





Digitalization: The Not-So-Flashy Capability You Can't Live Without

Major Robert W. Thompson

JCSP 46 DL

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.

© 2021 Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence.

PCEMI 46 AD

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.

© 2021 Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale.

Canadä

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 DL – PCEMI 46 AD

2019 – 2021 SOLO FLIGHT

DIGITALIZATION: THE NOT-SO-FLASHY CAPABILITY YOU CAN'T LIVE WITHOUT

By Major Robert W. Thompson

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

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

DIGITALIZATION: THE NOT-SO-FLASHY CAPABILITY YOU CAN'T LIVE WITHOUT

INTRODUCTION

Disruptive technologies such as cloud-based computing, the aggregation of big data, and the use of Artificial Intelligence (AI) have been touted as gateways to a new age of information use and sharing. Companies such as Google, Microsoft and Amazon have expended significant effort to generate algorithms that examine patterns in data to anticipate the needs and wants of consumers. This allows these companies to tailor the consumer's experience to the maximum extent possible in an effort to generate more clicks, more likes, and more sales. But even deeper, this data is used to teach algorithms to anticipate behaviours *en masse*, allowing these companies to, for example, pre-position stock where it is most likely to be consumed to meet requests in unprecedentedly short timelines. That companies are able to achieve short delivery timelines during a period when demand for goods ordered online is at an unprecedented high due to the ongoing COVID-19 pandemic highlights the proactive approach to supply chain management this enables. But can this seeming ability to read the future have an impact on modern warfare? Are we actually ready to tap the possibilities presented by these emerging capabilities? How do we go about setting ourselves up for success in the face of these technologies?

Based on the results of a literature review we will highlight how the institutionalization of a digitalized culture, coupled with the right infrastructure to support and enable decision-makers using information shared across domains is a joint capability in and of itself. We will begin by outlining some of the better-known disruptive technologies and call out a few of the ways they best enable operations, then outline digitalization and illustrate how it can support or enable these capabilities.

DISRUPTIVE TECHNOLOGIES

Some key disruptive technologies being examined in military and academic circles are a part of the every-day modernization of society. Technologies such as drones, the Internet of Things (IoT), AI, and Big Data take on a new meaning when more people, organizations and potential adversaries put more of their information on networks and use technologies whose functions rely on or are enhanced by being networked.

Drones

Drones have shown a number of promising capabilities that are being developed not in large expensive government procurement cycles, but rapidly and at low cost by commercial ventures. They can act as sensors, where "commercial demand for long-endurance surveillance systems is resulting in solutions that are much less expensive [than military models] and require only a few personnel [to operate]."¹ Since these devices are now being developed rapidly using open methods, they are lowering their development costs, which has already resulted in their widespread use by smaller states and non-state actors who would not normally have the capabilities offered by drones.

Drones are not limited to a passive role in military operations. Military drones with strike capabilities have been in use for many years now, but there have been several examples of non-state actors using drones for strike capabilities, and these are only going to improve as well. "Commercial firms are testing autonomous VTOL drones that are GPS-independent, hardened against electronic interference, range hundreds of miles, deliver with an accuracy of 1 meter, and are inexpensive enough to be disposable."² What they are delivering is only limited by payload and the imagination of the sender.

When these platforms are integrated with some of the other technologies on this list, such as AI, they start to become significantly more capable. Using independent AI, "drones will be able to start processing information that they are looking for, rather than sending back an endless video stream that requires hours of intense analytic analysis and interpretation, and is heavily human-intensive."³

The Internet of Things

Oracle Canada defines the Internet of Things (IoT) as "the network of physical objects - "things" - that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools."⁴

This is an important technology primarily due to its pervasiveness. With a current estimate of over 7 billion devices⁵ networked in this fashion and being a potential node on the internet: producing data on its status, recording preferences of its users, and drawing information from the environment; this represents both a risk and an opportunity. It is a synthesis of "low-

¹ Hammes, T.X. "Key Technologies and the Revolution of Small, Smart, and Cheap in the Future of Warfare." In *Strategic Assessment 2020: Into a New Era of Great Power Competition*. Washington: Institute for National Strategic Studies, National Defense University. p 122.

² Hammes, T.X. "Key Technologies and the Revolution of Small, Smart, and Cheap in the Future of Warfare." In *Strategic Assessment 2020: Into a New Era of Great Power Competition*. Washington: Institute for National Strategic Studies, National Defense University. p 123.

³ Coker, Christopher. "Targeting in Context." In *Targeting: The Challenges of Modern Warfare*. The Hague, Netherlands: Asser Press (Springer), 2016. p 23.

⁴ Oracle. "What is the Internet of Things." *Oracle Canada Website*, 2021. Accessed 17 May 2021. https://www.oracle.com/ca-en/internet-of-things/what-is-iot/

cost computing, the cloud, big data, analytics, and mobile technologies,"⁶ which allows "physical things [to] share and collect data with minimal human intervention [and] record, monitor, and adjust each interaction between connected things."⁷

From this "the joint force will have opportunities to use these devices to gain and maintain situational awareness."⁸ It also presents a risk since an adversary can also leverage this information, with the risk growing as more nodes are added to the net.

Artificial Intelligence and Big Data

A key enabler of the previous two technologies, and potentially the most disruptive on this list, is Artificial Intelligence (AI). Not only is robust AI a key component of some of the more enterprising applications of Drones and IoT, such as the promise of making drones that are immune to GPS spoofing and can identify a person or other target,⁹ but it can facilitate the efforts of the joint force on its own.

As Brad DeWees puts it "Artificial intelligence is a means of solving the ancient problem of limited cognitive capacity in an information-abundant world."¹⁰ How this technology impacts joint warfighting was very succinctly described by Alfred Crane:

Since warfare is an exercise in organizational learning and adaptation, the ability of AI to automatically update programming with the results of each engagement or operation should be a positive influence. The availability of this information will promote faster learning and dissemination of experiences than existing human-based methods. Thus, if

7 Ibid

⁶ Oracle. "What is the Internet of Things." *Oracle Canada Website*, 2021. Accessed 17 May 2021. https://www.oracle.com/ca-en/internet-of-things/what-is-iot/

⁸ 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, no. 3 (Jul-Sep 2016). p 42.

⁹ Hammes, T.X. "Key Technologies and the Revolution of Small, Smart, and Cheap in the Future of Warfare." In *Strategic Assessment 2020: Into a New Era of Great Power Competition*. Washington: Institute for National Strategic Studies, National Defense University. p 124.

¹⁰ DeWees, Brad. "Modern Solution, Ancient Problem: Measuring Military Effectiveness in the Age of Artificial Intelligence." *War on the Rocks*, 9 July 2018. Accessed 10 March 2021. https://warontherocks.com/2018/07/modern-solution-ancient-problem-measuring-military-effectiveness-in-the-age-of-artificial-intelligence/

learning and adaptation are positively correlated with success in warfare, AI should help.¹¹

The first and most obvious application of AI is to use it to parse the large volumes of data now available to intelligence analysts. "Experts estimate there were 23 million tweets involved in the self-proclaimed Islamic State's online marshalling of support and influence operations."¹² This much data will overwhelm current methods of intelligence analysis, presenting a dilemma:

"The digitization of human society has made huge amounts of information available for analysis. This information comes from an ever-increasing number of sources, like online social networks, digital sensors, or ubiquitous surveillance, and has been increasingly useful for intelligence. Too much information is being produced too quickly for an intelligence analyst to even comprehend it using current analysis techniques and software, much less derive meaningful intelligence from it or verify its veracity."¹³

This information will come both from traditional sources, and opportunities offered by the proliferation of drones and the IoT. Meaning a synergy between these technologies exists, if we can move the information between them.

Other parts of the security sector are making use of this proliferation of data. Police are using "neural network technology for pattern-matching to enable the security services to scan faces in a crowd and cross-reference them to known troublemakers."¹⁴ The intent is to take this application further: programming computers to "recognise patterns and relationships that we cannot recognise in each other—body language if you will—that betray anxiety, even perhaps an intention to plant a bomb."¹⁵ In addition, "Predictive policing' systems built by IBM sift through vast records of past offences, weather patterns, social media use, and other contributing factors to display maps showing where offences are likely to occur, prompting police to boost patrols at specific times."¹⁶

All this information has to be assembled, processed and analyzed to have value, which is where Big Data comes in. To enable the policing examples above, "[d]ata processing systems

13 Ibid

¹⁵ Ibid.

16 Ibid.

¹¹ Hoffman, Frank G. "Will War's Nature Change in the Seventh Military Revolution?" *Parameters* 47, no. 4 (Winter 2017-2018). p 27-28.

¹² Cruikshank, Iain. "The ABCs of AI-Enabled Intelligence Analysis." *War on the Rocks*, 14 February 2020. Accessed 16 May 2021. https://warontherocks.com/2020/02/the-abcs-of-ai-enabled-intelligence-analysis/

¹⁴ Coker, Christopher. "Targeting in Context." In *Targeting: The Challenges of Modern Warfare*. The Hague, Netherlands: Asser Press (Springer), 2016. p 13.

are also improving all the time. CCTV cameras can now be patched into information retrieval systems to facilitate a 'knowledge brokering' function which goes far beyond pinpointing people as they move about."¹⁷

"The [intelligence community]'s routine work of collection, [processing, exploitation, and dissemination], and analysis is still largely organized on the Cold War model of seeking out sparse and secret information. Now, however, it must cope with the inverse challenge (and exploit the opportunities) of managing and analyzing massive quantities of data"¹⁸ This means data analysis methods and effective data aggregation data are now key capabilities for our operational Sense and Command functions. How we store all this information and move it around is becoming mission critical. AI contributes here as well: as "not just a way to collect more information about effectiveness [or any other subject] - it is a way to make sense of all that information."¹⁹

DIGITIZATION, DIGITALIZATION AND THE CANADIAN ARMED FORCES

Digitization: A Simple Example from the Past

Organizations with roots in an analogue, paper-based past, such as the Canadian Armed Forces (CAF), have struggled to leverage digital technologies. Several initiatives have attempted to use computers and the Internet to "Digitize" the force. Significant effort has been expended on these initiatives which have been successful individually, but the resulting ability to make use of emerging technologies with the agility demonstrated in the private sector has failed to materialize. The issue arises from the approach taken.

Digitization is "the process of changing from analog to digital form, also known as digital enablement. Said another way, digitization takes an analog process and changes it to a digital form without any different-in-kind changes to the process itself."²⁰

A simple example is the process for leave approval for CAF members. Previously using physical leave passes with ink signatures, it has been digitized so that an exact electronic copy of the paper form is emailed and digitally signed by the requestor, recommender and approver. While this does eliminate the physical leave pass, the process is still functionally the same as the

¹⁹ DeWees, Brad. "Modern Solution, Ancient Problem: Measuring Military Effectiveness in the Age of Artificial Intelligence." *War on the Rocks*, 9 July 2018. Accessed 10 March 2021. https://warontherocks.com/2018/07/modern-solution-ancient-problem-measuring-military-effectiveness-in-the-age-of-artificial-intelligence/

²⁰ Gartner, Inc. "Definition – Digitization." *Gartner Information Technology Glossary*. 2021. Accessed 17 May 2021. https://www.gartner.com/en/information-technology/glossary/digitization/

¹⁷ Ibid.

¹⁸ Symon, Paul A. and Arzan Tarapore. "Defense Intelligence Analysis in the Age of Big Data." *Joint Force Quarterly no.* 79 (Q4 2015). p 5.

legacy process, even to the point where the leave pass is printed by Orderly Rooms to provide an audit trail prior to entry into the Human Resources Management System, then physically stamped indicating entry. Some efficiencies are achieved, but the end result is nearly identical to the old process.

Digitalization: The Way of the Future

Digitalization, on the other hand, "is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business."²¹ While the concepts of revenue and value-production are not commonly applied to CAF operations, the concept of value could be exchanged with efficiency, readiness or operational effectiveness to illustrate why this is beneficial.

The digitalized version of the leave approval process above would look more like an endto-end digital solution wherein requestors submit leave, approvers render their decisions, and the resulting leave status and balance of leave remaining is adjusted automatically within the system. It is noteworthy that DND has a digitalized process for civilian leave, whereas CAF's system is digitized. Put another way, "[Digitization] is mostly about enabling business as usual and "staying in the game," while [Digital Transformation or Digitalization] is about building real, long-term competitive advantage to succeed."²²

The Challenges with Getting from Here to There

The reason Digitization is more common than Digitalization is because Digitalization is not a straightforward transformation. It involves more than technology, impacting processes, structures, and levels of staffing. The frictions associated with a transformation of sufficient depth to truly digitalize are often beyond the change management threshold typically acceptable to CAF stakeholders: either because of a desire to preserve existing processes and structures, or because of a lack of longevity among the individuals championing a particular change.

Digitalization involves more "than asking people to work in new ways within the confines of the old organizational model[, w]inners in the digital era break up old power structures so that new ideas and capabilities can be scaled more collaboratively."²³ This is difficult for the CAF to undertake:

"Changing the military so that software can handle many of its problems is, admittedly, a far harder task than any other "market transformation." It is different from optimizing food delivery or ensuring that you can watch streaming video anywhere in the world. Military leaders come from traditions with rich histories and deeply embedded cultures.

²¹ Ibid.

²² Leinwand, Paul and Mahadeva Matt Mani. "Digitizing Isn't the Same as Digital Transformation." *Harvard Business Review*. 26 March 2021. Accessed 16 May 2021. https://hbr.org/2021/03/digitizing-isnt-the-same-as-digital-transformation

Their mission has a unique sense of gravity [since] they protect their citizens and their way of life using lethal force, all the time acting subject to democratic obligations."²⁴

Without a fundamental change to the way the CAF approaches, handles and shares information, we can expect to fall further behind. Our allies struggle with this too: "A standard [US] Department of Defense 24-month acquisition plan in the digital world will likely already be out of date by the time it is implemented. The technology industry iterates in months, not years."²⁵ This is more than a procurement problem, however. The ability to capitalize on the wealth of information applies at all levels of conflict.

At the strategic level, "information technology is the key to both economic and military power. In this era, the countries best able to control the flow of information across the world's networks tend to make the system's rules."²⁶

At the operational and tactical levels, effective use of information is "a major determinant of tactical and operational effectiveness [and] part of winning the 'narrative' by minimising collateral damage [and is now] seen as an end in itself."²⁷ Information is important: the ability to rapidly and clearly collect, collate, analyze and distribute information will win conflicts by shortening decision-makers decision-action cycle. As a result, "the military should come to see itself as a software-enabled enterprise."²⁸

This does not mean the complete abandonment of existing military processes. "[T]he joint targeting cycle still provides a common framework with which the Army can target and provide complimentary effects with other services in the joint environment."²⁹ This collaborative targeting is only possible if stakeholders in each domain can effectively share information. Common processes must be supported by technologies that enable sharing of information in a consistent and timely manner.

²⁵ Ibid.

²⁷ Coker, Christopher. "Targeting in Context." In *Targeting: The Challenges of Modern Warfare*. The Hague, Netherlands: Asser Press (Springer), 2016. p 12.

²⁴ Lynch, Chris and Oliver Lewis. "On the Digital Brink." *War on the Rocks*, 11 March 2021. Accessed 16 May 2021. https://warontherocks.com/2021/03/on-the-digital-brink/

²⁶ Richard B. Andres, "Cyber Conflict and Geopolitics by Richard B. Andres," Great Decisions 2019, Foreign Policy Association, 2019. From Andres, Richard. "Emerging Critical Information Technology and Great Power Competition." In *Strategic Assessment 2020: Into a New Era of Great Power Competition*, 139-151. Washington: Institute for National Strategic Studies, National Defense University. p 141.

²⁸ Lynch, Chris and Oliver Lewis. "On the Digital Brink." *War on the Rocks*, 11 March 2021. Accessed 16 May 2021. https://warontherocks.com/2021/03/on-the-digital-brink/

²⁹ Borne, Kyle David. "Targeting in Multi-Domain Operations." *Military Review* 99, no. 3 (May/June 2019). p 63.

For this reason, Digitalization is an absolute necessity to ensure leaders are able to make decisions faster, and based on a better understanding of the situation. There is, however, a danger these systems may have the opposite effect: bogging commanders down in data or enabling the tendency to centralize authority contrary to the tenets of mission command. We need to ensure our approach to Digitalization enables our way of war, rather than forces us into an approach we did not select, or worse, introduces more friction into our existing processes.

DIGITALIZATION: THE CAPABILITY

What is the key change we need to make in order to break ourselves out of the confines of a merely digitized set of capabilities and start to really make these disruptive technologies work for us? It all hinges around data. The common thread of all of the technologies described above is that they produce, use and move data. Becoming more efficient at using data will enable all the other benefits we expect to reap from these technologies. We need to take a Data Centric approach to our information systems.

"Data centric refers to an architecture where data is the primary and permanent asset, and applications come and go. In the data centric architecture, the data model precedes the implementation of any given application and will be around and valid long after it is gone."³⁰ It means the information we collect and store needs to be retained and protected not only for policy or historical reasons, but because it is an operational asset. It means the systems we acquire have to treat data in the manner we prescribe, so it can be incorporated with and exploited alongside the data we already have.

"Digital data is most useful when it is stored in a way that maintains some kind of consistent format (i.e., all data entries have the same fields of information: date, time, location, for example) and can be easily accessed (i.e., can be queried from the same programming environment where the analysis is taking place: the analyst doesn't have to launch a new program or window to search the database)."³¹

If the information we collect is improperly documented, uses bespoke formats, and may or may not duplicate existing information, then analysts or systems using this data will spend most of their time navigating the myriad information sources, downloading data and manually fixing errors and hunting duplications in order to get usable data. "This severely inhibits an

³⁰ McComb, Dave. "The Data-Centric Revolution: Data-Centric vs. Data Driven." *The Data Administration Newsletter*, 21 September 2016. Accessed 16 May 2021. https://tdan.com/the-data-centric-revolution-data-centric-vs-data-driven/20288

³¹ Cruikshank, Iain. "The ABCs of AI-Enabled Intelligence Analysis." *War on the Rocks*, 14 February 2020. Accessed 16 May 2021. https://warontherocks.com/2020/02/the-abcs-of-ai-enabled-intelligence-analysis/

analyst from using advanced, computational tools as much of their time will necessarily be spent manually downloading and formatting data."³²

To build a Data-Centric system, two key concepts must be adopted: "First, analysis tools and applications should change with the data, and second, data should be easily accessible. Analysts must be able to configure the tools and algorithms of the systems to meet the realities of the battlefield, and data access should be as seamless as possible."³³ This puts an additional burden of skill on the analysts, as they will have to obtain "some programming skills and basic data science skills."³⁴ While this would seem to increase rather than decrease the burden on data analysts, especially considering all the other specialized skills required, "if one considers how much time intelligence analysts spend manually handling data, military organizations can't afford *not* teach these skills to their intelligence analysts."³⁵ In addition, "having analysts that can configure their tools and algorithms to the battlefield environment will decrease operational risk,"³⁶ since we can be better assured the toolset being applied actually matches the situation in hand.

Digitalization represents an opportunity to become more efficient at using these emerging tools. It is not even necessary to have the latest thing in Big Data at our disposal. During World War II, the British leveraged the emerging technology of RADAR despite the fact they "lagged behind the Germans technologically[. They] more than compensated for the shortfall by the way they wove radar into every aspect of air defense...during the 1940 Battle of Britain. According to Winston Churchill, "it was operational efficiency rather than novelty of equipment that was the British achievement."³⁷ Proper integration of new technology was more important in that case than the quality of the technology: the same can be said for the modern revolution underway. Digitalization is a key part of that integration: it enables the passage of information between traditional and emerging sensors and the decision-making processes they feed. It also allows us to bring AI to bear to enable the synthesis of information and speed up the ISTAR process: collating the significant amount of data available to commanders faster than a conventional staff

33 Ibid.

³⁴ Ibid.

35 Ibid.

³⁶ Ibid.

³² Cruikshank, Iain. "The ABCs of AI-Enabled Intelligence Analysis." *War on the Rocks*, 14 February 2020. Accessed 16 May 2021. https://warontherocks.com/2020/02/the-abcs-of-ai-enabled-intelligence-analysis/

³⁷ Cronin, Audrey K. "Technology and Strategic Surprise: Adapting to an Era of Open Innovation." *Parameters* 50, no. 3 (Autumn 2020). p 75.

using "Big Data Analytics and knowledge management/decision making tools...to filter and make sense of all of the data being obtained."³⁸

THE WAY FORWARD

Information is the common thread that binds key disruptive technologies such as Drones, the Internet of Things, Big Data and Artificial Intelligence, and handling information is the key to enabling the CAF to make use of these technologies. The way our processes handle the information produced and consumed by these technologies will determine our success in future operations. Underlying all is the requirement to lay the groundwork. Self-contained, bespoke systems will have to give way to standardized, open systems that enable inter-connection in order to allow information to flow from the places it is generated, through a robust process of analysis and into the hands of decision-makers, targeteers and shooters for use. To enable agile decision-making in a joint context, interoperability in the form of seamless sharing of information, enabled by common information standards and a shared architecture, is a capability we cannot afford to do without.

³⁸ 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, no. 3 (Jul-Sep 2016). p 42.