National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

FROM COMMON OPERATING PICTURE TO COMMON OPERATING SYSTEM

Major Ian Watt

JCSP 44

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 44

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 44 – PCEMI 44
2017 – 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

FROM COMMON OPERATING PICTURE TO COMMON OPERATING SYSTEM

By Major Ian Watt

FROM COMMON OPERATING PICTURE TO COMMON OPERATING SYSTEM

Introduction

Many commanders, officers, observers and pundits have identified over a sustained period of time that leveraging the variety of information sources on the modern battlefield to develop a cohesive common operating picture has been a challenge[1]. In particular, many will cite that the problem is no longer getting the data and information but now it is organizing it so it can be understood in a reasonable amount of time. Some have indicated that this task is too daunting and unachievable such that it cannot be reasonably done with the current approaches in place[2]. However, it will be argued that it is possible to develop a common operating system that links and exploits all elements and data of a force. First, the framework of what such a system might be will be briefly discussed to provide an understanding of the basic concept short of detailed technical examination. Then how possible first, second and third levels of the system might be implemented will be outlined. Finally, key obstacles to creating a system will be identified along with potential mitigations for overcoming those obstacles.

Framework

A detailed technical examination of a common operating system is beyond the scope of this paper with an initial technical architecture likely to take hundreds or thousands of hours to initiate, design and develop[3]. However, the higher-level framework and key ideas behind a common operating system are important to understanding that it would be possible to implement. Firstly, the term "common operating system" in this case implies the set of key functions and

[1] Chris Young, *Military Intelligence Redefined: Big Data in the Battlefield* (Forbes, March 2012).
[2] Aaron Mehta, *Pentagon tech advisers target how the military digests data* (DefenceNews April 2017).
[3] Michael Bloch, Sven Blumberg, and Jürgen Laartz, *Delivering large-scale IT projects on time, on budget, and on value* (McKinsey, October 2012).

relationships that allow for the system to be created. This does not necessarily imply that it would replace an existing operating system such as windows or Linux nor does it imply that it would not. That is tangential to the core elements and would be deduced during technical planning. Instead, in this case "common operating system" implies a common system where all data and information can be gathered and subsequently accessed for various purposes. With that as the basic premise, a critical element of the system is common and uniform data structures. There are many types of data such a system would have to manage including video, images, various types of reports, various forms, audio and different languages among many others. A critical element of the system would be uniform and defined data rules such that data of the same type is stored and handled the same way[4], much like operating systems have rules that data must conform to. The particular emphasis of this system is military data, with data structures defined in such a way that provides clear and as simple as possible rules for standardization. While it is difficult to know without doing a complete analysis what the starting set of data structures and standards would be, it is reasonable to assume it would cover the aforementioned types of data among others at a minimum. As important as standard data structures is a standard way to define new data structures along with a method to ensure that new data structures are not duplicating or approximating existing data structures. This is important to ensure that the system can be improved on a fundamental level from a predetermined start state. This also ensures the system will not be overly complicated in the long run as it becomes too convoluted and complex to maintain the purpose and utility originally intended. Of further importance to such a system are the security and access controls. As the system would fundamentally be a military system with life and death importance, security of the system would be paramount. Unlike some existing

[4] Rohit Jain, *It's time to establish big data standards: The deployment of big data tools is being held back by the lack of standards in a number of growth areas* (O'Reilly, August 2018).

frameworks and protocols which leave connections and access open unless otherwise restricted, this system would leave connections and access closed unless otherwise granted through software defined access by a well designed software define network[5]. While there are many more security considerations beyond the scope of this paper this fundamental approach would go a long way to ensuring the system remains secure. Further is that while many sensors, people and devices might be able to put various types of data into the system, accessing and utilizing the data in the system would be less common. Access would be restricted both by automation controls and by human review for any new device, sub-system, module or similar such that it would have access to only the data required to perform its clearly defined function. Overall, critical to the framework is carefully analysed and implemented common data structures, a defined method for creating new data structures, an authorization process for ensuring new data structures are not duplicating or approximating existing data structures, a closed security posture, a system and human reviewed data access approach and a limitation to access for purpose are the critical elements of the overall common operating system framework. This forms the basis, which can be built upon to provide significant utility to the total force. We now turn to how this utility can be put into place.

First Level Development

With a common framework in place to build upon, the first level of utility could be developed. It is worth pointing out that a key approach to developing and leveraging the system is incrementally based, with key sets of functionality being developed in small steps rather than large systems implementation[6]. This helps to avoid large missteps that can occur with large-

[5] Scott Fulton, *What is SDN? How software-defined networking changed everything* (ZDNet, May 2018).
[6] New Line Technologies, *Incremental Model of Software Development Life Cycle* (January 2018).

scale systems implementation such as those recently experienced during the implementation of the Phoenix pay system[7]. The first series of steps to be taken with the system is getting all existing sensors to input data into the system for future use. With the common framework outlined each individual sensor would then need some development work completed, similar to developing device drivers[8], that enables the data gathered by the sensor to be entered into the common system. Likewise, integrations[9] with existing information systems and other forms that collect human inputs such as orders, emails, intelligence reports, movement reports and contact reports among many others would have to be developed according to the common framework. While each integration or development for existing sensors would be a small effort, the total effort would be significant[10]. However, the key to successful implementation is the incremental approach with each step being easy to process and manage with limited room for failure[11]. With existing devices and information systems enabled to input information to the common system, a standard for new equipment, capabilities and modules would be put in place so that any new capabilities in development could account for integration. In turn, this ensures that the system remains current with technology advancement and continues to include relevant data. With all data entered into a common system and continually updated by active sensors and information systems the baseline data could then be utilized in a consolidated manner. A likely first effort would be to develop a superior common operating picture based on the input of all available sensors and information systems. This would likewise be achieved in an incremental manner. An incremental approach might first include building modules that identify relevant data for the common operating picture, then modules that prioritize and eliminate conflicts that might arise

[7] CBC News, *Phoenix pay system cost could total $2.6B before cheaper replacement ready* (May 2019).
[8] Tammy Noergaard, *Embeded Systems Architecture: Chapter 8 Device Drivers* (Newnes, 2013).
[9] CIO Whitepapers Review, *What is Software Integration* (2018).
[10] Niall McCarthy, *Europe Has Six Times As Many Weapon Systems As The U.S.* (Forbes, 2018).
[11] New Line Technologies, *Incremental Model . . .*

between different data sources and then modules that provide statistical analysis to determine confidence levels in various elements of the common operating picture. While there would more than likely be other steps as well as more detailed increments[12], the key is that a common operating picture output is developed incrementally in sizeable steps to reduce risk in implementation[13]. Further, it should be noted that developing system capabilities might require additional data structures but these would in turn be developed and approved according to the initially defined approach.

Second Level Development

With the system built, data gathered and the initial utility of the system to provide a common operating picture established, second level implementations can be considered. Such a system would undoubtedly cost a significant amount to build and subsequently maintain, potentially ranging into billions of dollars over time[14]. A cost benefit analysis of the system could possibly result in a low prioritization relative to other capabilities[15] leading to the system never being built in the first place, or not being maintained and utilized once it was built. At the core of the framework and the system development is the solution to this issue. Each incremental step is not likely to be individually costly and is low risk due to the incremental paradigm[16]. Costs to build and maintain the system can therefore be spread out both over capabilities and over time. Further, rather than procuring an omnibus common operating picture or other functionality, small

[12] Nancy Jones-Bonbrest, *U.S. Army's common operating picture tool continues to evolve* (U.S. Army, December 2012).
[13] New Line Technologies, *Incremental Model . . .*
[14] Government Accountability Office, *Weapon System Sustainment: DOD Needs to Better Capture and Report Software Sustainment Costs* (United States Government Accountability Office, February 2019), 1.
[15] Government Accountability Office, *ARMY MODERNIZATION: Steps Needed to Ensure Army Futures Command Fully Applies Leading Practices* (United States Government Accountability Office, January 2019), 7-8.
[16] New Line Technologies, *Incremental Model . . .*

steps can be procured to reduce costs. Also many modules could be competitively contracted to reduce costs and spread across multiple contractors to meet various industrial regional benefit policy requirements[17]. This can be leveraged in the case of military alliances, such as NATO, in a number of ways. Firstly, incremental developments can be spread across members of the alliance, with each member nation being responsible for component parts of the system or parts of the incremental development of the system. Further, each member nation of an alliance would be responsible for the development for its own links to the system for each of its own sensor platforms and information systems, spreading the costs more. Additionally, each nation could also build additional functionality beyond common operating picture functions to suit its own purpose which it could then choose to extend to other nations if appropriate. This highlights a further advantage of the system that makes it possible to build and maintain. Specifically, nations can use the same base system, potentially with the same base data, and build and use their own module and capabilities on top of the system which may only be accessible by that nation[18]. This approach can also be extended to the underlying data with nations augmenting the base data with their own data managed in a similar method[19] but only accessible by that nation to ensure secrecy and security of data conducive with that nation's preference and intelligence sharing parameters[20]. With the conditions set by the common system framework, in particular the closed access paradigm, controlling use of the system by members in an alliance becomes straightforward. Together this eliminates obstacles to implementation stemming from costs,

[17] Government of Canada, *Industrial and Technological Benefits: Policy Features: Investment Framework Guidelines* (April 2019).
[18] Wout Hofman and Madan Rajagopal, *A Technical Framework for Data Sharing* (Journal of theoretical and applied electronic commerce research, 2014), 1.
[19] Ibid.
[20] NATO Library, *Intelligence/Information Sharing in Combating Terrorism* (NATO Multimedia Library, May 2019).

common use throughout an alliance as well as data control in accordance with national preferences. This in turn sets the conditions for a third level implementation of the system.

Third Level Development

A third level of implementation of the common operating system would take advantage of advances in technology and future trends. With both a pool of current data from an operating environment and over time an extensive pool of historical data from operating environments the conditions would be set for artificial intelligence to be developed[21]. Much like other developments of the system any artificial intelligence capabilities would be developed incrementally and most likely build upon each other. It would be reasonable to expect decision aids[22] and some automation[23] of decisions to be developed with exact scope to be determined. These decisions aids could process vast amounts of current and historical data to provide recommendations based on automated analysis and scenario simulation to commanders facing various types of decisions. These might include targeting decisions, operational options considerations and decisions that have legal and political ramifications among many others that commanders routinely face. As the decision aids would be based on historical information as well current operational data it would be reasonable to expect that well-built modules would considerably improve commander decision making and therefore be highly desirable. Further, a level of automation of decision making would be possible and potentially better informed using the data available. This would possibly allow decision makers to accept more advanced

[21] Karen Lin, *Role of Data Science in Artificial Intelligence* (Towards Data Science, February 2018)
[22] Robert Rasch, Alexander Knott and Kenneth D. Forbus, *Incorporating AI into Military Decision Making: An Experiment* (IEEE Computer Society, 2003), 25.
[23] Karel van den Bosch and Adelbert Bronkhorst, *Human-AI Cooperation to Benefit Military Decision Making* (S and T Organization, Aug 2003), 9.

automated decision making[24] with less risk due to potentially improved decision making capabilities of automated systems. In the extreme, with a sufficiently trained artificial intelligence, that was incrementally developed and improved over time the upper limit capability of the system could be complete automation of military forces. Platforms, decision making and targeting could all be automated based on the data collected in the system, in turn limiting the need for both personal engagement in combat by soldiers as well as operational and tactical decision making totally divested to an automated decision making capability. While this might never be fully realized due to ethical and science fiction rise of the machine type concerns[25], the modularized development of the system could act as a suitable check on total machine control with additional levels of advanced automation being acceptable. This would be the case because each artificial intelligence module could be isolated from others and fully tested for compliance to limit the possibility of a total control advance artificial intelligence from taking over everything like in science fiction movies[26].

Potential Obstacles

While a system as described might be achievable, there are some obstacles that merit consideration if it is to be argued that it is in fact possible to build such as system. Firstly, a major obstacle to building a system would be to achieve an agreed upon standard and subsequently enforce that standard. In the context of an alliance framework that would be challenging in so much as each member nation might have a different idea of what is desirable. This in turn points to one nation taking the lead and setting the standards. In the context of the

[24] Kirsten Gronlund, *State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons* (Future of Life Institute, May 2019).
[25] Andy Potts, *Rise of the machines: Artificial intelligence scares people—excessively so* (The Economist, May 2015).
[26] Luke Dormehl, *The best A.I. movies of all time* (Digital Trends, Nov 2018).

NATO alliance the solution for developing the framework would most likely fall to the United States as the dominate member with the resource to initiate such a project, in turn partially justifying the U.S. enforcement of the standard. The context of a single nation initiating the development of the system is more achievable with the setting of a common standard a matter of the single hierarchy undertaking the development of the system. Maintaining the standard is potentially more problematic as the nations would have to maintain their private data and their own interfaces with the system and might have strong preferences for how things should work to make maintaining their own systems less costly or to increase their benefits. This could be partially offset by the primary nation dictating maintenance standards as in the case of development as well as other nations maintaining their private elements as they see fit. However setting and maintaining a standard would be possible much like NATO has successfully standardized on a number of issues and areas over the years[27]. Another obstacle might be the overall costs off initiating and maintaining the system. As mentioned earlier, the general spread of costs across many capability developments, the incremental approach and potential sharing of costs as previously outlined among members of an alliance could largely mitigate the costs of building and implementing the system. Beyond that is that the cost benefits of such a system are particularly compelling. In a fully realized form that provides a robust consolidated common operating picture and sets the conditions for advanced artificial intelligence development the benefits are substantial. They include saving soldier and civilian life, prosecuting conflicts much quicker and dramatically reducing the resources required to resolve a conflict through improved efficiency[28]. These benefits could more than offset the costs of producing and maintaining such a system. Another obstacle would be perceived cyber vulnerabilities. However the framework

[27] North Atlantic Treaty Organization, *Standardization* (Jan 2017).
[28] Tejaswi Singh and Amit Gulhane, *8 Key Military Applications for Artificial Intelligence in 2018* (MarketResearch.com, May 2019).

itself provide much of the solution to this problem in that it closes off access unless deliberately granted, only allows inputs in standardized forms and restricts outputs to those only required and authorized. Further the modularized incremental approach allows for rigorous testing and security screening of input and output elements[29]. Finally a significant obstacle that could be encountered is general fear of the unknown. As outlined ,the system would set the conditions for rapid development of capabilities, in particular artificial intelligence capabilities, that could make many observes concerned about pursuing the system at all[30]. While this cannot be overcome completely, the modularized incremental approach does allow for significant controls and if required checks and balances against a complete takeover of the system by some advanced component. Additionally, the locked down access approach also limits potential for unreasonable exploitation by an advance artificial intelligence or similar. Decision makers could be made more comfortable with development if a series of milestones[31] and check ins were put in place throughout development as decision makers could exercise additional control over areas they have concerns with.

Conclusion

Implementing a system that links and exploits all elements and data of a joint force starts with defining the basic framework and data structures of that system. Standardizing how future data structures are developed and screened ensures that the system remains relevant. Using a closed access security paradigm with appropriate automated and human screening as well as only granting access for specified purposes limits potential security issues. From this foundation, existing and future sensors and information systems can be integrated to provide their data to the

[29] Poonam, *Detailed Explanation of Incremental Testing* (TestOrigen, Nov 2018).
[30] Andy Potts, *Rise of the machines: Artificial intelligence scares people—excessively so* (The Economist, May 2015).
[31] Government of Canada, *A Guide to Project Gating for IT-Enabled Projects* (Nov 2012).

system. Once relevant data is captured according to a common standard it can be leveraged to develop a robust common operating picture. The system costs can be spread across different contractors and capability programs and can be leveraged and cost shared within an alliance structure. With controlled access provisions national customized use of the system is workable and sets the conditions for different nations' involvement. With pooled data, artificial intelligence training and development is possible which in turn leads to further development of system modules making the system very advanced and capable. As all of these steps are incremental and modularized, management of development is simple and overall risks to development and implementation are reduced throughout every stage. While there are some obstacles, these are largely mitigated by the framework and approach to building the system including the incremental approach, security set up and cost spreading elements. There could be some residual concern over the development of advanced artificial intelligence beyond preferred controls however, suitable check points can be established to provide decision makers with appropriate control. The overall approach, framework, incremental modularization and mitigations make building such a system possible. As has been argued, it is possible to develop a common operating system that links and exploits all elements and data of a force.

Bibliography

Armistead, Edwin, and Scott Starsman. “Perception Shaping and Cyber Macht: Russia and Ukraine.” *International Conference on Cyber Warfare and Security,* 2015.

Arquilla, John, and David Ronfeldt. “Cyberwar is Coming!” In *Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation, 1997.

Banach, Colonel Stefan J., and Alex Ryan. "The Art of Design: A Design Methodology." *Military Review* 89, no. 2, March-April 2009.

Bergen, Peter, and Katherine Tiedemann. "Washington's Phantom War: The Effects of the U.S. Drone Programs in Pakistan." *Foreign Affairs* 90, no. 4, July/August 2011.

Betz, David J., and Tim Stevens. “Conclusion.” In *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon: Routledge, 2011.

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

Bloch, Michael, Sven Blumberg, and Jürgen Laartz. "Delivering large-scale IT projects on time, on budget, and on value." *McKinsey*, October 2012.

Bowers, Christopher O. “Future Megacity Operations - Lessons from Sadr City.” *Military Review 95,* Iss. 3, May/Jun 2015.

Byman, Daniel. "Do Targeted Killings Work?" *Foreign Affairs* 85, no. 2, March/April 2006.

Byrnes, Michael W. “Nightfall: Machine Autonomy in Air-to-Air Combat.” *Air & Space Power Journal 28*, no. 3, May/Jun 2014.

CBC News. "Phoenix pay system cost could total $2.6B before cheaper replacement ready." May 2019.

CIO Whitepapers Review. "What is Software Integration." 2018.

Corbett, Mike. “A New Approach to Ballistic Missile Defense for Countering Antiaccess/Area-Denial Threats from Precision-Guided Weapons.” *Air & Space Power Journal*; Maxwell AFB, Mar/Apr 2013.

Crane, Alfred C., and Richard Peeke. “Using the Internet of Things to Gain and Maintain Situational Awareness in Dense Urban Environments and Megacities.” *Military Intelligence Professional Bulletin 42,* Iss. 3, Jul-Sep 2016.

Denning, Dorothy. “A Theory of Information Warfare.” Chapter 2 in *Information Warfare and Security.* New York: ACM Press, Addison Wesley, 1999. US Army School of Advanced

Military Studies. *Army Design Methodology: A Commander's Resource.* Fort Leavenworth, KS: US Army, Oct 2011.

Dormehl, Luke. "The best A.I. movies of all time." *Digital Trends* Nov 2018.

Duvanova, Dinissa, Alexander Semenov, and Alexander Nikolaev. "Do social networks bridge political divides? The analysis of VKontakte social network communication in Ukraine." *Post-Soviet Affairs 31,* Iss. 3, April 2015.

Evans, Michael. "Future war in cities: Urbanization's challenge to strategic studies in the 21st century." *International Review of the Red Cross 98,* Iss. 1, 2016.

Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." *Defense & Security Analysis 33,* No. 3, 14 Jul 2017.

Fulton, Scott. "What is SDN? How software-defined networking changed everything." *ZDNet,* May 2018.

Giegerich, Bastian. "Hybrid Warfare and the Changing Character of Conflict." *Connections: The Quarterly Journal*; Garmisch-Partenkirchen, Spring 2016.

Government Accountability Office. "ARMY MODERNIZATION: Steps Needed to Ensure Army Futures Command Fully Applies Leading Practices" *United States Government Accountability Office,* January 2019.

Government Accountability Office. "Weapon System Sustainment: DOD Needs to Better Capture and Report Software Sustainment Costs" *United States Government Accountability Office,* February 2019.

Government of Canada. "A Guide to Project Gating for IT-Enabled Projects." Nov 2012.

Government of Canada. "Industrial and Technological Benefits: Policy Features: Investment Framework Guidelines" April 2019.

Greer, Jim Col (Ret'd). Overview of Design Theory. Canadian Forces College Presentation, April 2015.

Gronlund, Kirsten. "State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons." *Future of Life Institute,* May 2019.

Hofman, Wout and Madan Rajagopal. "A Technical Framework for Data Sharing*." Journal of theoretical and applied electronic commerce research,* 2014.

Iulian, Chifu. "Hybrid Warfare, Lawfare, Informational War. The Wars of the Future." *International Scientific Conference* "Strategies XXI", Bucharest "Carol I" National Defence University, 2015.

Jain, Rohit. "It's time to establish big data standards: The deployment of big data tools is being held back by the lack of standards in a number of growth areas." *O'Reilly*, August 2018.

Jones-Bonbrest, Nancy "U.S. Army's common operating picture tool continues to evolve." *U.S. Army,* December 2012.

Karlsen, Geir Hågen. "Tools of Russian Influence: Information and Propaganda." Chapter 9 in *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, Edited by Janne Haaland Matlary and Tormod Heier, Palgrave Macmillan, Cham, 2016.

Kent, Randolph, Dr. "The future of warfare: Are we ready?" *International Review of the Red Cross*; Cambridge, Dec 2015.

Lauder, Matthew. "Systemic Operational Design: Freeing Operational Planning from the Shackles of Linearity." *Canadian Military Journal* 9, no. 4, 2009.

Lawton, Joel, Matthew Santaspirt, and Michael Crites. "Army Operations in Megacities and Dense Urban Areas: A Mad Scientist Perspective." *Military Intelligence Professional Bulletin 42*, Iss. 3, July 2016.

Libicki, Martin C. "Hostile Conquest as Information Warfare." In *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.

Lin, Karen. "Role of Data Science in Artificial Intelligence." *Towards Data Science,* February 2018.

Lucian Ștefan. "Unconventional Technologies in the Modern Warfare: Weapons, Concealment/Camouflage Systems, Means of Transportation." *Strategic Impact 55*, No. 2, Apr. 2015.

Luft, Gal. "The Logic of Israel's Targeted Killing." *Middle East Quarterly* 10, no. 1, Winter 2003.

Lynn, William J. III. "Defending a New Domain." *Foreign Affairs* 89, no. 5, Sep/Oct 2010.

Mac Ginty, Roger. "Everyday Peace Indicators: An Alternative Form of Assessment" Chapter 13 in *Innovations in Operations Assessment: Recent Developments in Measuring Results in Conflict Environments.* Norfolk, VA: NATO ACT, 2013.

McCarthy, Niall. "Europe Has Six Times As Many Weapon Systems As The U.S." *Forbes,* 2018.

McInnis, Kathleen J. "Lessons in coalition warfare: Past, present and implications for the future." *International Politics Reviews*, Vol. 1, Issue 2, Dec 2013.

Mehta, Aaron. "Pentagon tech advisers target how the military digests data." *DefenceNews,* April 2017.

NATO Library. "Intelligence/Information Sharing in Combating Terrorism." *NATO Multimedia Library,* May 2019.

Neal, Curtis. ”The explication of the social: Algorithms, drones and (counter-)terror.” *Journal of Sociology 52,* no. 3, 15 June 2016.

New Line Technologies. "Incremental Model of Software Development Life Cycle" January 2018.

Noergaard, Tammy. "Embeded Systems Architecture: Chapter 8 Device Drivers" *Newnes,* 2013.

North Atlantic Treaty Organization. "Standardization." Jan 2017.

O'Steen, Thomas W. “Adapting to the Evolving Strategic Environment: Applying the Lessons of the Global War on Terror to Future Threats.” *Harvard International Review*; Cambridge, Summer 2016.

Patch, John. "Obstacles to Effective Joint Targeting." *Joint Force Quarterly 45,* Spring 2007.

Perez, Lieutenant Colonel Celestino, Jr. "A Practical Guide to Design, A Way to Think About It and a Way to Do It." *Military Review* 91, no. 2, March-April 2011.

Poonam. "Detailed Explanation of Incremental Testing." *TestOrigen,* Nov 2018.

Potts, Andy. "Rise of the machines: Artificial intelligence scares people—excessively so." *The Economist,* May 2015.

Quackenbush, Stephen L., and Amanda Murdie. “We Always Fight the Last War? Prior Experiences in Counterinsurgency and Conventional Warfare and War Outcomes.” *International Interactions*, Vol. 41 Issue 1, Jan-Mar 2015.

Rasch, Robert, Alexander Knott, Kenneth D. Forbus. "Incorporating AI into Military Decision Making: An Experiment." *IEEE Computer Society*, 2003.

Reilly, Jeffrey M. “Multidomain Operations.” *Air & Space Power Journal 30*, Iss. 1, Maxwell AFB, 2016.

Rid, Thomas. "Cyberwar Will Not Take Place." *Journal of Strategic Studies* 35, no. 1, Feb 2012.

Sampaio, Antonio. “Before and after urban warfare: Conflict prevention and transitions in cities.” *International Review of the Red Cross 98,* Iss. 1, 2016.

Schmitt, Michael N. “The Law of Cyber Targeting.” *Naval War College Review 68,* Iss. 2, Spring 2015.

Singh, Tejaswi and Amit Gulhane. "8 Key Military Applications for Artificial Intelligence in 2018" *MarketResearch.com,* May 2019.

Tarantola, Andrew. “Will we be able to control the killer robots of tomorrow?”. *Engadget*, New York: AOL Inc., 2017.

TRADOC, US Army. “MultiDomainBattle: Evolution of Combined Arms for the 21st Century” YouTube, Oct 7, 2017.

Tsuruoka, Michito. “NATO's Challenges as Seen from Asia: Is the European Security Landscape Becoming Like Asia?” The Polish Quarterly of International Affairs, Warsaw, 2016.

Turner, C.C., and Richard Goette. *Joint Targeting: Concepts and Theory.* Canadian Forces College, April 2016.

Van den Bosch, Karel and Adelbert Bronkhorst. "Human-AI Cooperation to Benefit Military Decision Making." *S and T Organization,* Aug 2003.

Wass de Czege, Huba. "Systemic Operational Design: Learning and Adapting in Complex Missions." *Military Review* 89, no. 1, January - February 2009.

Wilcox, Lauren. “Embodying algorithmic war: Gender, race, and the posthuman in drone warfare.” *Security Dialogue 48,* no. 1, 2017.

Williams, Andrew, *et al.* “The Rationale, Challenges and Opportunities in Operations Assessments.” Chapter 1 in *Innovations in Operations Assessment,* edited by Andrew Williams, James Bexfield, Fabrizio Fitzgerald Farina, and Johannes de Nijs. Virginia, USA: NATO ACT, 2013.

Young, Chris. "Military Intelligence Redefined: Big Data in the Battlefield." *Forbes,* March 2012.