), media response lines, and key leader engagements (KLEs) based on national and regional behaviours and preferences;

c. Diagnostic analysis would greatly assist in capturing, understanding, and better implementing lessons learned from successes and failures of specific operations with feedback into the IntCom for future consideration to either of the above forms of Big Data; and

d. Descriptive analysis could be leveraged as metrics regarding performance to certain statistics and be displayed as dashboards to enhance the COP in the region or for national consumption.

---

[11] Bagiwa, 'Big Data', 183.
[12] 'Joint Intelligence Doctrine.', 4–3, accessed 19 January 2022.
[13] Landon-Murray, 'Big Data and Intelligence', 100.
[14] Ibid., 100.

Blockchain

10. Blockchain works by capturing data, packaging it into a block, and linking that data with a timestamp (verifies interaction), a hash (linkage with previous block) and nonce (verifier of the hash). Once all the information is validated it is added to the chain and can no longer by altered backwards (unless the entire chain is altered); only additions may be made forwards, as illustrated in Figure 2.[15] There is significant technical complexity associated with each of these component parts; however, comprehensive discussion into this complexity is not deemed by the author as required for the purposes of conveying the utility of Blockchain for CAF operations.

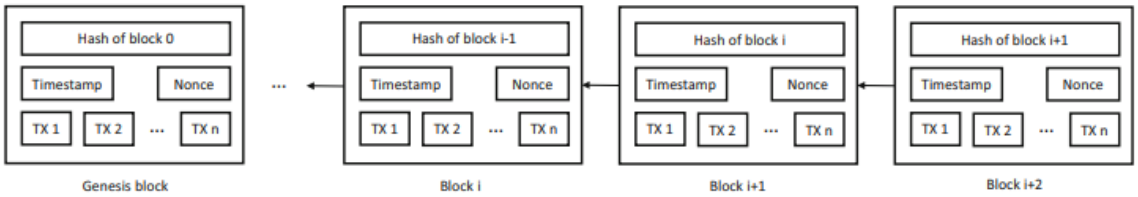

Figure 2 – Example of a Blockchain
Source: Nofer et al., *Blockchain*, 184

11. Rabah, within their *Lake Institute Review* of emerging technologies, states that "blockchain technology is proving to be the most significant technology breakthrough since the innovation of the internet".[16] Blockchains ability to assure the integrity of the data within its chain is its value proposition, a benefit based upon what Tijan et al. deem its properties of transparency, decentralization, and security as shown in Figure 3[17]. The innovative architecture transitions away from traditional server-to-client models and even from cloud technologies, both of which are centralized, to an edge-like approach leveraging peer-to-peer (P2P) technology. This gives owners full control, auditability, limited concern regarding corruption, bad or missed data, or espionage like actions, and finally, options for open or private access.[18]

[15] Michael Nofer et al., 'Blockchain', *Business & Information Systems Engineering* 59, no. 3 (June 2017): 184, http://dx.doi.org/10.1007/s12599-017-0467-3.
[16] Rabah and Research, 'Convergence of AI, IoT, Big Data and Blockchain: A Review', 3.
[17] Edvard Tijan et al.
[18] Ibid., 4–5.

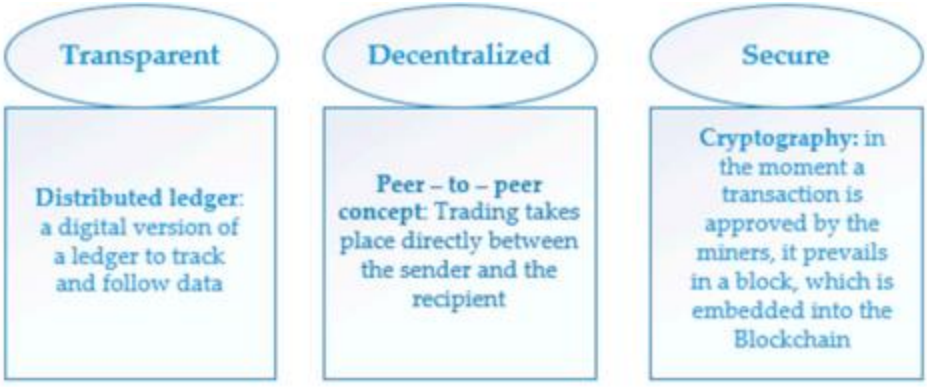

Figure 3 – Properties of Blockchain
Source: Tijan et al., *Blockchain technology Implementation in Logistics*, 3

12. Russia, China, and the United States (US) are all discussing and adopting Blockchain technologies within their respective nations and state forces.[19] Each state is considering Blockchain with a different focus, but nonetheless seeking application from process enhancements, through tactical enablement, to supporting international great power competition.[20]

13. Figure 4 highlights considered applications of Blockchain by our closest ally, the US, and our two most significant adversarial threats, Russia and China. When considering the FLOE[21] and how Canada will "engage in the world,"[22] attention towards US considerations of Blockchain for interoperability as well as effective contribution to and benefits from the US must be afforded. Proposed focal points for the CAF are therefore Command and Control (C2), Command, Control, Communications, Computers, Int, Surveillance, and Reconnaissance (C4ISR)[23], and *Logistics* (as primary).

[19] Bilyana Lilly and Sale Lilly, 'Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia', *The RUSI Journal* 166, no. 3 (16 April 2021): 46–56, https://doi.org/10.1080/03071847.2021.1886871.
[20] Ibid., 55.
[21] 'Close Engagement : Land Power in an Age of Uncertainty : Evolving Adaptive Dispersed Operations', 11.
[22] 'Strong, Secure, Engaged : Canada's Defence Policy: National Defence, accessed 21 January 2022. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html
[23] Ibid., 56.

Warfare Focus	Specific Use Case	US	China	Russia
Civil–Military Integration	• Smart contract management. • Civilian supply chain auditing. • Critical defence infrastructure monitoring.	✓ ✓	✓	 ✓
Command and Control (C2)	• Anti-hacking, intrusion detection. • Battle orders management. • Network and data redundancy. • Digital order-of-battle verification.	✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓
Communications (C4ISR)	• Encrypted communications client. • Credentialled identity management.	✓ ✓	✓	✓
Operations	• Drone swarms, micro-UAV management. • Airborne ISR platforms.	 ✓	✓	✓
Military Intelligence	• Handler and source/informant tool. • Confidential payment platform.		✓ ✓	 ✓
Military Logistics	• Supply chain management (inventory). • Quality assurance. • Additive manufacturing/3D printing.	✓ ✓ ✓	✓ ✓ ✓	✓
Psychological Operations	• Decentralised propaganda channels.		✓	
Training	• Professional military education. • Officer and NCO career tracking.		✓ ✓	
Terrorism and Counterterrorism (CT)	• CT tracking, targeting and disruption. • CT sanctions, finance enforcement.	✓ ✓		

Figure 4 – Intended Use Cases for US, China, and Russia
Source: Lilly and Lilly, *Weaponising Blockchain*, 49

14. An applicable scenario showcasing the utility of Blockchain within the Logistical and C2 domains would be during either routine operations (garrison) or deployed on operations:

a. Routine: Blockchain could not only act as an integrator for various systems of record such as the Land Equipment Management System (LEMS), Defence Resource Management Information System (DRMIS), and various Communications Security (COMSEC) Management Softwares (CSMS) but would also assure integrity and audit trails, traceability, and may still reside on principle employed networks such as the Defence Wide Area Network (DWAN) or Canadian Deployed Mission

Network (CDMN) through a P2P design rather than server architecture. These benefits would enhance stewardship from contract management within Force Development, to asset tracking and logistical COP supporting Ops VECTOR, LASER, LENTUS, to zero risk tolerance areas such as finance, COMSEC, weapons, etc.

b. Deployed Operations: Within the FLOE and the debated future operating concept of multi-domain operations (MDO)[24], anti-access and anti-denial (A2/AD)[25] is of great concern. Adopting a Blockchain technology mitigates this threat, creates data and network "resilience"[26], and could also support tamper-proof battle orders management and distribution[27] ensuring many principles of warfare.[28]

IoT

15. The IoT is defined by the International Telecommunication Union (ITU), an agency of the United Nations, as "a global infrastructure…enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies."[29] The underlying premise is a device's ability to communicate with other devices, meaning, first, that devices cannot be designed and produced as standalone, or isolated, piece(s) of equipment such as the historical doorbell, and second, that there is a "vehicle" to send transmissions between pieces of equipment (Infra-Red, Bluetooth, Cellular, WiFi, etc.); the type and capability of the "vehicle" allows for either very local or worldwide connectivity.[30]

16. The CAF is already employing this form of technology via use of tactical satellite links, radio communications, etc., but not to the full appreciation that is possible, such as automated services, real or near real-time data, or utility as a backbone to greater systems and technologies such as Big Data and/or Blockchain: this is where the most benefit and advantage could be achieved. Xianli et al. discuss military IoT from a Chinese military logistics perspective[31] as depicted by Figure 5 (recreated to capture all concepts).

---

[24] 'Townsend-Multi-Domain.Pdf', accessed 21 January 2022, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-18/Townsend-Multi-Domain.pdf.
[25] Sam Tangredi, 'Parameters 49 (1-2) Spring-Summer2019', *US Army War College Quarterly Parameters* 49, no. 1–2 (n.d.): 5.
[26] Lilly and Lilly, 'Weaponising Blockchain', 54.
[27] Ibid., 49.
[28] 'Canadian Military Doctrine.', 2–5.
[29] Felix Wortmann and Kristina Flüchter, 'Internet of Things: Technology and Value Added', *Business & Information Systems Engineering* 57, no. 3 (June 2015): 221, http://dx.doi.org/10.1007/s12599-015-0383-3.
[30] Wortmann and Flüchter, 222.
[31] Li Xianli et al., 'The Application Research on Military Internet of Things', in *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 2020, 187, https://doi.org/10.1109/ICCWAMTIP51612.2020.9317321.

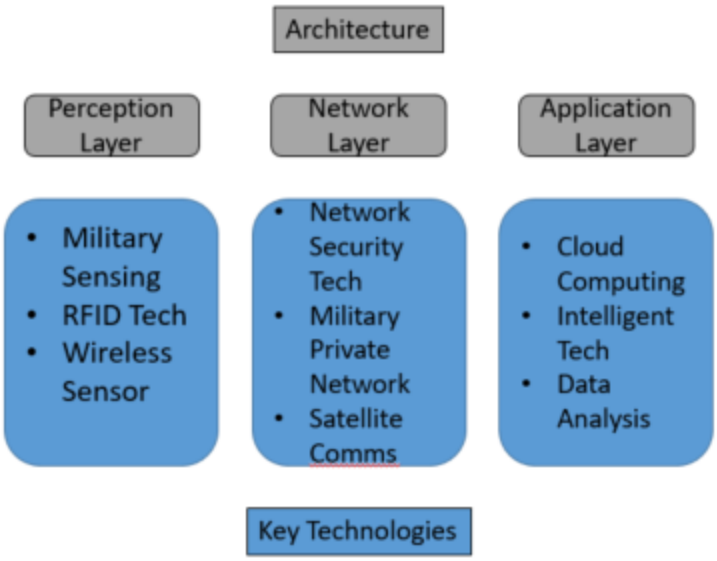

Figure 5 – Recreated Architecture and Key Technologies of MIoT
Source: Xianli et al., *The Application Research on Military Internet of Things*, 188

17. The main issues around IoT technology are adaptation to the processes and models sustaining the organization to maximize benefit[32], security concerns associated with data integrity or intercept[33], and with the shear amount of data collected and shared via the IoT and an organization's capacity to store, search, collate, and interpret/leverage said data to support decision making[34].

18. The solution to at least the latter two challenges described may be through the fusion of IoT, Big Data, and Blockchain. Indeed, Chen et al. outline that the IoT and Big Data are very much connected to produce and derive new forms of value to an organization: "IoT is not only an important source of big data, but also provides opportunities for the application and development of big data." They continue to state that "Ubiquitous computing aims to create ambient [automated] intelligence where network devices are embedded."[35] If this signifies the future of computing and decision support tools, one would want to safeguard access to only trusted parties, who in turn analyze and create operational advantage; Blockchain may be the answer. This is perfectly summarized by Rabah: "In the first epoch of big data, power resided with those who owned the data. In the blockchain epoch of big data, power will reside with those who can access the most data and who can gain the most insights most rapidly."[36]

19. Returning to the original scenario, one can see that through the deployment of internal IoT enabled devices and collection of public IoT devices data, a substantial

[32] Wortmann and Flüchter, 'Internet of Things', 224.
[33] Rabah and Research, 'Convergence of AI, IoT, Big Data and Blockchain: A Review', 6.
[34] Li Xianli et al., 'The Application Research on Military Internet of Things', 190.
[35] Chen et al., 'Big Data Analytics and Big Data Science', 23.
[36] Rabah and Research, 'Convergence of AI, IoT, Big Data and Blockchain: A Review', 14.

amount of information is available and available to all. Integrate and superimpose Big Data with this data collection will provide options of aforementioned analytics to produce useful as well as timely information. Finally, as the CAF would want to secure our internal IoT devices/data as well as analytical processes and outputs, Blockchain could accomplish this. This combination would provide the CAF a substantially better chance at information superiority via intelligence leading to operational advantage for our commanders in decision making and mission actions.

CONCLUSION

20. This paper has demonstrated through academic research as well as practical application to current and likely future mission sets, how Big Data concepts, namely Big Data, Blockchain, and the IoT can not only be applied to CAF operations but how they would significantly enhance domains of certain operational functions from the tactical to strategic level.

21. Further expansion and use of IoT not only as communications "vehicles" but sensory devices bolsters the quantity of CAF sense capabilities as a starting point to Int led operations. Big Data, either partially or fully implemented would translate this data into information complimenting extant Int processes, setting the conditions for unknown opportunities and/or improved command led initiatives for CAF objectives. Blockchain provides an innovative way to distribute and access data, while also reinforcing our security posture, shielding ourselves and our assets, and bolstering our resource stewardship in order to sustain operations.

RECOMMENDATIONS

22. The following are recommended should command endorse the inclusion of Big Data concepts into CAF operations. Although this author believes all of these technologies could evolve the CAF into a more agile and potent contributor with allies, should only certain technologies be endorsed, or at least endorsed initially until more information and applicability is prevalent, it would represent a step into the future. That concept is captured by Rabah as the essence of these technological evolutions by concluding his review with the following statement:

> "it's important to note it doesn't matter if its [*sic*] blockchain, big data, [or IoT], these technologies …depend upon the other for an effective solution. What matters, is the transformative power … in enhancing business competitiveness."

Recommendation 1: Further Study

23. Research and reports on the elements excluded from this service paper must occur. A thorough understanding of the resource, education, training and integration, and structure requirements must be known in addition to any potential process or doctrinal updates prior to any partial or full implementation of the concept(s). With this

information, Commander CJOC, or other commanders, will be able to appropriately assess their appetite and willingness for these technologies and more specifically within which domains or operations.

24. Without this comprehensive level of detail, critical assessment of cost, perceived benefits, and other influencing factors would likely be ill-informed and could lead to lost investment, and/or worse, unsatisfactory results with a deterioration in operational capacity and excellence that the CAF could not afford. Should extant priorities or resources conflict, and concurrent progress on recommendations not be achievable, this recommendation must be privileged.

Recommendation 2: Experimentation

25. Prior to "active" implementation, experimentation should be considered for all technologies, as mentioned during discussion of Big Data, within the Canadian Forces Warfare Centre (CFLWC) and/or other Warfare Centres. Provided with specific questions/targets, trialing these technologies will provide a breadth of outputs for assessment regarding which technologies provide the most ROI, which environments within the CAF could these technologies benefit the most, as well as evaluate operational functions, risks, mutual benefit with international allies, and if desired, the strategic/political interface.

26. Of specific note, outputs should include not only the upside potential, but also the unforeseen challenges associated with any or all technologies discussed. Coupled with the additional research from recommendation one, an all-encompassing package will be available to inform respective and apt commanders, as well as provide indications of how their decisions may impact the future operating environment and how the CAF will succeed within it.

Recommendation 3: Risk/Reward Implementation Approach

27. Implementation through a phased/risk based approach is recommended. Informed by the outputs of experimentation, roll-out of selected technologies should be focused on domestic routine operations initially and could be compartmentalized if necessary. This could be followed by further expansion into other networks and operations, with expeditionary last (despite its potential to provide the best return as indicated in the scenarios provided). This process will ensure user feedback on each technology implemented, user acceptance and understanding, stability, as well as infrastructure growth in-line with complexity of support.

BIBLIOGRAPHY

Bagiwa, Lawal. 'Big Data: Concepts, Approaches and Challengest'. Accessed 15 January 2022. https://www.proquest.com/docview/1940161994?pq-origsite=gscholar&fromopenview=true

'Canadian Military Doctrine.' Accessed 18 January 2022.

Çetin, Şahin, and Kerim Goztepe. *International Conference on Military and Security Studies 2015 ICMSS Proceedings*, 2015.

Chen, Yong, Hong Chen, Anjee Gorkhali, Yang Lu, Yiqian Ma, and Ling Li. 'Big Data Analytics and Big Data Science: A Survey'. *Journal of Management Analytics*, 26 February 2016.

'Close Engagement : Land Power in an Age of Uncertainty : Evolving Adaptive Dispersed Operations'. Accessed 17 January 2022.

'Joint Intelligence Doctrine.' Accessed 19 January 2022.

Landon-Murray, Michael. 'Big Data and Intelligence: Applications, Human Capital, and Education'. *Journal of Strategic Security* 9, no. 2 (Summer 2016): n/a. http://dx.doi.org/10.5038/1944-0472.9.2.1514.

Lilly, Bilyana, and Sale Lilly. 'Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia'. *The RUSI Journal* 166, no. 3 (16 April 2021): 46–56. https://doi.org/10.1080/03071847.2021.1886871.

Xianli, Li, Pan Wei, An Jianyong, and Wan Ping. 'The Application Research on Military Internet of Things'. In *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 187–91, 2020. https://doi.org/10.1109/ICCWAMTIP51612.2020.9317321.

Nofer, Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck. 'Blockchain'. *Business & Information Systems Engineering* 59, no. 3 (June 2017): 183–87. http://dx.doi.org/10.1007/s12599-017-0467-3.

Rabah, Kefa, and Mara Research. 'Convergence of AI, IoT, Big Data and Blockchain: A Review' 1, no. 1 (2018): 18.

'Strong Secure Engaged : Canada's Defence Policy: National Defence - DesLibris'. Accessed 21 January 2022. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html

Tangredi, Sam. 'Parameters 49 (1-2) Spring-Summer2019'. *US Army War College Quarterly Parameters* 49, no. 1–2 (n.d.): 118.

Tijan, Edvard, Saša Aksentijević, Katarina Ivanić, and Mladen Jardas. "Blockchain Technology Implementation in Logistics." Sustainability 11, no. 4 (2019): 1185. doi:http://dx.doi.org/10.3390/su11041185. https://www.proquest.com/scholarly-journals/blockchain-technology-implementation-logistics/docview/2574340262/se-2.

'Townsend-Multi-Domain.Pdf'. Accessed 21 January 2022. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-18/Townsend-Multi-Domain.pdf.

Wortmann, Felix, and Kristina Flüchter. 'Internet of Things: Technology and Value Added'. *Business & Information Systems Engineering* 57, no. 3 (June 2015): 221–24. http://dx.doi.org/10.1007/s12599-015-0383-3.