National Defence Défense nationale

Canadian Forces College
Collège des Forces Canadiennes

# ACHIEVING DECISION SUPERIORITY:
# THE NEED FOR A SECURE CLOUD CAPABILITY

**Major Denis Lopes**

| JCSP 50 | PCEMI n° 50 |
|---|---|
| **Service Paper** | **Étude militaire** |
| **Disclaimer** | **Avertissement** |
| 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. | 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 50 - PCEMI n° 50
2023 - 2024

Service Paper – Étude militaire

# ACHIEVING DECISION SUPERIORITY: THE NEED FOR A SECURE CLOUD CAPABILITY

**Major Denis Lopes**

*"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."*

*« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de difuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »*

# ACHIEVING DECISION SUPERIORITY:
# THE NEED FOR A SECURE CLOUD CAPABILITY

## AIM

1. The Canadian Armed Forces (CAF) needs a secure cloud if it is serious about digitalization and, more importantly, decision superiority. There are two options: enter an arrangement with the US Government to use their secret cloud or find a way to secure data in a public cloud.[1] For both effectiveness and redundancy, both options are needed. As the CAF's CIO Group is currently working on accessing the US Government's secret cloud, this paper addresses the benefits, obstacles, and a solution of storing classified data in a public cloud.[2]

## BACKGROUND

### Current DND/CAF Priorities

2. The Department of National Defense (DND) and the CAF have discussed the need for cloud capabilities since at least 2017. In the Strong, Secure and Engaged (SSE) Defense Policy, several initiatives point to the need to modernize CAF Command and Control (C2), such as:

a. Initiative 41: Improve the Army's ability to operate in remote regions by investing in modernized communications…;

b. Initiative 43: Modernize land-based C2, …;

c. Initiative 59: Modernize and enhance Special Operations Forces C2 and Communication Information Systems;

d. Initiative 62: Acquire joint C2 systems and equipment, specifically for integrated information technology and communications;

e. Initiative 65: Improve cryptographic capabilities; and

[1] Microsoft Azure, "Azure Government Top Secret Now Generally Available for US National Security Missions," Blog Post, Microsoft Azure Blog, August 16, 2021, https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/.

[2] Amanda Connolly, "Will Cloud Computing Be Canada's next Big Military Procurement? Here's What to Know - National | Globalnews.Ca," News, Global News, April 5, 2022, https://globalnews.ca/news/8706412/canada-national-security-classified-cloud-services/; Treasury Board of Canada, "Government of Canada White Paper: Data Sovereignty and Public Cloud," report on plans and priorities, Government of Canada White Paper: Data Sovereignty and Public Cloud, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.

f. Initiative 68: Integrate existing and future assets into a networked, joint system-of-systems that will enable the flow of information among multiple interconnected platforms and operational headquarters.[3]

3. The Pan-Domain Force Employment Concept (PFEC) is the CAF's latest defence publication. It provides fourteen ways the CAF must evolve to prevail in today's operating environment. Of the fourteen, the following three elements indicate a need to modernize how C2 is executed:

a. Element 8: Artificial Intelligence (AI) to meet the demands of contemporary operations;

b. Element 10: Evolved planning and C2 to enable integration in all its forms and thrive in our environment; and

c. Element 12: Broad Interoperability to allow force elements to act internally and externally to the CAF as part of a coherent whole.[4]

4. On top of SSE and PFEC outlining the importance of modernizing decision-making, different L1s have also stated the importance of digitalizing. For example, the Canadian Army's modernization initiative has six principles. The first principle is "digitization and enhanced networking."[5] As such, one of the highest priorities of the CAF is to modernize decision-making across all levels.

## What Is the Competitive Advantage of a Secure Cloud?

5. Cloud computing is vital for achieving decision superiority over a peer adversary or competitor. Firstly, cloud computing provides a means to aggregate vast and diverse data sources, enabling organizations to analyze large volumes of structured and unstructured data in real-time. This wealth of information allows decision-makers to make data-informed decisions, leading to better results. Additionally, cloud-based analytics and machine learning tools can uncover valuable insights and patterns within the data, further enhancing the quality of decision-making processes.[6]

6. However, it is impossible for an organization to "jump" straight into machine learning analytics (cloud computing's real competitive advantage). An organization must progress up what is commonly called the "data hierarchy of needs."[7] The CAF is no different.

[3] National Defence, "Strong, Secure, Engaged: Canada's Defence Policy," policies, Strong, Secure, Engaged: Canada's Defence Policy, September 22, 2017, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html.

[4] National Defense, "Pan-Domain Force Employment Concept" (Department National Defense, October 2023), https://mars.cfc.forces.gc.ca/CFCLearn/mod/folder/view.php?id=7378.

[5] Canadian Army National Defence, "Advancing with Purpose: The Canadian Army Modernization Strategy," education and awareness, January 7, 2021, https://www.canada.ca/en/army/services/for-the-soldier/canadian-army-modernization-strategy.html.

[6] Yara Alghofaili et al., "Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges," *Applied Sciences* 11, no. 19 (September 27, 2021): 4–5, https://doi.org/10.3390/app11199005.

[7] R Alan Blackburn, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy," 2018, 14, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

7. The data hierarchy of needs, inspired by Maslow's hierarchy of needs, provides a conceptual framework for understanding the five general steps of data utilization to achieve decision superiority. The data hierarchy of needs is a pyramid structure, with foundational layers supporting more advanced data processing and analysis stages. The steps starting from the base are "data collection," "data infrastructure," "data hygiene," "data aggregation," and, at the pinnacle, "data insights." For the CAF to achieve decision superiority, it must evolve starting at the bottom of the pyramid.

8. The hierarchy's base is the collection of data. Data can be collected through many different means, including sensors. In general, the CAF is good at collecting data. Doctrinally, the term "ISR" (Intelligence Surveillance and Reconnaissance) is used to collect adversarial or terrain information. But equally, data can also be generated from any internal processes. The second level of the pyramid is the data infrastructure needed to move and store the collected data. The CAF urgently needs to evolve its legacy networks to that of public and private cloud infrastructure to enable higher levels in the pyramid.

## What Is Cloud Computing?

9. Cloud computing refers to delivering computer services, including storage, processing power, and applications, over the internet. This is a fundamental change from traditional on-premises computer infrastructure models managed by CAF signals technicians. Cloud computing allows users to access and utilize computing resources flexibly. The essence of cloud computing lies in the abstraction of physical hardware and the provision of virtualized resources, allowing users to deploy and manage applications without the need for extensive investment in dedicated hardware. Critical aspects of cloud computing are on-demand self-service, high bandwidth requirement, more efficient resource sharing, and data-driven quality-of-service.[8] Cloud computing has gained widespread adoption across various industries due to its cost-effectiveness, scalability, and the ability to offload infrastructure management responsibilities to service providers. It is considered the norm in the private sector.

10. Cloud computing will significantly expedite the CAF's ability to leverage AI. Although the cloud is not a requirement for AI, it is highly advantageous. Firstly, AI models require a significant amount of computational power for training. Managing this infrastructure is costly in terms of both human and financial resources. The cloud offers scalable and powerful computer resources, reducing the human resource burden. Secondly, the cloud provides extensive storage capabilities, which is crucial for managing large datasets used in training AI models. The flexibility of cloud storage allows organizations to efficiently store and retrieve data, making it easier to feed information into AI algorithms.

[8] Muhammad Dawood et al., "Cyberattacks and Security of Cloud Computing: A Complete Guideline," *Symmetry* 15, no. 11 (2023): 1, https://doi.org/10.3390/sym15111981.

### What Are the Different Types of Clouds?

11. **Public Cloud.** This is the colloquial "cloud". A third-party company that offers computing, storage, and applications over the internet. The size and scale of public clouds allow for the easy onboarding of software and enabling AI algorithms and AI-powered applications.

12. **Private Cloud.** In contrast, private cloud refers to dedicated infrastructure provided to a single organization, either on-premises or in a third-party location.[9] Many CAF networks are now virtualized and, in essence, are small-scale private clouds. The benefit of a private cloud is often its cybersecurity posture, as its servers are physically separate from other networks. As such, private clouds can meet security standards for secret and above networks. The largest secret and top secret accredited private clouds are the different US Government clouds.[10] Although several orders of magnitude larger than CAF networks, it is still at a much smaller scale than the public cloud. Transitioning CAF networks onto the US Secret Government cloud significantly evolves the current CAF network architecture.

### What Is Homomorphic Encryption?

13. Homomorphic encryption is a cryptographic technique that allows computations to be performed on encrypted data. The result of the computation is also encrypted, which can then be decrypted to obtain the desired result.[11] This method enables secure computation of classified data without revealing the data itself. The possibility of homomorphic encryption was first proved in 2009, and since then, many improvements have been made to increase its performance and efficiency.

## DISCUSSION

### How Does the Data Hierarchy of Needs Factor In?

14. The goal is to achieve decision superiority by leveraging AI/ML and data-driven decision-making. In that case, the CAF must evolve starting at the bottom of the data hierarchy pyramid. The first step is ensuring that all the collected data is in a digital format and can be leveraged.

15. Secondly, re-architecting critical networks to be data-centric starts with investing in infrastructure. To offload the human resource requirements, transitioning networks to commercial clouds is an excellent first step. The real benefit is providing a scalable data

[9] Saja J. Mohammed and Dujan B. Taha, "From Cloud Computing Security towards Homomorphic Encryption: A Comprehensive Review," *Telkomnika* 19, no. 4 (August 2021): 1153, https://doi.org/10.12928/TELKOMNIKA.v19i4.16875.

[10] Carten Cordell, "Oracle's Cloud Network Gains Top Secret Approval with Intelligence Agencies," news releases, Oracle's cloud network gains top secret approval with intelligence agencies, August 15, 2023, https://www.nextgov.com/modernization/2023/08/oracles-cloud-network-gains-top-secret-approval-intelligence-agencies/389437/.

[11] Jean-Pierre Hubaux, "Homomorphic Encryption," in *Trends in Data Protection and Encryption Technologies*, ed. Valentin Mulder et al. (Cham: Springer Nature Switzerland, 2023), 35–39, https://doi.org/10.1007/978-3-031-33386-6_8.

environment to enable work at the higher levels of the pyramid. Due to the sensitivities associated with some CAF data, this infrastructure will likely need a combination of a public and private cloud solution.

16. A cross-domain solution (CDS) is a security technology that enables the secure transfer of data between different networks with varying classification levels. The goal of a CDS is to facilitate the controlled transfer of data while maintaining its confidentiality, integrity, and availability. CDS' typically include a combination of hardware, software, and procedural controls to enforce security policies and ensure compliance with regulatory requirements. For the CAF, CDS would become an important infrastructure to bridge our private cloud with a commercial cloud. Furthermore, leveraging homomorphic encryption would allow higher levels of the data hierarchy of needs to occur on the public cloud.

17. Data hygiene denotes the processes aimed at maintaining the accuracy and consistency of data within a dataset. It involves defining the data and identifying and correcting errors, inconsistencies, and redundancies. This is an important layer in the pyramid to ensure data is reliable, relevant, and useful.

18. Once the data is clean, it can be augmented with external data sources to help further increase decision quality. Given the CAF is a relatively smaller generator of data, the cloud allows CAF data to be nested within other sources of similar types of data. For example, the Canadian Army purchased 1587 Medium Support Vehicle System (MSVS), a military off-the-shelf truck.[12] On top of sales to other militaries, Mack manufactures the commercial variant of the same truck, meaning there are tens of thousands of similar trucks. Using all the different sources of data allows maintainers to better predict faults and future issues, which should increase the lifespan of the truck. A challenge arises when a portion of the CAF data is classified. Using Homomorphic encryption would allow the CAF to "share" its data on the cloud to make use of the rest of the available truck data while keeping its own data protected.

19. Now at the top of the pyramid, data-based insights can be made. This can be done either through traditional statistical analysis or by leveraging AI/ML algorithms. These insights can be both descriptive and predictive in nature. The value of doing these types of analyses on the public cloud is the ability to use commercial algorithms on private data. These insights now leverage a much larger dataset which would improve decision quality. Furthermore, the insights could be transferred back through the CDS into the CAF's private cloud.

## Challenges of Homomorphic Encryption

20. The major technology challenge with homomorphic encryption is associated with computational complexity, thus creating a huge performance overhead. The problem is further exacerbated by large and complex datasets. This performance overhead can lead to increased

[12] Mack Defense, "Mack Defense Builds Final Truck For Canadian Medium Support Vehicle System (MSVS) Program - Mack Defense," OEM Corporate Website, news release, November 4, 2022, https://www.mackdefense.com/mack-defense-builds-final-truck-for-canadian-medium-support-vehicle-system-msvs-program/.

latency in encrypted data processing and the need for large amounts of memory, storage and computational cycles.[13] Although there have been significant improvements in the technology, it continues to be a challenge. Leveraging the public cloud offsets some of these challenges. As the technology develops, improvements will also help the user experience.

21. Another major technological challenge with homomorphic encryption is that it is not inherently resistant to a quantum computer. An adversary with a quantum computer could decrypt the CAF data and expose sensitive or classified information. Although quantum computers are not widespread, several big tech firms have announced both research and success in developing them, indicating that the technology is more than just theoretical. Like several currently in-use cryptography, which is not post-quantum resistance, the quantum decryption risk associated with homomorphic encryption must simply be accepted. Transient data services like secure voice, secure video teleconference or positional data for CAF operations, although classified, quickly become irrelevant. As such, these are prime options for early adoption of homomorphic encryption as it would be low risk if compromised.

22. The perhaps most critical challenge is that current accreditation does not permit homomorphic encryption for classified use. The Communication Security Establishment (CSE) accredits encryption techniques and schemas. Homomorphic encryption is not currently approved.[14] However, CSE has approved some of the advanced mathematic models used in homomorphic encryption schemas, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH), for up to Protected B.[15] With any cryptographic algorithm CSE verifies any change and provides guidelines on how it needs to be implemented so that it can remain accredited. As such, with the right priority, CSE could publish the exact requirements of how homomorphic encryption could be used to secure CAF data.

23. Homomorphic Encryption is currently being used by both Microsoft and Amazon Web Services (AWS), two of the largest public cloud providers. Microsoft SEAL (Simple Encrypted Arithmetic Library) is an open-source set of homomorphic cryptographic algorithms that support RSA and ECC CDH, which are CSE-approved.[16] Similarly, AWS has a homomorphic solution called SageMaker, which uses the Cheon-Kim-Kim-Song (CKKS) algorithm.[17] CSE currently does not report on CKKS; however, the American regulator, NIST, recognizes it as Advanced

[13] Genesh Kumar Mahato and Swarnendu Kumar Chakraborty, "A Comparative Review on Homomorphic Encryption for Cloud Security," *IETE Journal Of Research* 69, no. 8 (2023): 5124–33, https://doi.org/10.1080/03772063.2021.1965918.

[14] Canadian Centre for Cyber Security, "Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111," Info Sharing, Canadian Centre for Cyber Security, August 1, 2016, https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111.

[15] Elaine Barker et al., "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography" (Gaithersburg, MD: National Institute of Standards and Technology, April 2018), https://doi.org/10.6028/NIST.SP.800-56Ar3.

[16] "Microsoft SEAL: Fast and Easy-to-Use Homomorphic Encryption Library," GitHub Microsoft SEAL, *Microsoft Research* (blog), January 2023, https://www.microsoft.com/en-us/research/project/microsoft-seal/.

[17] Liv D'Aliberti et al., "Enable Fully Homomorphic Encryption with Amazon SageMaker Endpoints for Secure, Real-Time Inferencing | AWS Machine Learning Blog," AWS Blob, AWS Machine Learning Blog, March 23, 2023, https://aws.amazon.com/blogs/machine-learning/enable-fully-homomorphic-encryption-with-amazon-sagemaker-endpoints-for-secure-real-time-inferencing/.

Encryption Scheme (AES) compliant.[18] AES is the commercial standard for encryption. In summary, homomorphic encryption is starting to become both commercially available and recognized by American and Canadian regulators. However, a critical step would be for it to be approved for classified networks.

24. The National Security Agency (NSA) Commercial Solutions for Classified (CSfC) Program enables commercial encryptions (typically AES-compliant) to be accredited for secret use. CSfC has guidelines for how RSA and ECC CDH need to be implemented to achieve accreditation. Given that the security standard for secret is the same in the USA as in Canada, the fact that the NSA has approved RSA and ECC CDH for secret use indicates it could also be approved in Canada.

## RECOMMENDATIONS

25. Based on SSE, PFEC and various L1s stating that decision superiority is a modernization priority, the CAF must aggressively modernize its C2 networks. Using the data hierarchy of needs as a glide path, the CAF must dedicate money and effort to transition its current networks to a combination of the US secret Government cloud and develop a solution to store secret data on the public cloud. Advances in homomorphic encryption allow the CAF to securely augment its data into larger datasets and leverage commercial AI tools. As such, the CAF, specifically the CIO Group, must work with CSE to prioritize the accreditation of commercial homomorphic encryption. Secondly, cross-domain solutions must be established to push homomorphically encrypted data into the public cloud. Once this critically enabling infrastructure is in place, data hygiene and data-driven insights can be improved.

## CONCLUSION

26. Achieving decision superiority, whether the ability to make better or faster decisions, has historically been decisive in combat. Today, in the contemporary operating environment, that means leveraging the public cloud and commercial AI algorithms to make sense of the vast quantities of data for both better and faster decisions. Commercial encryption, specifically homomorphic encryption, would maintain security around CAF data while leveraging insights derived from commercial AI tools.

[18] Nir Drucker, "Note about Authenticated Transciphering: Decrypting AES under HE Using CKKS | CSRC," CSRC Presentation, CSRC | NIST, September 21, 2023, https://csrc.nist.gov/presentations/2023/mpts2023-day2-talk-fhe-aes-transcipher.

## BIBLIOGRAPHY

Alemami, Yahia, Ali M. Al-Ghonmein, Khaldun G. Al-Moghrabi, and Mohamad Afendee Mohamed. “Cloud Data Security and Various Cryptographic Algorithms.” *International Journal of Electrical and Computer Engineering* 13, no. 2 (April 2023): 1867–79. https://doi.org/10.11591/ijece.v13i2.pp1867-1879.

Alghofaili, Yara, Albatul Albattah, Noura Alrajeh, Murad A. Rassam, and Bander Ali Saleh Al-rimy. “Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges.” *Applied Sciences* 11, no. 19 (September 27, 2021): 9005. https://doi.org/10.3390/app11199005.

Alzubi, Jafar A., Omar A. Alzubi, Majdi Beseiso, Anil Kumar Budati, and K. Shankar. “Optimal Multiple Key-based Homomorphic Encryption with Deep Neural Networks to Secure Medical Data Transmission and Diagnosis.” *Expert Systems* 39, no. 4 (May 2022): 1–17. https://doi.org/10.1111/exsy.12879.

Amanda Connolly. “Will Cloud Computing Be Canada’s next Big Military Procurement? Here’s What to Know - National | Globalnews.Ca.” News. Global News, April 5, 2022. https://globalnews.ca/news/8706412/canada-national-security-classified-cloud-services/.

Azure, Microsoft. “Azure Government Top Secret Now Generally Available for US National Security Missions.” Blog Post. Microsoft Azure Blog, August 16, 2021. https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/.

Barker, Elaine, Lily Chen, Allen Roginsky, Apostol Vassilev, and Richard Davis. “Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.” Gaithersburg, MD: National Institute of Standards and Technology, April 2018. https://doi.org/10.6028/NIST.SP.800-56Ar3.

Blackburn, R Alan. “Summary of the 2018 Department of Defense Artificial Intelligence Strategy,” 2018. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

Canadian Centre for Cyber Security. “Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111.” Info Sharing. Canadian Centre for Cyber Security, August 1, 2016. https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111.

Carten Cordell. “Oracle’s Cloud Network Gains Top Secret Approval with Intelligence Agencies.” News releases. Oracle’s cloud network gains top secret approval with intelligence agencies, August 15, 2023. https://www.nextgov.com/modernization/2023/08/oracles-cloud-network-gains-top-secret-approval-intelligence-agencies/389437/.

Dawood, Muhammad, Shanshan Tu, Chuangbai Xiao, Hisham Alasmary, and Muhammad Waqas. "Cyberattacks and Security of Cloud Computing: A Complete Guideline." *Symmetry* 15, no. 11 (2023): 1981. https://doi.org/10.3390/sym15111981.

Defence, National. "Strong, Secure, Engaged: Canada's Defence Policy." Policies. Strong, Secure, Engaged: Canada's Defence Policy, September 22, 2017. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html.

Genesh Kumar Mahato and Swarnendu Kumar Chakraborty. "A Comparative Review on Homomorphic Encryption for Cloud Security." *IETE Journal Of Research* 69, no. 8 (2023): 5124–33. https://doi.org/10.1080/03772063.2021.1965918.

Gnana Sophia, S., K. K. Thanammal, and S. S. Sujatha. "Secure Storage and Accessing the Data in Cloud Using Optimized Homomorphic Encryption." *Journal of Control and Decision* 10, no. 1 (January 2, 2023): 90–98. https://doi.org/10.1080/23307706.2022.2078436.

Government of Canada. "Privacy Preserving Technologies Part Two: Introduction to Homomorphic Encryption," August 30, 2021. https://www.statcan.gc.ca/en/data-science/network/homomorphic-encryption.

Huang, Jie, this link will open in a new tab Link to external site, and Dehua Wu. "Cloud Storage Model Based on the BGV Fully Homomorphic Encryption in the Blockchain Environment." Edited by Mohammad Ayoub Khan. *Security and Communication Networks* 2022 (2022). https://doi.org/10.1155/2022/8541313.

Hubaux, Jean-Pierre. "Homomorphic Encryption." In *Trends in Data Protection and Encryption Technologies*, edited by Valentin Mulder, Alain Mermoud, Vincent Lenders, and Bernhard Tellenbach, 35–39. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-33386-6_8.

Hughes, Chris. "Kubernetes Hardening: Drilling down on the NSA/CISA Guidance." *CSO*, Aug 23, 2021. https://www.proquest.com/docview/A196B86A47874A0APQ/1.

Kiesel, Raphael, Marvin Lakatsch, Alexander Mann, Karl Lossie, Felix Sohnius, and Robert H. Schmitt. "Potential of Homomorphic Encryption for Cloud Computing Use Cases in Manufacturing." *Journal of Cybersecurity and Privacy* 3, no. 1 (2023): 44. https://doi.org/10.3390/jcp3010004.

Liv D'Aliberti, Joe Kovba, Manbir Gulati, Sami Hoda, and Ben Sniverly. "Enable Fully Homomorphic Encryption with Amazon SageMaker Endpoints for Secure, Real-Time Inferencing | AWS Machine Learning Blog." AWS Blob. AWS Machine Learning Blog, March 23, 2023. https://aws.amazon.com/blogs/machine-learning/enable-fully-homomorphic-encryption-with-amazon-sagemaker-endpoints-for-secure-real-time-inferencing/.

Mack Defense. “Mack Defense Builds Final Truck For Canadian Medium Support Vehicle System (MSVS) Program - Mack Defense.” OEM Corporate Website. news release, November 4, 2022. https://www.mackdefense.com/mack-defense-builds-final-truck-for-canadian-medium-support-vehicle-system-msvs-program/.

Microsoft Research. “Microsoft SEAL: Fast and Easy-to-Use Homomorphic Encryption Library.” GitHub Microsoft SEAL, January 2023. https://www.microsoft.com/en-us/research/project/microsoft-seal/.

Mohammed, Saja J., and Dujan B. Taha. “From Cloud Computing Security towards Homomorphic Encryption: A Comprehensive Review.” *Telkomnika* 19, no. 4 (August 2021): 1152–61. https://doi.org/10.12928/TELKOMNIKA.v19i4.16875.

National Academies of Sciences, Engineering, and Medicine, Division on Engineering and Physical Sciences, Intelligence Community Studies Board, and Committee on the Future of Encryption. *Cryptography and the Intelligence Community: The Future of Encryption*. Washington, D.C., UNITED STATES: National Academies Press, 2022. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=30171797.

National Defense, Canadian Army. “Advancing with Purpose: The Canadian Army Modernization Strategy.” January 7, 2021. https://www.canada.ca/en/army/services/for-the-soldier/canadian-army-modernization-strategy.html.

National Defense. “Pan-Domain Force Employment Concept.” Department National Defense, October 2023. https://mars.cfc.forces.gc.ca/CFCLearn/mod/folder/view.php?id=7378.

Nir Drucker. “Note about Authenticated Transciphering: Decrypting AES under HE Using CKKS | CSRC.” CSRC Presentation. CSRC | NIST, September 21, 2023. https://csrc.nist.gov/presentations/2023/mpts2023-day2-talk-fhe-aes-transcipher.

Rupa, Ch, Greeshmanth, and Mohd Asif Shah. “Novel Secure Data Protection Scheme Using Martino Homomorphic Encryption.” *Journal of Cloud Computing* 12, no. 1 (December 2023): 47. https://doi.org/10.1186/s13677-023-00425-7.

Seth, Bijeta, Surjeet Dalal, and Raman Kumar. “Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage.” In *Recent Advances in Computational Intelligence*, edited by Raman Kumar and Uffe Kock Wiil, 71–92. Studies in Computational Intelligence. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-12500-4_5.

Treasury Board of Canada. “Government of Canada White Paper: Data Sovereignty and Public Cloud.” Report on plans and priorities. Government of Canada White Paper: Data Sovereignty and Public Cloud, July 28, 2020. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.