National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

The Evolution of Secrecy: How CANSOFCOM Can Systematically Defeat Ubiquitous Technical Surveillance

Major Denis Lopes

JCSP 50

Exercise Solo Flight

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 n° 50

Exercice Solo Flight

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 50 - PCEMI n° 50
2023 - 2024

Exercise Solo Flight – Exercice Solo Flight

The Evolution of Secrecy: How CANSOFCOM Can Systematically Defeat Ubiquitous Technical Surveillance

Major Denis Lopes

THE EVOLUTION OF SECRECY:
HOW CANSOFCOM CAN SYSTEMATICALLY DEFEAT
UBIQUITOUS TECHNICAL SURVEILLANCE

Ubiquitous Technical Surveillance (UTS) is an emerging concept that describes the evolving state of surveillance in many nations trending towards complete societal coverage.[1] It invokes visions of George Orwell's novel 1984, including telescreens and Big Brother. UTS is the pervasive integration of traditional surveillance technologies, such as cameras and microphones, with digital surveillance and bulk digital data collection. UTS encompasses the systematic monitoring, collection, aggregation, and analysis of data across diverse environments enabled by an extensive array of interconnected devices and networks. This integration extends beyond traditional surveillance methods, permeating physical and digital realms to achieve unprecedented granularity and scope.[2] Artificial Intelligence (AI) advancements have significantly increased the ability to detect patterns, anomalies, individuals, or objects of interest.[3] This provides states with real-time intelligence and pattern-of-life analysis, which has the potential to undermine special operations.

UTS continues to change the contemporary operating environment. Achieving and maintaining secrecy is now more challenging.[4] As such, the Canadian Special Operations Forces Command (CANSOFCOM) security approach will become increasingly ineffective due to the growing sophistication and reach of adversaries' UTS programs unless it takes a systematic approach to evolve this approach, particularly to counter UTS applications for anti-access and area denial (A2AD). This evolution must include: 1. An overhauled Operational Security (OPSEC) approach to minimize the effectiveness of adversarial bulk data collection; 2. A focus on signature management across the physical, electronic, and digital environments; 3. Implementing AI defeating measures; 4. Leveraging cyber operations; and 5. Prioritizing Force Development efforts for UTS-defeating.

This paper describes UTS' security implications for special operations forces (SOF) and the importance of evolving security approaches to counter UTS. It explains the doctrinal consequences of UTS, proving the imperative to change. It provides examples of UTS's growing pervasiveness and how countries use it for A2AD. Finally, it recommends how CANSOFCOM can defeat adversarial UTS capabilities. Although exploiting UTS for CANSOFCOM's benefits could help provide technological overmatch, it is outside this paper's scope.

---

[1] Sergio Sanchez, "Ubiquitous Technical Surveillance: Counterintelligence Bliss, or Nightmare?" (Master of Science of Strategic Intelligence Thesis, Washington, D.C., UNITED STATES, National Intelligence University, 2020), 3, https://doi.org/10.13140/RG.2.2.23516.16002.
[2] Craig W. Gruber et al., *Fostering Innovation in the Intelligence Community: Scientifically-Informed Solutions to Combat a Dynamic Threat Environment* (Cham, Switzerland: Springer International Publishing AG, 2023), 2, http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=30684902.
[3] Utsav Sharma Gaire, "Application of Artificial Intelligence in the Military: An Overview," *Unity Journal* 4, no. 01 (February 15, 2023): 167–68, https://doi.org/10.3126/unityj.v4i01.52237.
[4] Eric Schmidt, "AI, Great Power Competition & National Security," *Daedalus* 151, no. 2 (May 1, 2022): 289, https://doi.org/10.1162/daed_a_01916.

WHY DOES UTS MATTER?

Against a modern adversary, UTS will permeate every facet of special operations. It's the watchful eye that stands guard in the shadows. Once in an operation area, the team will be enveloped by an adversary's network of advanced sensors, drones, and monitoring devices seamlessly integrated into the environment. Surveillance drones will fly overhead, and satellites orbit above them, their cameras capturing every movement with precision. Microphones in the foliage pick up the team's faintest whispers while motion sensors alert the adversary of the intrusion. Even the ground on which the operator stands seems wired, with seismic sensors detecting the subtlest vibrations. Every keystroke, every transmission, every heartbeat is logged and analyzed, feeding vital intelligence back to the adversary thousands of kilometres away. The CANSOFCOM team is spotted and tracked. There is no surprise, no speed; they are compromised. Mission Fail!

Although this may be a current stretch of today's battlefield, it is not a distant reality. Omnipresent surveillance is a reality today. Cities are dotted with CCTV cameras, homes are filled with various electronic sensors, and our online personas are all feeding the algorithms that know exactly who we are and what we do.[5] The concept of secrecy needs to evolve to adapt to the realities of UTS.

UTS isn't just a factor within operations areas. It is an ever-present reality, including within Canadian garrisons. A series of cameras enabled with facial recognition and long-range microphones can be set up outside any Canadian base, including Dwyer Hill Training Center. Both data streams are combined and further augmented by video from cars passing by, drones, and satellites overhead. Cell phone data could provide fidelity in who enters and leaves the facilities and a lens to everyone's personal life. Lastly, bulk data collection on the facility can occur, amplifying the pattern of life and detecting the spikes and valleys of encrypted traffic. This helps determine periods when the facility is on high alert. Collecting social media accounts from the facility worker's family members provides further insight into the facility's hierarchy and critical moments.[6] With such UTS in place, all aspects of this military compound and its people are no longer secret. Thus, the effectiveness of all the units and individuals within it is at risk.

Security is paramount in special operations.[7] But now, given the pervasiveness of surveillance and the invasive modern technologies, it needs to factor into the entire lives of SOF members and not just when operations start. SOF must defeat the adversaries' UTS to remain effective.

---

[5] Sanchez, "Ubiquitous Technical Surveillance," 9; Panagiotis Karampelas and Thirimachos Bourlai, eds., *Surveillance in Action: Technologies for Civilian, Military and Cyber Surveillance*, Advanced Sciences and Technologies for Security Applications (Cham: Springer International Publishing, 2018), 353–55, https://doi.org/10.1007/978-3-319-68533-5.

[6] Valanarasu, R., "Comparative Analysis for Personality Prediction by Digital Footprints in Social Media," *Journal of Information Technology and Digital World* 3, no. 2 (May 31, 2021): 79, https://doi.org/10.36548/jitdw.2021.2.002.

[7] Colonel Bernd Horn, "When Cultures Collide: The Conventional Military / SOF Chasm," *Canadian Military Journal* Autumn 2004 (2004): 10.

THE IMPORTANCE OF SECURITY

Special operations are often politically sensitive, and if compromised by an adversary, it could lead to mission failure, endangering the lives of the SOF members or political backlash.[8] Historically, maintaining the secrecy of these operations has minimized the risk of the adversary detecting, intercepting or interfering.[9] Former Commander US Special Operations Command Admiral William H McRaven claimed that security is one of six characteristics that all special operations require for success.[10] On top of the strategic and political importance of secrecy, there are also operational and tactical importance. Secrecy allows SOF to maintain an element of surprise. This includes protecting the identities of special operations personnel to prevent detection, protecting specialized tactics, techniques, and procedures (TTPs) to prevent an adversary from developing countermeasures and preventing the adversary from being prepared against a specific operation. As such, secrecy is of utmost importance to special operations.

Surveillance is a countermeasure to secrecy. The more surveillance capability an adversary has, the more it can detect both special and conventional operations.[11] However, too much surveillance can be counterproductive if there are not enough analysts to process the acquired surveillance data. Leveraging AI allows a state to increase its surveillance ability while automating and facilitating the turning of said increased data throughput into decision-quality intelligence. As such, UTS jeopardizes SOF's ability to conduct undetectable operations.

CROSS-DOMAIN IMPACTS OF SURVEILLANCE

Conflict and competition occur today in an increasingly multi-domain and dynamic battle and competition space, often coined as the contemporary or future operating environment.[12] Multi-domain means physical actions on the land, sea, and air can have impacts and are affected by actions in cyber, space and the information domain.

---

[8] Nicholas A. Bredenkamp and Mark Grzegorzewski, "Supporting Resistance Movements in Cyberspace," *Special Operations Journal* 7, no. 1 (January 2, 2021): 19, https://doi.org/10.1080/23296151.2021.1904570.
[9] Robert G. Spulak Jr., "A Theory of Special Operations: The Origin, Qualities, and Use of SOF," *Joint Special Operations University* JSOU Report 07-7 (October 2007): 23–24.
[10] William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice* (Novato, CA: Random House Publishing Group, 1995), 37, https://cfc.overdrive.com/media/212046.
[11] Edward Wolcoff, *Special Reconnaissance and Advanced Small Unit Patrolling: Tactics, Techniques and Procedures for Special Operations Forces*, 1st ed. (Havertown, USA: Pen & Sword Books Limited, 2021), 84, http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=6996018; Edward Wolcoff, *FM 31-20-5 Special Reconnaissance Tactics, Techniques, & Procedures For Special Forces*, 1–10, accessed March 18, 2024, http://archive.org/details/milmanual-fm-31-20-5-special-reconnaissance-tactics-techniques--proced.
[12] Neil Chuka and Heather Hrychuk, "CAF Operations: A Comprehensive Approach to Enable Future Operations," in *Canadian Defence Policy in Theory and Practice*, ed. Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic, Canada and International Affairs (Cham: Springer International Publishing, 2020), 4, https://doi.org/10.1007/978-3-030-26403-1_18; 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.

Surveillance occurs in all these domains.[13] Special operations can be detected through any physical domain, including space, or by actions and reactions occurring in cyberspace or the information domain. That means camouflage and other physical concealment must be as good as digital, information security, and signature management.

IMPACTS TO THE THRESHOLD OF WAR

Another aspect of the contemporary operating environment is the concept of a conflict threshold. Above the threshold are declared hostilities, and below the threshold are activities that are deniable or that individually do not amount to international armed conflict, thus providing enough legal and political ambiguity to avoid international backlash.[14] This is called the grey zone or below-threshold activities. Deniability is diminished if the activity is detected. Discovering an adversary's special operations within another sovereign state could push that activity above the conflict threshold and lead to an international backlash. Therefore, UTS allows a state to detect activities that traditionally were more challenging to detect, defying one of the aspects of the grey zone.

Denying below-threshold activities has positive and negative consequences. On the positive side, it could act as a deterrent. Countries potentially would be less willing to initiate coercive activities if they knew the likelihood of detection, and thus, international repercussions would be much higher.[15] However, that could cause an escalatory effect.[16] A state may determine that a more discreet option is impossible due to UTS; therefore, they would choose a much more aggressive conventional option. Regardless, the ability to monitor extensively and thus deny an adversary a potential means of conflict has a changing characteristic of the contemporary operating environment. As such, UTS must be factored within all SOF operations. As UTS changes the likelihood of SOF detection, the political risk calculus potentially changes. Operationally and tactically, SOF must continue to evolve the way missions are conducted.

UTS' GLOBAL EXPANSION

The Chinese surveillance strategy ensures internal security and insight into its population. It is rooted in technological advancements, sensor proliferation, and data aggregation. The Chinese Communist Party (CCP) has surveillance policies to bolster national security and its perception of social stability.[17] This approach started in the 1990s

---

[13] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, First Trade Paperback Edition (New York: Public Affairs, 2020), 32.
[14] Javier Jordan, "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict," *Journal of Strategic Security* 14, no. 1 (2020): 3–8, https://doi.org/10.5038/1944-0472.14.1.1836; C. Anthony Pfaff, "Military Ethics below the Threshold of War," *U.S. Army War College's Parameters*, Leadership and Innovation, 50, no. 2 (Summer 2020): 2.
[15] Michael Poznansky, "Revisiting Plausible Deniability," *Journal of Strategic Studies* 45, no. 4 (June 7, 2022): 525–26, https://doi.org/10.1080/01402390.2020.1734570.
[16] Costantino Pischedda and Andrew Cheon, "Does Plausible Deniability Work? Assessing the Effectiveness of Unclaimed Coercive Acts in the Ukraine War," *Contemporary Security Policy* 44, no. 3 (July 3, 2023): 351, https://doi.org/10.1080/13523260.2023.2212464.
[17] Susan Trevaskes and Bernot Ausma, "Surveillance Infrastructure in China: Key Concepts and Mechanisms Enhancing the Party-State's Governance Ambitions," *Global Media and China* 8, no. 3 (September 2023): 327–42, https://doi.org/10.1177/20594364231171013; Minxin Pei, *The Sentinel State:*

with closed-circuit television (CCTV) cameras, electronic eavesdropping, and internet monitoring technologies.[18] More recently, these technologies have grown both in number and sophistication. Central to this technological evolution is the widespread use of AI, such as facial recognition, licence plate readers and predictive analysis. These tools, integrated into various aspects of Chinese daily life, empower the CCP to monitor and track individuals extensively, ostensibly to combat crime and maintain social order. This ubiquitous ability to detect and monitor the physical domain also has a national security benefit.

Furthermore, China's surveillance apparatus extends beyond physical spaces to encompass digital realms, enabling comprehensive monitoring of online activities and communications.[19] This comprehensive digital surveillance infrastructure serves domestic governance objectives. It acts as a mechanism to detect adversary actions and as a deterrent against any below-threshold mission.[20] By monitoring physical and virtual domains ubiquitously, China erects formidable A2AD to strategic adversaries, safeguarding its national interests and security.

China is also expanding its UTS capabilities beyond its borders. This strategic effort extends its influence and enhances its international surveillance capabilities. Through the Belt and Road Initiative (BRI), China has been exporting surveillance technologies and expertise to its partner states, fostering deeper economic and strategic ties while simultaneously amplifying its information-gathering and control capacity in those regions. By embedding surveillance infrastructure in foreign countries, China expands its data acquisition and cultivates dependencies among its partners.[21] This approach serves China's geopolitical ambitions by enabling it to exert soft power by providing telecommunication and surveillance technologies, thereby advancing its interests. China is systematically expanding its UTS both within its borders and beyond. It allows the CCP to detect below-threshold activities and serves as a deterrence.

Domestic surveillance isn't limited to China. Many Western countries have surveillance programs that include domestic mandates.[22] For example, the USA conducts various forms of technical surveillance domestically, but the extent to which it can be characterized as ubiquitous is debatable. The U.S. government utilizes multiple surveillance technologies and techniques through agencies such as the National Security

---

Surveillance and the Survival of Dictatorship in China (Cambridge, UK: Harvard University Press, 2024), 131, http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=31074387.

[18] Birol Akduman, "From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance," *International Journal of Social Sciences* 7, no. 28 (May 13, 2023): 12, https://doi.org/10.52096/usbd.7.28.30.

[19] Pei, *The Sentinel State*, 131–54.

[20] Otto C. Fiala, "Resistance Resurgent: Resurrecting a Method of Irregular Warfare in Great Power Competition," *Special Operations Journal* 7, no. 2 (July 3, 2021): 120, https://doi.org/10.1080/23296151.2021.1994746.

[21] Pei, *The Sentinel State*, 232–62.

[22] Santiago Gómez, Daniel Mejía, and Santiago Tobón, "The Deterrent Effect of Surveillance Cameras on Crime," *Journal of Policy Analysis and Management* 40, no. 2 (March 2021): 553–55, https://doi.org/10.1002/pam.22280.

Agency (NSA), the Federal Bureau of Investigation (FBI), and others.[23] These include monitoring electronic communications, such as phone calls, emails, and internet activity, and employing tools like CCTV cameras, facial recognition systems, and license plate readers for physical surveillance. While these surveillance activities are carried out under various legal frameworks and oversight mechanisms, concerns arise as commercial entities also increase their surveillance data holdings, a trend referred to as the privatization of surveillance.[24] Security companies like Nest, owned by Google, or Ring, owned by Amazon, are growing in popularity. Many American urban streets are constantly being filmed via countless doorbell cameras, with these video surveillance streams being uploaded to internet cloud providers. Due to the growing number of vehicles with cameras and aftermarket dashcams, video is constantly recorded for traffic flow, weather monitoring, and physical surveillance in American urban centers. Arguably, it is ubiquitous. This poses a security risk to CANSOFCOM if this data is ever inappropriately sold or stolen.

After 9/11, the Patriot Act was passed to help find and prosecute terrorists. It also provided the US government access to all commercial data held within its territorial state.[25] The US Government can acquire the commercial data held by Nest, Ring and many dashcam companies via a court order. Once they have said physical surveillance data, it can be combined with bulk NSA data collection.[26] Companies like Palantir Technologies market their services to the US Government to aggregate surveillance data and leverage AI for efficiencies.[27] As such, although the US Government does not openly claim it has a domestic UTS program through its ability to compel commercial companies to provide surveillance data and then fuse it to power AI-supported decisions, it essentially has all the elements of a comprehensive UTS program, which poses a future risk to CANSOFCOM if this data were ever inappropriately sold or stolen.

---

[23] "National Security Agency," US Government Department Website, National Security Agency, accessed March 19, 2024, https://www.nsa.gov/about/; "Federal Bureau of Investigation (FBI)," US Government Department Website, Federal Bureau of Investigation, accessed March 19, 2024, https://www.fbi.gov/investigate.

[24] Antti Oulasvirta et al., "Long-Term Effects of Ubiquitous Surveillance in the Home," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Ubicomp '12: The 2012 ACM Conference on Ubiquitous Computing, Pittsburgh Pennsylvania: ACM, 2012), 41–50, https://doi.org/10.1145/2370216.2370224; Sarah Brayne, "The Banality of Surveillance," *Surveillance & Society* 20, no. 4 (December 16, 2022): 374, https://doi.org/10.24908/ss.v20i4.15946.

[25] Christoph Dyllick-Brenzinger, "Patriot Act vs. Privacy - How to Process Canadian Data Independently of U.S. Providers," Corporate Website, *SeaTable* (blog), July 17, 2023, https://seatable.io/en/patriot-act-vs-privacy-canada/; Treasury Board of Canada Government of Canada, "Frequently Asked Questions: USA PATRIOT ACT Comprehensive Assessment Results," Government of Canada, USA PATRIOT ACT Comprehensive Assessment Results, March 28, 2006, https://www.tbs-sct.canada.ca/pubs_pol/gospubs/tbm_128/usapa/faq-eng.asp; Sebastian Rodriguez, "The United States of Surveillance: A Review of America's Mass Surveillance Laws, Programs, and Oversight," *IDEAH, University of Toronto* 3, no. 2 (December 14, 2022): 5, https://doi.org/10.21428/f1f23564.f20c77b2.

[26] Nicholas Gane, Couze Venn, and Martin Hand, "Ubiquitous Surveillance: Interview with Katherine Hayles," *Theory, Culture & Society* 24, no. 7–8 (December 2007): 356, https://doi.org/10.1177/0263276407086405.

[27] "Palantir," Corporate Website, Palantir, accessed March 19, 2024, https://www.palantir.com/.

Like the USA and many other modern nations, Canada employs various forms of domestic technical surveillance for national security and law enforcement. However, describing it as ubiquitous would be an overstatement. The Canadian government utilizes surveillance technologies and techniques such as electronic communications monitoring, video surveillance, and publicly available information on the internet to address security threats and investigate criminal activities. Agencies like the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) are responsible for conducting lawful and warranted surveillance operations within the boundaries of Canadian law and with appropriate oversight mechanisms in place.[28] This surveillance is directed and used to support CSIS or RCMP efforts. Like Americans, Canadians are increasing the number of home and auto cameras. However, unlike the American Patriot Act, nothing in Canada can easily compel commercial entities to provide the Canadian government with surveillance data. Furthermore, data from the RCMP, CSIS, other departments, and commercial entities are not aggregated, nor are AI-powered tools like facial recognition being used. As such, although Canada has domestic surveillance, it is far from a coordinated UTS approach.

Although domestic and allied surveillance could help CANSOFCOM, its growing global pervasiveness is a concern.[29] Should an American data center or Canadian company's systems become compromised, all the images, videos and data collected by these surveillance programs are potentially available for adversaries. While a specific piece of data may have limited value, it could provide a security risk to an operation once combined with other collected data. For example, a collected face of a CANSOFCOM member in uniform in Ottawa could alert a future adversary once that face reappears many years later in an operations area. Secondly, as these technologies are exported, they become more common in other nations, many with less stringent privacy laws. As such, there is a downstream OPSEC risk for CANSOFCOM due to the growth of surveillance by commercial products and domestic surveillance to enable smart homes and safe cities.

WHY DOES CANSOFCOM NEED TO EVOLVE?

CANSOFCOM delivers counterterrorism and other SOF responses domestically and abroad. It excels as a military force capable of operating in the national defence and security nexus within the grey zone of conflict.[30] As UTS capabilities grow in adversarial territories and other potential crisis or conflict zones, CANSOFCOM may not achieve

---

[28] Government of Canada, "Canadian Security Intelligence Service Mandate," Government of Canada Department Website, Canadian Security Intelligence Service Mandate, April 30, 2018, https://www.canada.ca/en/security-intelligence-service/corporate/mandate.html; Government of Canada, "Royal Canadian Mounted Police," Government of Canada Department Website, Royal Canadian Mounted Police, March 18, 2024, https://www.rcmp-grc.gc.ca/en.

[29] Xu Xu, "To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance," *American Journal of Political Science* 65, no. 2 (April 2021): 309–11, https://doi.org/10.1111/ajps.12514; Omar Elharrouss, Noor Almaadeed, and Somaya Al-Maadeed, "A Review of Video Surveillance Systems," *Journal of Visual Communication and Image Representation* 77 (May 2021): 103116, https://doi.org/10.1016/j.jvcir.2021.103116.

[30] Canadian Special Operations Forces DND, "Canadian Special Operations Forces Command," Government of Canada Institutional profile, Canadian Special Operations Forces Command, December 1, 2020, https://www.canada.ca/en/special-operations-forces-command.html.

sufficient security or surprise by its current security posture. If CANSOFCOM wants to remain a 'force of choice,' it must evolve its security practices to ensure its freedom of manoeuvre domestically and globally.

HOW DOES CANSOFCOM NEED TO EVOLVE?

CANSOFCOM must undergo a systematic evolution to defeat adversarial UTS. It must evolve its OPSEC approach to minimize the effectiveness of bulk data collection.[31] Furthermore, how it trains and selects individuals must advance to improve its security-conscious culture. It needs to focus signature management efforts across the physical, electronic, and digital environments. It must implement AI-defeating measures, leverage cyber operations, and prioritize the force development of low signature technologies.

THE UPSTREAM RISK OF BULK DATA COLLECTION

Defeating an adversary's UTS starts with a systematic OPSEC approach to minimizing an adversary's ability to glean intelligence from bulk data collection.[32] This must be done as part of the daily garrison and corporate routines and operations.[33] Reducing the digital connections between DND, CAF, CANSOFCOM, and the SOF members on both a financial and persona front could reduce adversaries' future physical surveillance effectiveness.

Corporations use advertising data to improve marketing schemes, but governments also use it to understand sentiment, social trends, and intelligence.[34] Today, most websites, social media and online platforms use tracking pixels and cookies to monitor users' activities.[35] When a user visits a website, tracking pixels and cookies

---

[31] Bruce Schneir, "Ubiquitous Surveillance and Security," *IEEE Technology and Society Magazine* 34, no. 3 (September 2015): 39–40, https://doi.org/10.1109/MTS.2015.2461232.

[32] Rose Bernard, Gemma Bowsher, and Richard Sullivan, "COVID-19 and the Rise of Participatory SIGINT: An Examination of the Rise in Government Surveillance Through Mobile Applications," *American Journal of Public Health* 110, no. 12 (December 2020): 1780–85, https://doi.org/10.2105/AJPH.2020.305912; H. M. Verhelst, A. W. Stannat, and G. Mecacci, "Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma," *Science and Engineering Ethics* 26, no. 6 (December 2020): 2975–84, https://doi.org/10.1007/s11948-020-00254-w; Vian Bakir, "Freedom or Security? Mass Surveillance of Citizens," in *Handbook of Global Media Ethics*, ed. Stephen J. A. Ward (Cham: Springer International Publishing, 2021), 939–59, https://doi.org/10.1007/978-3-319-32103-5_47; Alex Joel, "Necessity, Proportionality, and Executive Order 14086," *American University Washington College of Law*, Policy Across Borders, May 2023, 24–25.

[33] Cruden, Christopher, "Ubiquitous Technical Surveillance and the Challenges of Military Operations in the Era of Great Power Competition," in *Great Power Cyber Competition: Competing and Winning in the Information Environment* (Oxford, UNITED KINGDOM: Taylor & Francis Group, 2024), 176, http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=31020371.

[34] Masoomali Fatehkia et al., "Using Facebook Advertising Data to Describe the Socio-Economic Situation of Syrian Refugees in Lebanon," *Frontiers in Big Data* 5 (November 30, 2022): 1033530, https://doi.org/10.3389/fdata.2022.1033530; Meng-Lun Wu et al., "Aggregate Two-Way Co-Clustering of Ads and User Data for Online Advertisements: Journal of Information Science & Engineering," *Journal of Information Science & Engineering* 28, no. 1 (January 2012): 83–97.

[35] Garett Sloane, "TikTok Adjusts Ad Business Ahead of Privacy Rules: App Will Lean on Data from within Its Walls for Abetter Picture of Consumers," *Advertising Age* 92, no. 3 (March 22, 2021): 10.

collect data about the user's browsing behaviour, such as pages visited, products viewed, and user actions. This data can be analyzed to infer significant intelligence, such as the individual's location, family and friend networks, social and economic status, employment, hobbies, interests, etc. This bulk advertisement data augments a corporation's understanding of an individual digital persona.[36] This, combined with other surveillance and data collection, can provide valuable intelligence to an adversary. For example, it can give the history or pattern of how CANSOFCOM travels or moves into operations areas. Thus, protecting and disassociating this data with CANSOFCOM members reduces adversarial UTS effectiveness.

The second essential bulk data collection is financial data. Following money has always been critical to associating individuals with each other, determining locations, solving crimes, and gathering intelligence.[37] For example, by collecting data from Brookfield Global Relocation Services (BGRS), an adversary would know personal banking information associated with all CAF members who were posted, where they were posted, information about their family, where they live, etc.[38] Similar, data collection from the DND's travel service, HRG, would indicate when and where individuals are travelling for work.[39] Combined, an adversary would be able to glean who was a member of the CAF, where they were posted, determine travel patterns, travel partners, etc. Furthermore, this data could be combined with social media profiles to gather pictures, which would help corollate facial images to CAF personnel, which can be fed into Facial recognition algorithms. As such, reducing the amount of personal and financial data associated with CANSOFCOM members would reduce an adversary's UTS effectiveness.

Understanding who is a CANSOFCOM member and when and where they are travelling undermines the SOF principle of security. It can also prevent an SOF team from achieving tactical surprise.[40] Two principles must be applied to reduce the risk of bulk collection on individuals. Firstly, when possible, individuals should minimize digital exposure. To maintain a digital security culture within CANSOFCOM, online exposure checks must occur as part of selection and periodic checks. Updates to screening and selection to include digital habits would select new individuals with a digital security mindset who would be open to future training. This underpins the security culture.

---

[36] Lee McGuigan, *Selling the American People: Advertising, Optimization, and the Origins of Adtech*, Distribution Matters (Cambridge, Massachusetts: The MIT Press, 2023), 27–29.
[37] Longbing Cao, Qiang Yang, and Philip S. Yu, "Data Science and AI in FinTech: An Overview," *International Journal of Data Science and Analytics* 12, no. 2 (August 2021): 82, https://doi.org/10.1007/s41060-021-00278-w.
[38] National Defence, "Update: Privacy Breach and Return to Service of BGRS and SIRVA Canada," Government of Canada Announcement, Privacy breach and return to service of BGRS and SIRVA Canada, November 21, 2023, https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2023/11/update-privacy-breach-return-to-service-brookfield-global-relocation-services-sirva-canada.html.
[39] American Express Global Business Travel, "HRG Shared Travel Service Privacy Statement," HRG Corporate Privacy Statement, HRG Shared Travel Service Privacy Statement, accessed March 20, 2024, https://hrg-isuite.com/gcportal/en-ca/Legal/Privacy-Statement.
[40] Cruden, Christopher, "Ubiquitous Technical Surveillance and the Challenges of Military Operations in the Era of Great Power Competition," 1.

"Digital dust" refers to the residual data generated as a by-product of digital interactions, activities, and transactions conducted by individuals online.[41] This term encompasses all data trails accumulated over time across digital platforms, devices, and networks. Digital dust includes metadata, cookies, browsing history, temporary files, cached data, and other remnants of digital interactions that may seem inconsequential but collectively contribute to a broader digital footprint.[42] While individual pieces of digital dust may not contain sensitive or personal information, their aggregation and analysis can yield valuable insights into user behaviour, associations, and trends. Everyone has digital dust; therefore, it must be accepted that CANSOFCOM members have their own dust. However, selecting and maintaining individuals who have less dust and are cognisant of it helps reduce the risk of adversarial UTS.

FROM A 'DIAMOND ON A CUSHION' TO 'A NEEDLE IN A HAYSTACK'

To further challenge adversarial bulk collection programs, CANSOFCOM should reduce its reliance on unclassified governmental systems.[43] CANSOFCOM uses open governmental processes to embed its data only within the overall public service pool. There are currently approximately 270,000 federal public servants.[44] As such, it is easier to glean intelligence from this data pool than if CANSOFCOM used a fully open process that all 40 million Canadian citizens use.[45] For example, booking travel through Expedia with a credit card would allow CANSOFCOM members to better blend in with all other travelling Canadians. The more CANSOFCOM can distance itself digitally from the Government of Canada, the more challenging it would be for an adversary to begin its upstream data collection. Disassociating digital linkage between CANSOFCOM members and the Canadian government challenges pattern finding in bulk data collection, thus making adversarial UTS less effective.

---

[41] Valanarasu, R., "Comparative Analysis for Personality Prediction by Digital Footprints in Social Media," 78–80; L. V. Kapustina, "Digital Footprint Analysis to Develop a Personal Digital Competency-Based Profile," in *Current Achievements, Challenges and Digital Chances of Knowledge Based Economy*, ed. Svetlana Igorevna Ashmarina and Valentina Vyacheslavovna Mantulenko, vol. 133, Lecture Notes in Networks and Systems (Cham: Springer International Publishing, 2021), 591–96, https://doi.org/10.1007/978-3-030-47458-4_68.

[42] Mats Sjöberg et al., "Digital Me: Controlling and Making Sense of My Digital Footprint," in *Symbiotic Interaction*, ed. Luciano Gamberini et al., vol. 9961, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2017), 2, https://doi.org/10.1007/978-3-319-57753-1_14; Isabelle Böhm and Samuel Lolagar, "Open Source Intelligence: Introduction, Legal, and Ethical Considerations," *International Cybersecurity Law Review* 2, no. 2 (December 2021): section 3, https://doi.org/10.1365/s43439-021-00042-7.

[43] Bing Chen et al., "Secret Sharing Based Reversible Data Hiding in Encrypted Images with Multiple Data-Hiders," *IEEE Transactions on Dependable and Secure Computing*, 2020, 978–80, https://doi.org/10.1109/TDSC.2020.3011923; A. K. Singh, "Data Hiding: Current Trends, Innovation and Potential Challenges," *ACM Transactions on Multimedia Computing, Communications, and Applications* 16, no. 3s (October 31, 2020): 1–16, https://doi.org/10.1145/3382772.

[44] Treasury Board of Canada Secretariat, "Population of the Federal Public Service," Government of Canada statistics, April 18, 2011, https://www.canada.ca/en/treasury-board-secretariat/services/innovation/human-resources-statistics/population-federal-public-service.html.

[45] Verhelst, Stannat, and Mecacci, "Machine Learning Against Terrorism," 2976.

CULTURE STARTS WITH INDIVIDUALS

The importance of digital security training must be recognized.[46] It reinforces the security culture and allows for continuous updates to TTPs. This training is essential for all CANSOFCOM members, not just deploying individuals. Many individuals working in force development, sustainment, and management travel and liaise on behalf of the command. This exposure and potential connection with those in operations also pose a risk. Pan-command training would raise the collective floor and help improve the overall security culture. This enhanced security culture will underpin UTS defeat and allow novel UTS defeating TTPs and capabilities to flourish.

SIGNATURE MANAGEMENT

A signature is defined as an object that is distinguishable from its background.[47] This object can be a visual distinction, an electromagnetic spectrum distinction, or a digital distinction. CANSOFCOM and its members have a signature within all three. Reducing digital dust, digital linkages between CANSOFCOM members and the Government, and financial signatures could make the digital signatures only as distinguishable as any other Canadian citizen. Physical and electromagnetic signatures must also be reduced to blend into the background effectively.

Physical signatures occur both at the individual and at the command level. A person's face links them to their identity, and a licence plate links that vehicle to a person or organization. A specific aircraft, like the CV-22 Osprey, with specific tail numbers, can be a distinguishable signature for special operations. In October 2020, a US SOF hostage rescue of US citizen Philip Walton was exposed through an open-source aircraft tracking website.[48] Reducing the digital dust of both helps reduce the distinction of physical signatures in the future. Facial recognition works by matching records with current images. With no historical data, the algorithm cannot accurately match the face with an identity. Similarly, CANSOFCOM's newly acquired CE-145 Vigilance will create a distinguishable physical, electronic, and digital signature.[49] Depending on how it is used for training, it will inevitably create signature data that could jeopardize a future CANSOFCOM operation.

Understanding signature and continuing to factor it into all aspects of planning, both at the corporate level and for operations, would allow for a systematic approach to

---

[46] Eunkyung Kweon et al., "The Utility of Information Security Training and Education on Cybersecurity Incidents: An Empirical Evidence," *Information Systems Frontiers* 23, no. 2 (April 2021): 2, https://doi.org/10.1007/s10796-019-09977-z; Veselin Slavchev, "Using Cyber Ranges in Cybersecurity Management Educational Programmes," *Information & Security: An International Journal* 50 (2021): 3, https://doi.org/10.11610/isij.5007.

[47] Kent Andersson, "On the Military Utility of Spectral Design in Signature Management: A Systems Approach," *National Defense University Press*, 1, 21 (2018): 16.

[48] Cruden, Christopher, "Ubiquitous Technical Surveillance and the Challenges of Military Operations in the Era of Great Power Competition," 175.

[49] Ryan Finnerty, "Canada Takes Delivery of New King Air 350ER-Based Surveillance Aircraft," news releases, Flight Global, March 6, 2024, https://www.flightglobal.com/fixed-wing/canada-takes-delivery-of-new-king-air-350er-based-surveillance-aircraft/157263.article.

managing risk associated with adversarial UTS.[50] Signature management is the practice of manipulating a signature. It starts with understanding its characteristics and how the adversary detects said signal and perceives the changes. Good signature management can deceive an adversary.[51] The harder it is to distinguish the CANSOFCOM signature from any other, the more surprise a SOF team could achieve. Furthermore, if CANSOFCOM could deceive an adversary, it would further enhance its ability to achieve surprise.

Although good signature management could deceive an adversary, its effectiveness in a UTS environment remains questionable, except for potentially small tactical activities. Deception aims to focus an adversary's sensors and attention elsewhere.[52] However, a limited reaction would be achieved if an adversary could detect and process sensor data ubiquitously. Furthermore, the larger and more multidimensional a signature is (like a military plane or a large group of military members with physical, electronic, and digital signatures), the harder it would be to deceive all an adversary's sensors simultaneously.

However, whenever a human is in the decision-making process, there is potential deception that could be used for tactical advantage.[53] If humans are distracted by several false signals, they could ignore a real event. Deception in a UTS environment means having the user perceive a system error.[54] For example, if thousands of incidents are flagged, humans would unlikely have the cognitive capacity to process all flagged incidents, leading to either ignoring future incidents or the systems being adjusted to stop flagging incidents. In this case, deception is achieved by the user focusing its attention on fixing the system. This deception activity could be tactically important and have military utility, but it should only be used once due to the risk of triggering a significant adversarial reaction.

IMPLEMENTING AI-DEFEATING MEASURES

Another way of potentially deceiving UTS is by defeating the AI algorithm. Facial or licence plate spoofing could have tactical benefits.[55] Whether celebrities are looking to avoid paparazzi or SOF operators looking to defeat UTS, there is an emerging desire for facial recognition defeat. Understanding the basics of facial recognition is

---

[50] Cruden, Christopher, "Ubiquitous Technical Surveillance and the Challenges of Military Operations in the Era of Great Power Competition," 178–79.
[51] Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44, no. 3 (January 2020): 6, https://doi.org/10.1162/isec_a_00367.
[52] William S Hefron, "Unconventional Warfare Logistics: Utilizing Networked Non-Standard Approaches and Deception," *Naval Postgraduate School*, Thesis, December 2014, 61–64; Mark Johnson and Jessica Meyeraan, "Military Deception: Hiding the Real - Showing the Fake:" (Fort Belvoir, VA: Defense Technical Information Center, March 7, 2003), 4, https://doi.org/10.21236/ADA421609.
[53] James L. Regens and Charles B. Vandepeer, "Piercing the Veil of Darkness? Deception and Intelligence in Warfare," *Journal of Military and Strategic Studies*, Centre of Military and Strategic Studies, 22, no. 3 (April 25, 2023): 224.
[54] Johnson and Meyeraan, "Military Deception," 13.
[55] Bishal Shrestha et al., "Adversarial Sample Generation and Training Using Geometric Masks for Accurate and Resilient License Plate Character Recognition," *Cornell University Library*, Computer Vision and Pattern Recognition, October 25, 2023, 1, https://doi.org/10.48550/ARXIV.2311.12857.

important to realize how to defeat it. Most facial recognition technology uses the following steps: image collecting, image processing (i.e., detecting the face within the image), feature extraction, feature databasing, and query matching.[56] Any of these phases is a potential vulnerability to facial recognition technology.

Solutions to defeat facial recognition range in complexity. For example, unplugging a camera prevents the first step and is potentially an easy solution for a single CCTV camera, but it is challenging within cities with thousands of cameras.[57] As such, defeating the phase of collecting the image is impractical within a UTS environment. Solutions like flash and camera-disturbing fashion scarfs look to defeat the image processing phase.[58] This technology looks to make detecting a face challenging or impossible. Other anti-facial recognition fashion solutions, like clothing, scarfs, COVID-19 masks, jewelry and hats with faces and face-like objects, aim to defeat the feature extraction process. Essentially, tricking the AI into identifying the real subjects' features creates false or inaccurate data.[59] Lastly, the final phases of databasing and querying would require data to be deleted, corrupted, or changed to prevent the image from being properly correlated to other images.[60] This would potentially require a complex cyber solution.[61] In summary, it is possible to defeat current facial recognition algorithms. Although solutions range in complexity, they must all be institutionalized within CANSOFCOM to have a redundant approach.

Each of these facial recognition defeat options has optimal use cases and benefits but also potential drawbacks. For example, an anti-flash scarf could work in a dimly lit street but would not work in an airport customs situation. Furthermore, each of these actions increases the signature differently. If a cyber-attack to corrupt data is detected, a state would inevitably interrogate the data, potentially increasing the surveillance of suspected individuals. Like deception, defeating a facial recognition algorithm could

---

[56] Emily Wenger et al., "SoK: Anti-Facial Recognition Technology," in *2023 IEEE Symposium on Security and Privacy (SP)* (2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA: IEEE, 2023), 3, https://doi.org/10.1109/SP46215.2023.10179445; Denise Almeida, Konstantin Shmarko, and Elizabeth Lomas, "The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks," *AI and Ethics* 2, no. 3 (August 2022): 377–87, https://doi.org/10.1007/s43681-021-00077-w.

[57] Christopher Flaherty, "The Role of CCTV in Terrorist TTPs: Camera System Avoidance and Targeting," *Small Wars Journal*, September 1, 2015, https://smallwarsjournal.com/jrnl/art/the-role-of-cctv-in-terrorist-ttps-camera-system-avoidance-and-targeting.

[58] ISHU Inc, "ISHU - Technology & Fashion," Corporate Website, ISHU - Technology & Fashion, accessed April 2, 2024, https://theishu.com/.

[59] Irene Calvi, "Countersurveillance Aesthetic: The Role of Fashion in the Reappropriation of Identity," *ZoneModa Journal*, October 26, 2023, 78, https://doi.org/10.6092/ISSN.2611-0563/17936.

[60] Daniel F. Smith, Arnold Wiliem, and Brian C. Lovell, "Face Recognition on Consumer Devices: Reflections on Replay Attacks," *IEEE Transactions on Information Forensics and Security* 10, no. 4 (April 2015): 737, https://doi.org/10.1109/TIFS.2015.2398819.

[61] Zuheng Ming et al., "A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices," *Journal of Imaging* 6, no. 12 (December 15, 2020): 179, https://doi.org/10.3390/jimaging6120139; Kim Zetter, "Popular Surveillance Cameras Open to Hackers, Researcher Says," *Wired*, May 15, 2012, https://www.wired.com/2012/05/cctv-hack/; Richard McPherson, Reza Shokri, and Vitaly Shmatikov, "Defeating Image Obfuscation with Deep Learning," 2016, https://doi.org/10.48550/ARXIV.1609.00408.

cause an adversary to modify their behaviour, so its use must be selective. Once the adversary modifies their behaviour, the effectiveness of future uses becomes questionable. Thus, a systemic approach to when, where, and how to use these technologies is vital for development and implementation.

Like defeating facial recognition, licence plate recognition has tactical benefits for defeating A2AD or as a countersurveillance tool.[62] Many licence plate recognition systems work in a similar step manner to that of facial recognition. The step process includes collecting the image, processing the image (i.e. detecting the licence plate within the image), feature extraction (i.e. extracting the letters and numbers from the licence plate), databasing, and finally, query matching (finding the last time said licence plate was detected).[63] For decades, criminals would swap licence plates to deceive the police. Essentially, this was a manner to defeat query matching. Although this tactic still has benefits, more sophisticated options to corrupt databases and more straightforward options to cover certain characters and flash-dazzling tape also exist to defeat the licence plate recognition system.[64] Like facial recognition, the adversary's reaction to these defeat mechanisms is unknown. Thus, licence plate recognition defeat must also be used systematically and deliberately.

LEVERAGING CYBER OPERATIONS

Cyber operations are another potential option for defeating UTS.[65] Defensive cyber operations can help harden and create resilience. Improving cyber security and hardening critical networks defend against bulk data collection.[66] Furthermore, Content Delivery Network (CDN) can enhance privacy, security, and resilience.

CDNs are distributed networks of servers worldwide to improve the performance and effectiveness of websites and other commercial internet traffic. In essence, placing servers geography close to clients reduces lag. Then, these child servers route traffic back to the main data centers and synchronize as per the available bandwidth.[67] From a security perspective, CDNs essentially wrap corporate traffic, adding to the overall data safeguard. As such, CDNs can help obfuscate digital traffic. For example, military encryption produces a distinctive digital signature, providing an adversary a beacon to

---

[62] Shrestha et al., "Adversarial Sample Generation and Training Using Geometric Masks for Accurate and Resilient License Plate Character Recognition," 2–3.
[63] Parneet Kaur, Yogesh Kumar, and Surbhi Gupta, "Artificial Intelligence Techniques for the Recognition of Multi-Plate Multi-Vehicle Tracking Systems: A Systematic Review," *Archives of Computational Methods in Engineering* 29, no. 7 (November 2022): 4898, https://doi.org/10.1007/s11831-022-09753-4.
[64] John Gilliom, "Struggling with Surveillance: Resistance, Consciousness, and Identity," in *The New Politics of Surveillance and Visibility*, ed. Kevin Haggerty and Richard Ericson, 5 (Toronto, Ontario, Canada: University of Toronto Press, 2005), 111–30, https://doi.org/10.3138/9781442681880-006.
[65] Peter Donaldson, "Cyber-Enabled SOF," *Military Technology* 43, no. 12 (2019): 52–53, https://web-p-ebscohost-com.cfc.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=2&sid=fe01bf5b-a9ce-4291-a091-f565b5ba5e12%40redis.
[66] Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro, "Cyber Security: State of the Art, Challenges and Future Directions," *Cyber Security and Applications* 2 (2024): 1–2, https://doi.org/10.1016/j.csa.2023.100031.
[67] Behrouz Zolfaghari et al., "Content Delivery Networks: State of the Art, Trends, and Future Roadmap," *ACM Computing Surveys* 53, no. 2 (March 31, 2021): 348, https://doi.org/10.1145/3380613.

military assets.[68] Having the military encrypted network within the CDN obfuscates the distinguishable traffic.[69] Although Virtual Private Networks (VPNs) are commonly used, CDNs are only growing. CANSOFCOM must continue to understand its digital signature and the internet's regular pattern wherever it deploys to allow tools like CDN to hide its digital signature. Actively hiding digital signatures is another way CANSOFCOM can look to defeat adversarial UTS.

Further to defensive cyber operations, cyber surveillance and offensive cyber operations can be used to understand an adversary's UTS approach. Similarly, data can be collected on adversaries' UTS systems.[70] This can provide valuable insight into the placement of sensors and the overall system design, which is critical for targeting. Ultimately, adequately synchronized, an offensive cyber operation could disrupt an adversary's UTS capability to allow a tactical activity to occur without triggering alerts. As such, cyber operations are a critical enabler for defeating UTS.

PRIORITIZING UTS-DEFEAT IN FORCE DEVELOPMENT

The systematic approach required for defeating UTS extends beyond tactical and operational improvements. Should CANSOFCOM prioritize systematic UTS defeat, the force development directorate has a considerable role to play.[71] The role of force development and procurement is to reduce digital exposure systematically, prioritize low-signature equipment, and develop signature-reducing technologies and countermeasures like decoys in conjunction with industry.

Reducing exposure prevents adversaries from collecting and understanding what equipment CANSOFCOM owns. As per the earlier example, the telegraphed procurement of CE-145 Vigilance provides adversaries with a distinctive signature. Given the open nature of the procurement, the aircraft specifications can be programmed to be alerted within any adversaries' surveillance system. This is akin to all other large procurements that are telegraphed openly. CANSOFCOM needs to develop and procure a series of

---

[68] Adel A. Ahmed and Omar M. Barukab, "Unforgeable Digital Signature Integrated into Lightweight Encryption Based on Effective ECDH for Cybersecurity Mechanism in Internet of Things," *Processes* 10, no. 12 (December 7, 2022): 1, https://doi.org/10.3390/pr10122631; B. Maruthu Kannan et al., "Secure Communication in IoT-Enabled Embedded Systems for Military Applications Using Encryption," in *2023 2nd International Conference on Edge Computing and Applications (ICECAA)* (2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India: IEEE, 2023), 1,3, https://doi.org/10.1109/ICECAA58104.2023.10212400.

[69] Amit Sahai and Brent Waters, "How to Use Indistinguishability Obfuscation: Deniable Encryption, and More," in *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing* (STOC '14: Symposium on Theory of Computing, New York New York: ACM, 2014), 475–84, https://doi.org/10.1145/2591796.2591825.

[70] Shuo Zhang et al., "A Novel Traffic Obfuscation Technology for Smart Home," *Electronics* 12, no. 16 (August 17, 2023): 3, https://doi.org/10.3390/electronics12163477; Joseph M. Brown and Tanisha M. Fazal, "#SorryNotSorry: Why States Neither Confirm nor Deny Responsibility for Cyber Operations," *European Journal of International Security* 6, no. 4 (November 2021): 412–13, https://doi.org/10.1017/eis.2021.18.

[71] Michael C. Horowitz and Shira Pindyck, "What Is a Military Innovation and Why It Matters," *Journal of Strategic Studies* 46, no. 1 (January 2, 2023): 89–93, https://doi.org/10.1080/01402390.2022.2038572.

concealed technologies for which a future adversary has no historical signature, negating the effectiveness of AI in detecting and matching signatures.

Force development must partner with industry to harness innovative approaches to reducing signatures.[72] Priority funding must be given to technologies and approaches that reduce individual and organizational signatures. This included procuring items to reduce the physical, electronic, and digital signatures of current and future CANSOFCOM capabilities. Furthermore, leveraging the industry could provide a novel approach for which there is no historical CANSOFCOM signature. This means prioritizing signature management and UTS defeat within force development and procurement. Capabilities with low and concealed signatures provide options for force employment with less risk of adversarial UTS detection, thus increasing the likelihood of mission success while reducing risk for those conducting the operations.

Force development and procurement can also enable deception through the procurement of decoys.[73] There is a need for decoys within the physical, electronic, and digital domains. In the physical domain, realistic dummies with sufficiently real-looking faces could be a manner to deceive or distract adversaries' UTS while an operational act occurs. For example, if an individual is declared to be in the country, a dummy with their face could be placed in view of a facial recognition CCTV, allowing them to conduct the operational task. Equally, decoy networks must be developed to ensure the digital signature matches the physical one. Similarly, electronic decoys can confuse or distract adversarial electronic warfare. As such, the force development team within CANSOFCOM plays a critical role in the systematic approach to defeating UTS.

CONCLUSION

CANSOFCOM needs to modernize its security approach according to the technological advances in surveillance to continue its operational success. This paper proves that evolving CANSOFCOM's security approach will provide Canada with below-the-threshold options while protecting its members in operations. This OPSEC evolution requires action institutionally, operationally and by each member. Defeating adversarial UTS requires a systematic approach, starting with minimizing signatures and having options to defeat, deceive, disturb, or degrade an adversary's UTS to enable operational success. As such, CANSOFCOM requires effort within Force Management (i.e. modernize selection and recruiting, personal online digital dust), Force Employment (i.e. modernize TTP and systematic selective use), Force Sustainment (i.e. modernizing existing equipment to reduce signatures) and Force Development (i.e. procuring anti-facial recognition fashion).

---

[72] John Taft, Liz Gormisky, and Joe Mariani, "Special Operations Forces and Great Power Competition: Talent, Technology, and Organizational Change in the New Threat Environment" (Deloitte Center for Government Insights, 2019), 12, https://www2.deloitte.com/content/dam/insights/us/articles/4980_special-operations-forces/DI_special-operations-forces.pdf.

[73] Aden C. Magee, "Counterintelligence Black Swan: KGB Deception, Countersurveillance, and Active Measures Operation," *International Journal of Intelligence and CounterIntelligence* 37, no. 1 (January 2, 2024): 247–50, https://doi.org/10.1080/08850607.2023.2192374.

UTS can be seen as the convergence of technology and surveillance. To that end, UTS will continuously advance in globalization and expand to different domains, different communications infrastructures, more Internet of Things (IoT) and smart devices, and the expansion and maturation of AI use. As such, defeating UTS will continue to be a “cat and mouse” game, but undoubtedly of growing importance to special operations.

It is acknowledged that the pervasive nature of UTS presents privacy risks. UTS’ indiscriminate personal information monitoring raises concerns about eroding privacy and individual freedoms. UTS enables the profiling, tracking, and targeting of individuals based on their behaviour, preferences, and affiliations, leading to the misuse of surveillance data for oppressive purposes by either maligned states or overly powerful corporations. As UTS continues to evolve, public awareness initiatives to protect individuals' privacy rights and ensure accountability and oversight of surveillance activities may need new international legal frameworks and technological safeguards. However, this only becomes effective if all states, non-state actors and especially corporations comply.

CANSOFCOM also has much to gain from exploiting the rapid proliferation of UTS. Harnessing others' efforts to operationalize surveillance provides a cost-effective way to achieve technological overmatch. More research is needed to understand how CANSOFCOM and other government departments can collaborate to leverage the UTS video feeds and data for mutual benefit.

BIBLIOGRAPHY

Admass, Wasyihun Sema, Yirga Yayeh Munaye, and Abebe Abeshu Diro. "Cyber Security: State of the Art, Challenges and Future Directions." *Cyber Security and Applications* 2 (2024): 100031. https://doi.org/10.1016/j.csa.2023.100031.

Ahmed, Adel A., and Omar M. Barukab. "Unforgeable Digital Signature Integrated into Lightweight Encryption Based on Effective ECDH for Cybersecurity Mechanism in Internet of Things." *Processes* 10, no. 12 (December 7, 2022): 2631. https://doi.org/10.3390/pr10122631.

Akduman, Birol. "From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance." *International Journal of Social Sciences* 7, no. 28 (May 13, 2023): 442–69. https://doi.org/10.52096/usbd.7.28.30.

Al-Maksousy, Hassan, and Hussein Abdulhussein. "Robust Visible Digital Stamp for Instant Documents Authentication and Verification." *IOP Conference Series: Materials Science and Engineering* 765 (March 17, 2020): 012071. https://doi.org/10.1088/1757-899X/765/1/012071.

Almeida, Denise, Konstantin Shmarko, and Elizabeth Lomas. "The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks." *AI and Ethics* 2, no. 3 (August 2022): 377–87. https://doi.org/10.1007/s43681-021-00077-w.

American Express Global Business Travel. "HRG Shared Travel Service Privacy Statement." HRG Corporate Privacy Statement. HRG Shared Travel Service Privacy Statement. Accessed March 20, 2024. https://hrg-isuite.com/gcportal/en-ca/Legal/Privacy-Statement.

Andersson, Kent. "On the Military Utility of Spectral Design in Signature Management: A Systems Approach." *National Defense University Press*, 1, 21 (2018): 185.

Anning, Stephen. "Operationalizing Human Security in Contemporary Operating Environment." *The Journal of Intelligence, Conflict, and Warfare* 4, no. 3 (March 8, 2022): 270–74. https://doi.org/10.21810/jicw.v4i3.4208.

Bakir, Vian. "Freedom or Security? Mass Surveillance of Citizens." In *Handbook of Global Media Ethics*, edited by Stephen J. A. Ward, 939–59. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-319-32103-5_47.

Bateman, Aaron. "The KGB and Its Enduring Legacy." *The Journal of Slavic Military Studies* 29, no. 1 (January 2, 2016): 23–47. https://doi.org/10.1080/13518046.2016.1129863.

Bernard, Rose, Gemma Bowsher, and Richard Sullivan. “COVID-19 and the Rise of Participatory SIGINT: An Examination of the Rise in Government Surveillance Through Mobile Applications.” *American Journal of Public Health* 110, no. 12 (December 2020): 1780–85. https://doi.org/10.2105/AJPH.2020.305912.

Böhm, Isabelle, and Samuel Lolagar. “Open Source Intelligence: Introduction, Legal, and Ethical Considerations.” *International Cybersecurity Law Review* 2, no. 2 (December 2021): 317–37. https://doi.org/10.1365/s43439-021-00042-7.

Bontridder, Noémi, and Yves Poullet. “The Role of Artificial Intelligence in Disinformation.” *Data & Policy* 3 (2021). https://doi.org/10.1017/dap.2021.20.

Brayne, Sarah. “The Banality of Surveillance.” *Surveillance & Society* 20, no. 4 (December 16, 2022): 372–78. https://doi.org/10.24908/ss.v20i4.15946.

Bredenkamp, Nicholas A., and Mark Grzegorzewski. “Supporting Resistance Movements in Cyberspace.” *Special Operations Journal* 7, no. 1 (January 2, 2021): 17–28. https://doi.org/10.1080/23296151.2021.1904570.

Brown, Joseph M., and Tanisha M. Fazal. “#SorryNotSorry: Why States Neither Confirm nor Deny Responsibility for Cyber Operations.” *European Journal of International Security* 6, no. 4 (November 2021): 401–17. https://doi.org/10.1017/eis.2021.18.

Calvi, Irene. “Countersurveillance Aesthetic: The Role of Fashion in the Reappropriation of Identity.” *ZoneModa Journal*, October 26, 2023, 75-91 Pages. https://doi.org/10.6092/ISSN.2611-0563/17936.

Cao, Longbing, Qiang Yang, and Philip S. Yu. “Data Science and AI in FinTech: An Overview.” *International Journal of Data Science and Analytics* 12, no. 2 (August 2021): 81–99. https://doi.org/10.1007/s41060-021-00278-w.

Chen, Bing, Wei Lu, Jiwu Huang, Jian Weng, and Yicong Zhou. “Secret Sharing Based Reversible Data Hiding in Encrypted Images with Multiple Data-Hiders.” *IEEE Transactions on Dependable and Secure Computing*, 2020, 1–1. https://doi.org/10.1109/TDSC.2020.3011923.

Chen, Jim Q. “Deception Detection in Cyber Conflicts: A Use Case for the Cybersecurity Strategy Formation Framework.” *International Journal of Cyber Warfare and Terrorism* 6, no. 3 (July 1, 2016): 31–42. https://doi.org/10.4018/IJCWT.2016070103.

Christopher Flaherty. “The Role of CCTV in Terrorist TTPs: Camera System Avoidance and Targeting.” *Small Wars Journal*, September 1, 2015. https://smallwarsjournal.com/jrnl/art/the-role-of-cctv-in-terrorist-ttps-camera-system-avoidance-and-targeting.

Chuka, Neil, and Heather Hrychuk. “CAF Operations: A Comprehensive Approach to Enable Future Operations.” In *Canadian Defence Policy in Theory and Practice*, edited by Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic, 313–30. Canada and International Affairs. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-26403-1_18.

Cruden, Christopher. “Ubiquitous Technical Surveillance and the Challenges of Military Operations in the Era of Great Power Competition.” In *Great Power Cyber Competition: Competing and Winning in the Information Environment*, 173–84. Oxford, UNITED KINGDOM: Taylor & Francis Group, 2024. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=31020371.

Defence, National. “Update: Privacy Breach and Return to Service of BGRS and SIRVA Canada.” Government of Canada Announcement. Privacy breach and return to service of BGRS and SIRVA Canada, November 21, 2023. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2023/11/update-privacy-breach-return-to-service-brookfield-global-relocation-services-sirva-canada.html.

DND, Canadian Special Operations Forces. “Canadian Special Operations Forces Command.” Government of Canada Institutional profile. Canadian Special Operations Forces Command, December 1, 2020. https://www.canada.ca/en/special-operations-forces-command.html.

Donaldson, Peter. “Cyber-Enabled SOF.” *Military Technology* 43, no. 12 (2019). https://web-p-ebscohost-com.cfc.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=2&sid=fe01bf5b-a9ce-4291-a091-f565b5ba5e12%40redis.

Dyllick-Brenzinger, Christoph. “Patriot Act vs. Privacy - How to Process Canadian Data Independently of U.S. Providers.” Corporate Website. *SeaTable* (blog), July 17, 2023. https://seatable.io/en/patriot-act-vs-privacy-canada/.

Edward Wolcoff. *FM 31-20-5 Special Reconnaissance Tactics, Techniques, & Procedures For Special Forces*. Accessed March 18, 2024. http://archive.org/details/milmanual-fm-31-20-5-special-reconnaissance-tactics-techniques--proced.

Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. “A Review of Video Surveillance Systems.” *Journal of Visual Communication and Image Representation* 77 (May 2021): 103116. https://doi.org/10.1016/j.jvcir.2021.103116.

Emily Spencer. *"In Pursuit of Excellence": SOF Leadership in the Contemporry Operating Environment*. 1st ed. Winnipeg, Canada: 17 Wing Winnipeg Publishing Office, 2017. https://canadacommons-ca.cfc.idm.oclc.org/artifacts/1196550/in-pursuit-of-excellence/1749674/view/.

Fatehkia, Masoomali, Zinnya Del Villar, Till Koebe, Emmanuel Letouzé, Andres Lozano, Roaa Al Feel, Fouad Mrad, and Ingmar Weber. "Using Facebook Advertising Data to Describe the Socio-Economic Situation of Syrian Refugees in Lebanon." *Frontiers in Big Data* 5 (November 30, 2022): 1033530. https://doi.org/10.3389/fdata.2022.1033530.

Federal Bureau of Investigation. "Federal Bureau of Investigation (FBI)." US Government Department Website. Accessed March 19, 2024. https://www.fbi.gov/investigate.

Fiala, Otto C. "Resistance Resurgent: Resurrecting a Method of Irregular Warfare in Great Power Competition." *Special Operations Journal* 7, no. 2 (July 3, 2021): 109–35. https://doi.org/10.1080/23296151.2021.1994746.

Gaire, Utsav Sharma. "Application of Artificial Intelligence in the Military: An Overview." *Unity Journal* 4, no. 01 (February 15, 2023): 161–74. https://doi.org/10.3126/unityj.v4i01.52237.

Gane, Nicholas, Couze Venn, and Martin Hand. "Ubiquitous Surveillance: Interview with Katherine Hayles." *Theory, Culture & Society* 24, no. 7–8 (December 2007): 349–58. https://doi.org/10.1177/0263276407086405.

Gilliom, John. "Struggling with Surveillance: Resistance, Consciousness, and Identity." In *The New Politics of Surveillance and Visibility*, edited by Kevin Haggerty and Richard Ericson, 111–30. 5. Toronto, Ontario, Canada: University of Toronto Press, 2005. https://doi.org/10.3138/9781442681880-006.

Gómez, Santiago, Daniel Mejía, and Santiago Tobón. "The Deterrent Effect of Surveillance Cameras on Crime." *Journal of Policy Analysis and Management* 40, no. 2 (March 2021): 553–71. https://doi.org/10.1002/pam.22280.

Gooch, John and Amos Perlmutter, eds. *Military Deception and Strategic Surprise!* 0 ed. London, UK: Routledge, 2012. https://doi.org/10.4324/9780203043394.

Government of Canada. "Canadian Security Intelligence Service Mandate." Government of Canada Department Website. Canadian Security Intelligence Service Mandate, April 30, 2018. https://www.canada.ca/en/security-intelligence-service/corporate/mandate.html.

Government of Canada. “Royal Canadian Mounted Police.” Government of Canada Department Website. Royal Canadian Mounted Police, March 18, 2024. https://www.rcmp-grc.gc.ca/en.

Government of Canada, Treasury Board of Canada. “Frequently Asked Questions: USA PATRIOT ACT Comprehensive Assessment Results.” Government of Canada. USA PATRIOT ACT Comprehensive Assessment Results, March 28, 2006. https://www.tbs-sct.canada.ca/pubs_pol/gospubs/tbm_128/usapa/faq-eng.asp.

Green, Brendan Rittenhouse, and Austin Long. “Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition.” *International Security* 44, no. 3 (January 2020): 48–83. https://doi.org/10.1162/isec_a_00367.

Gruber, Craig W., Benjamin Trachik, Catherine Kirby, Sara Dalpe, Lila Silverstein, Siobhan Frey, and Brendon W. Bluestein. *Fostering Innovation in the Intelligence Community: Scientifically-Informed Solutions to Combat a Dynamic Threat Environment*. Cham, Switzerland: Springer International Publishing AG, 2023. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=30684902.

Hanson, Peter, Lucas Truax, and David D. Saranchak. “IOT Honeynet for Military Deception and Indications and Warnings.” In *Autonomous Systems: Sensors, Vehicles, Security, and the Internet of Everything*, edited by Michael C. Dudzik and Jennifer C. Ricklin, 48. Orlando, United States: SPIE, 2018. https://doi.org/10.1117/12.2305071.

Hefron, William S. “Unconventional Warfare Logistics: Utilizing Networked Non-Standard Approaches and Deception.” *Naval Postgraduate School*, Thesis, December 2014, 125.

Horn, Colonel Bernd. “When Cultures Collide: The Conventional Military / SOF Chasm.” *Canadian Military Journal* Autumn 2004 (2004): 14.

Horowitz, Michael C., and Shira Pindyck. “What Is a Military Innovation and Why It Matters.” *Journal of Strategic Studies* 46, no. 1 (January 2, 2023): 85–114. https://doi.org/10.1080/01402390.2022.2038572.

ISHU Inc. “ISHU - Technology & Fashion.” Corporate Website. ISHU - Technology & Fashion. Accessed April 2, 2024. https://theishu.com/.

James L. Regens and Charles B. Vandepeer. “Piercing the Veil of Darkness? Deception and Intelligence in Warfare.” *Journal of Military and Strategic Studies*, Centre of Military and Strategic Studies, 22, no. 3 (April 25, 2023): 221–50.

Joel, Alex. “Necessity, Proportionality, and Executive Order 14086.” *American University Washington College of Law*, Policy Across Borders, May 2023, 34.

John Taft, Liz Gormisky, and Joe Mariani. “Special Operations Forces and Great Power Competition: Talent, Technology, and Organizational Change in the New Threat Environment.” Deloitte Center for Government Insights, 2019. https://www2.deloitte.com/content/dam/insights/us/articles/4980_special-operations-forces/DI_special-operations-forces.pdf.

Johnson, Mark, and Jessica Meyeraan. “Military Deception: Hiding the Real - Showing the Fake:” Fort Belvoir, VA: Defense Technical Information Center, March 7, 2003. https://doi.org/10.21236/ADA421609.

Jordan, Javier. “International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict.” *Journal of Strategic Security* 14, no. 1 (2020): 1–24. https://doi.org/10.5038/1944-0472.14.1.1836.

Josh Golding. “Byte, With, and Through: How Special Operations and Cyber Command Can Support Each Other.” Commentary. War on the Rocks, November 11, 2022. https://warontherocks.com/2022/11/byte-with-and-through-how-special-operations-and-cyber-command-can-support-each-other/.

Kannan, B. Maruthu, P. Solainayagi, H. Azath, Subbiah Murugan, and C. Srinivasan. “Secure Communication in IoT-Enabled Embedded Systems for Military Applications Using Encryption.” In *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 1385–89. Namakkal, India: IEEE, 2023. https://doi.org/10.1109/ICECAA58104.2023.10212400.

Kapustina, L. V. “Digital Footprint Analysis to Develop a Personal Digital Competency-Based Profile.” In *Current Achievements, Challenges and Digital Chances of Knowledge Based Economy*, edited by Svetlana Igorevna Ashmarina and Valentina Vyacheslavovna Mantulenko, 133:591–96. Lecture Notes in Networks and Systems. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-47458-4_68.

Karampelas, Panagiotis, and Thirimachos Bourlai, eds. *Surveillance in Action: Technologies for Civilian, Military and Cyber Surveillance*. Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-68533-5.

Kaur, Parneet, Yogesh Kumar, and Surbhi Gupta. “Artificial Intelligence Techniques for the Recognition of Multi-Plate Multi-Vehicle Tracking Systems: A Systematic Review.” *Archives of Computational Methods in Engineering* 29, no. 7 (November 2022): 4897–4914. https://doi.org/10.1007/s11831-022-09753-4.

Kim, Young-il, Yeo Geon Min, Park Seong Hee, Jeong Wun-Cheol, Song Soonyong, and Heo Tae-Wook. “The Analysis of Image Acquisition Method for Anti-UAV Surveillance Using Cameras Image.” In *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 549–54. Jeju, Korea (South): IEEE, 2020. https://doi.org/10.1109/ICTC49870.2020.9289164.

Kweon, Eunkyung, Hansol Lee, Sangmi Chai, and Kyeongwon Yoo. “The Utility of Information Security Training and Education on Cybersecurity Incidents: An Empirical Evidence.” *Information Systems Frontiers* 23, no. 2 (April 2021): 361–73. https://doi.org/10.1007/s10796-019-09977-z.

Larry Wortzel. “Chinese Expectations for Biotechnology And Cognitive Enhancement in Future Warfare.” *Modern War Institute at Westpoint Academy*, MWI Report, 1 (September 2022): 24.

Lonergan, Erica D., and Shawn W. Lonergan. “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises.” *Security Studies* 31, no. 1 (January 1, 2022): 32–64. https://doi.org/10.1080/09636412.2022.2040584.

Magee, Aden C. “Counterintelligence Black Swan: KGB Deception, Countersurveillance, and Active Measures Operation.” *International Journal of Intelligence and CounterIntelligence* 37, no. 1 (January 2, 2024): 232–64. https://doi.org/10.1080/08850607.2023.2192374.

McGuigan, Lee. *Selling the American People: Advertising, Optimization, and the Origins of Adtech*. Distribution Matters. Cambridge, Massachusetts: The MIT Press, 2023.

McPherson, Richard, Reza Shokri, and Vitaly Shmatikov. “Defeating Image Obfuscation with Deep Learning,” 2016. https://doi.org/10.48550/ARXIV.1609.00408.

Meng-Lun Wu, Chia-Hui Chang, Rui-Zhe Liu, and Teng-Kai Fan. “Aggregate Two-Way Co-Clustering of Ads and User Data for Online Advertisements: Journal of Information Science & Engineering.” *Journal of Information Science & Engineering* 28, no. 1 (January 2012): 83–97.

Miah Hammond-Errey. “Big Data and National Security: A Guide for Australian Policymakers.” *Lowry Institute*, February 1, 2022. https://www.lowyinstitute.org/publications/big-data-national-security-guide-australian-policymakers.

Ming, Zuheng, Muriel Visani, Muhammad Muzzamil Luqman, and Jean-Christophe Burie. “A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices.” *Journal of Imaging* 6, no. 12 (December 15, 2020): 139. https://doi.org/10.3390/jimaging6120139.

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.

National Security Agency. “National Security Agency.” US Government Department Website. Accessed March 19, 2024. https://www.nsa.gov/about/.

Norris, Clive, and Gary Armstrong. *The Maximum Surveillance Society: The Rise of CCTV*. 1st ed. Routledge, 2020. https://doi.org/10.4324/9781003136439.

Oulasvirta, Antti, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. “Long-Term Effects of Ubiquitous Surveillance in the Home.” In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 41–50. Pittsburgh Pennsylvania: ACM, 2012. https://doi.org/10.1145/2370216.2370224.

Palantir. “Palantir.” Corporate Website. Accessed March 19, 2024. https://www.palantir.com/.

Pei, Minxin. *The Sentinel State: Surveillance and the Survival of Dictatorship in China*. Cambridge, UK: Harvard University Press, 2024. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=31074387.

Pfaff, C. Anthony. “Military Ethics below the Threshold of War.” *U.S. Army War College’s Parameters*, Leadership and Innovation, 50, no. 2 (Summer 2020): 69–76.

Pischedda, Costantino, and Andrew Cheon. “Does Plausible Deniability Work? Assessing the Effectiveness of Unclaimed Coercive Acts in the Ukraine War.” *Contemporary Security Policy* 44, no. 3 (July 3, 2023): 345–71. https://doi.org/10.1080/13523260.2023.2212464.

Poznansky, Michael. “Revisiting Plausible Deniability.” *Journal of Strategic Studies* 45, no. 4 (June 7, 2022): 511–33. https://doi.org/10.1080/01402390.2020.1734570.

Raska, Michael. “The Sixth RMA Wave: Disruption in Military Affairs?” *Journal of Strategic Studies* 44, no. 4 (June 7, 2021): 456–79. https://doi.org/10.1080/01402390.2020.1848818.

Robert G. Spulak Jr. “A Theory of Special Operations: The Origin, Qualities, and Use of SOF.” *Joint Special Operations University* JSOU Report 07-7 (October 2007): 63.

Rodriguez, Sebastian. “The United States of Surveillance: A Review of America’s Mass Surveillance Laws, Programs, and Oversight.” *IDEAH, University of Toronto* 3, no. 2 (December 14, 2022): 19. https://doi.org/10.21428/f1f23564.f20c77b2.

Ryan Finnerty. “Canada Takes Delivery of New King Air 350ER-Based Surveillance Aircraft.” News releases. Flight Global, March 6, 2024. https://www.flightglobal.com/fixed-wing/canada-takes-delivery-of-new-king-air-350er-based-surveillance-aircraft/157263.article.

Sahai, Amit, and Brent Waters. “How to Use Indistinguishability Obfuscation: Deniable Encryption, and More.” In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, 475–84. New York New York: ACM, 2014. https://doi.org/10.1145/2591796.2591825.

Sanchez, Sergio. “Ubiquitous Technical Surveillance: Counterintelligence Bliss, or Nightmare?” Master of Science of Strategic Intelligence Thesis, National Intelligence University, 2020. https://doi.org/10.13140/RG.2.2.23516.16002.

Șcheau, Mircea Constantin, Monica Violeta Achim, Larisa Găbudeanu, Iulia Brici, and Alexandru-Lucian Vîlcea. “Legal, Economic and Cyber Security Framework Considerations for Drone Usage.” *Applied Sciences* 12, no. 9 (May 6, 2022): 4663. https://doi.org/10.3390/app12094663.

Schmidt, Eric. “AI, Great Power Competition & National Security.” *Daedalus* 151, no. 2 (May 1, 2022): 288–98. https://doi.org/10.1162/daed_a_01916.

Schneir, Bruce. “Ubiquitous Surveillance and Security.” *IEEE Technology and Society Magazine* 34, no. 3 (September 2015): 39–40. https://doi.org/10.1109/MTS.2015.2461232.

Government of Canada. Treasury Board of Canada Secretariat. “Population of the Federal Public Service.” Government of Canada statistics, April 18, 2011. https://www.canada.ca/en/treasury-board-secretariat/services/innovation/human-resources-statistics/population-federal-public-service.html.

Shrestha, Bishal, Griwan Khakurel, Kritika Simkhada, and Badri Adhikari. “Adversarial Sample Generation and Training Using Geometric Masks for Accurate and Resilient License Plate Character Recognition.” *Cornell University Library*, Computer Vision and Pattern Recognition, October 25, 2023, 10. https://doi.org/10.48550/ARXIV.2311.12857.

Singh, A. K. “Data Hiding: Current Trends, Innovation and Potential Challenges.” *ACM Transactions on Multimedia Computing, Communications, and Applications* 16, no. 3s (October 31, 2020): 1–16. https://doi.org/10.1145/3382772.

Sjöberg, Mats, Hung-Han Chen, Patrik Floréen, Markus Koskela, Kai Kuikkaniemi, Tuukka Lehtiniemi, and Jaakko Peltonen. “Digital Me: Controlling and Making Sense of My Digital Footprint.” In *Symbiotic Interaction*, edited by Luciano Gamberini, Anna Spagnolli, Giulio Jacucci, Benjamin Blankertz, and Jonathan Freeman, 9961:155–67. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-57753-1_14.

Slavchev, Veselin. “Using Cyber Ranges in Cybersecurity Management Educational Programmes.” *Information & Security: An International Journal* 50 (2021): 161–68. https://doi.org/10.11610/isij.5007.

Sloane, Garett. “TikTok Adjusts Ad Business Ahead of Privacy Rules: App Will Lean on Data from within Its Walls for Abetter Picture of Consumers.” *Advertising Age* 92, no. 3 (March 22, 2021): 10.

Smith, Daniel F., Arnold Wiliem, and Brian C. Lovell. “Face Recognition on Consumer Devices: Reflections on Replay Attacks.” *IEEE Transactions on Information Forensics and Security* 10, no. 4 (April 2015): 736–45. https://doi.org/10.1109/TIFS.2015.2398819.

Steingartner, William, Darko Galinec, and Andrija Kozina. “Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model.” *Symmetry* 13, no. 4 (April 3, 2021): 597. https://doi.org/10.3390/sym13040597.

Tebedo, Jason C. “Special Operations And Cyber Warfare.” Edited by Dorothy Denning. *Naval Postgraduate School*, December 2016, 77.

Trevaskes, Susan, and Bernot Ausma. “Surveillance Infrastructure in China: Key Concepts and Mechanisms Enhancing the Party-State’s Governance Ambitions.” *Global Media and China* 8, no. 3 (September 2023): 327–42. https://doi.org/10.1177/20594364231171013.

Valanarasu, R. “Comparative Analysis for Personality Prediction by Digital Footprints in Social Media.” *Journal of Information Technology and Digital World* 3, no. 2 (May 31, 2021): 77–91. https://doi.org/10.36548/jitdw.2021.2.002.

Verhelst, H. M., A. W. Stannat, and G. Mecacci. “Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma.” *Science and Engineering Ethics* 26, no. 6 (December 2020): 2975–84. https://doi.org/10.1007/s11948-020-00254-w.

Wenger, Emily, Shawn Shan, Haitao Zheng, and Ben Y. Zhao. “SoK: Anti-Facial Recognition Technology.” In *2023 IEEE Symposium on Security and Privacy (SP)*, 864–81. San Francisco, CA, USA: IEEE, 2023. https://doi.org/10.1109/SP46215.2023.10179445.

William H. McRaven. *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice*. Novato, CA: Random House Publishing Group, 1995. https://cfc.overdrive.com/media/212046.

Wolcoff, Edward. *Special Reconnaissance and Advanced Small Unit Patrolling: Tactics, Techniques and Procedures for Special Operations Forces*. 1st ed. Havertown, USA: Pen & Sword Books Limited, 2021. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=6996018.

Xu, Xu. "To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance." *American Journal of Political Science* 65, no. 2 (April 2021): 309–25. https://doi.org/10.1111/ajps.12514.

Zetter, Kim. "Popular Surveillance Cameras Open to Hackers, Researcher Says." *Wired*, May 15, 2012. https://www.wired.com/2012/05/cctv-hack/.

Zhang, Shuo, Fangyu Shen, Yaping Liu, Zhikai Yang, and Xinyu Lv. "A Novel Traffic Obfuscation Technology for Smart Home." *Electronics* 12, no. 16 (August 17, 2023): 3477. https://doi.org/10.3390/electronics12163477.

Zolfaghari, Behrouz, Gautam Srivastava, Swapnoneel Roy, Hamid R. Nemati, Fatemeh Afghah, Takeshi Koshiba, Abolfazl Razi, Khodakhast Bibak, Pinaki Mitra, and Brijesh Kumar Rai. "Content Delivery Networks: State of the Art, Trends, and Future Roadmap." *ACM Computing Surveys* 53, no. 2 (March 31, 2021): 1–34. https://doi.org/10.1145/3380613.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First Trade Paperback Edition. New York: Public Affairs, 2020.