Towards a data-driven military – an introduction

Peter B.M.J. Pijpers, Mark Voskuijl & Robert J.M. Beeres

Introduction

In October 2020, the Netherlands Ministry of Defence (MoD) published its Defence Vision 2035 (DV35) setting out guidelines for future doctrine, policy, innovation and acquisition.[1] This so-called White Paper envisages the 2035 defence organisation as a reliable partner and protector that is technologically advanced and able to execute information-driven operations. The future Netherlands defence organisation will avail of strong innovative capacities and focus on specialisation within the North Atlantic Treaty Organization (NATO) and the European Union (EU). Moreover, it will be an effective military actor in the information environment, making use of available data and information. In the near future, the Netherlands defence organisation will obtain an authoritative information position, be able to execute multi-domain and integrated information-driven operations, and to use information as a weapon.[2]

The use of information and data during war, armed conflict or interstate competition is as old as war itself. The Cold War era, where the military instrument was sometimes rendered obsolete due to the overwhelming strategic nuclear stalemate, proved a cornucopia for activities other than the use of force. Both the Soviet Union and its allies,[3] and the United States and its allies were very active in influencing each other by means of persuasion, coercion or manipulation. These were the heydays of both the Soviet doctrine of *Active Measures* as well as American *Political Warfare*.[4]

Recent technological advances in the field of computer science have impacted the ability to use information and data profoundly. Not only in business, but also in the military. Microelectronics and miniaturisation have enabled the development of a wide range of new products and capabilities for military systems. A relevant example worth mentioning in this context is the use of large remotely piloted aircraft systems (RPAS) such as the General Atomics MQ-1 Predator and MQ-9 Reaper in Iraq and Afghanistan over the last fifteen years.[5] Unmanned aircraft, equipped with impressive sensor suites and precision-guided munitions can be piloted from the other side of the world by means of satellite communication. At present, small low-cost unmanned aircraft systems are used world-wide for a variety of military applications such as information, surveillance and reconnaissance missions. In the future, swarms of weaponised unmanned aircraft with high levels of autonomy may be expected.

Meanwhile, information technology (IT) interconnectedness serves to enable cyberspace. This novel man-made domain unlocked the information environment, thereby providing new opportunities for trade and communication.[6] Customers anywhere in the world can easily buy products in China without Mandarin proficiency, and the Internet supports upcoming firms in their search for global markets instantly. As cyberspace will also serve as a platform in competition and conflict,[7] malign actors will be provided similar opportunities.

On 24 February 2022, the Russian Federation, conducting a 'special military operation', invaded Ukraine, thereby flagrantly violating international law and alarming international society.[8] Though military and kinetic activities gained most public and media attention – largely due to the damage and destruction they cause – the Ukraine-Russian war and, specifically, the run-up to the war, illustrates the use of data in modern warfare.

In hindsight, the 2014 Maidan revolution, the annexation of the Crimean Peninsula in February and March 2014, the subsequent pro-Russian revolts in the Donbass region, can be seen as triggers shaping up to the 2022 Ukraine-Russian war. Since 2014, the Russian Federation has executed numerous operations in or via cyberspace to undermine, compel or deter Ukraine, most prominently, the 2015 cyber-attack on the Ukrainian electricity network, leaving more than 200,000 people without power for over four hours.[9] In the direct run-up to the 2022 Ukraine-Russian war, Ukraine faced attacks by numerous cyber operations, ranging from the instalment of 'wiper-malware', destroying computer software, blocking government websites via distributed denial-of-service (DDoS) attacks, sabotaging the Viasat satellite system and leaking personal data of more than 2 million Ukrainians.[10]

The attributes of cyberspace, and the ubiquitous access to data changed the character of conflict. States are no longer the sole actors involved, and physical borders have lost relevance in cyberspace. In modern conflict numerous non-state actors, sympathisers (hacker groups such as Anonymous) have sided with one of the warring states without necessarily being belligerent entities; ICT businesses are more outspoken about intrusions in the ICT infrastructure; citizen journalism (for example Bellingcat) is involved in debunking disinformation disseminated on social media platforms; and even the traditionally covertly operating intelligence services are now sharing data via Twitter hoping to expose Russian plans and intentions.[11]

Increasingly, data has gained importance, not only in society at large but *ipso facto* in modern warfare,[12] the core theme of the Netherlands Annual Review of Military Studies (NL ARMS) 2022.

NL ARMS 2022 assesses the use of data and information on modern conflict from different scientific and methodological disciplines, aiming to generate valuable contributions to the on-going discourse on data, the military and modern warfare. Military Systems and Technology approaches the theme empirically by researching how data can be used to enhance the efficiency and effectiveness of military materiel and equipment, thereby generating valuable data to enhance and accelerate the decision-making process. War Studies takes a multidisciplinary approach on the evolution of warfare, while Military Management Studies takes a holistic organisational and procedural approach. Based on their scientific protocols and methods of research, the three domains put forward different research questions and perspectives, providing the unique character of NL ARMS 2022.

The next section provides an overview of the upcoming chapters. To this end, the editors selected a categorisation with reference to a data-driven military or defence organisation. Case-studies focus on the Netherlands Defence organisation. This volume's first part elaborates on how the use of data impacts organisation, focusing on the logistical, personnel and material aspects of the Defence organisation. The second part assesses how data-driven techniques can enhance or accelerate decisions made within the Defence organisation. The last part discusses how data affect the planning and conducting of operations.

Overview of the Chapters

The first part of the book discusses the organisational aspects of a data-driven military Defence organisation. In Chapter 1, Kramer and van Os sketch a sociotechnical perspective on digital transformation. In general, there is consensus that digital technology will hold profound transformative effects on society, organisations, and human beings. Notwithstanding this broad consensus, these transformative effects of digital technology are also controversial, notably, because the transformative impact of digital technology cannot be straightforwardly deduced from functional specifications of the technology itself. Op den Buijs, in Chapter 2, highlights one of the organisational aspects; human resource management. The use of big data analytics in the Human Resource Management (HRM) field has become enormously popular. It can therefore also be beneficial for the armed forces to cope with changes in the HRM environment related to technology, labour market, aging population, personnel recruitment. However, HRM data analytics do not only offer opportunities, they also pose challenges. The third and fourth chapters focus on maintenance. While data may be considered an important "weapon", data collection and analysis are also crucial in reducing the number of system failures, and thus, potentially, may increase systems availability and military performance considerably. In Chapter 3, Tinga, Homborg and Rijsdijk introduce the concept of data-driven maintenance using various maturity levels, ranging from detection of failures and automated diagnostics to advanced condition monitoring and predictive maintenance that are tested against practical cases to demonstrate the benefits and discuss the challenges that are encountered. In Chapter 4, Vriend, Tiddens and Jurrius argue that while machine learning is used successfully in many applications, challenges remain; data is often stored in separate places, and data used for training purposes ought to respect privacy. Federated learning circumvents the challenges and allows machine learning models to be trained based on privacy-sensitive data sets of multiple parties without having to share raw data. This promising technique is especially valuable in case of collaborative activities with external parties. De Gooijer, Hoogstrate, Schijvenaars, van Fenema and van Kampen, in Chapter 5, focus on the sustainment organisation of the MoD and explore the usability of data-driven maturity models to explore whether the Netherlands defence organisation can become an information and data-driven organisation.

The second part of this volume assesses the extent to which data can be used to support the decision-making process. Both during armed conflicts as well as while preparing for deployments, data can enhance the effectiveness and efficiency of decision-making processes. In Chapter 6, Hoogstrate analyses the effects of Big Data and Artificial Intelligence (AI) on the practice of forecasting in defence and military applications. By combining Big Data and AI, he expects that forecasting and foresight development will be greatly influenced and will impact on applications at the strategic, operational as well as tactical level. In Chapter 7, Lindelauf, Monsuur and Voskuijl investigate whether algorithmic techniques from the fields of operations research, data science and aircraft trajectory optimisation can aid military flight mission planning. Optimising military helicopter missions relates to aspects including instance route selection, helicopter configuration design, opponent modelling to personnel to platform allocations. In Chapter 8, van Ee, de Lima Filho and Monsuur research how maritime patrols conducted with multiple unmanned aerial vehicles can optimise their objectives to detect, locate and identify (opposing) vessels. The authors make clear that the routing problem including mutual support, can be modelled as a generalised travelling salesman problem (GTSP), thereby investigating the costs of requiring mutual support and comparing it to the costs of using separate drones that detect and identify vessels in the area of operations. Chapter 9 by Theunissen provides an overview of current trends in the development of Detect- and Avoid (DAA) systems required for the integration of remotely operated aircraft into non-segregated airspace. A DAA system provides the pilot with actionable information derived from real-time data about cooperative and non-cooperative traffic. Theunissen discusses the potential AI and Machine Learning techniques for the purpose of DAA and several associated legal, ethical, integration and certification issues are addressed. In Chapter 10, the final chapter of Part II, Horlings, Lindelauf and Rietjens describe how in the current information age, military intelligence and security organisations are confronted with information overload – a situation in which decision-makers face a level of information that is greater than their information processing capacity. Information overload is not only the result of the continuously increasing amount of the data, but also of the high levels of uncertainty of the data. Information overload has serious consequences hampering the effectiveness and efficiency of military intelligence and security organisations. In order to improve decision-making accuracy, organisations need to find ways to process more information without increasing the experienced information load.

The third part of the book is geared towards the use of data during operations. What legal framework applies when military units use, collect and process data in military operations, as well as while preparing for operations. Moreover, the question of how data serves as a weapon of influence is studied. In Chapter 11, Timmermans and Lindelauf elaborate on the advantages of data-driven methodologies regarding their beneficial impact on optimising solutions for decision problems, whilst, on the flipside, causing ethical risks, both to society at large and defence and military organisations in particular. Timmermans and Lindelauf conceptually investigate the trade-off between privacy on the one hand and algorithmic performance on the other, concerning the use of MoD relevant (bulk) datasets from a technical, moral and socio-political view. In Chapter 12, Ducheine, Pijpers and Pouw investigate the legal framework to execute ‘information-driven operations’, as depicted in the Defence White Paper “Defence Vision 2035”. Cyberspace has unlocked the information environment, raising obvious concerns about the use of data and potential infringements of privacy since it simultaneously gives new impetus to use data to improve military intelligence and understanding, as well as to enhance decision making, but also to use information as a “weapon of influence”. Deploying armed forces in the information environment is challenging since the current legal framework applicable to information manoeuvre hampers training and preparing for operations. In Chapter 13, Zwanenburg and van de Put analyse the use of biometrics during military operations extraterritorially from the perspective of the right to private life in Article 8 of the European Convention on Human Rights (ECHR). The authors argue that the ECHR is applicable to certain conduct of armed forces outside their own state’s territory, and that this includes situations involving the use of biometrics. Therefore, although states have a certain margin of appreciation, compliance with the right to private life during extraterritorial military operations appears to be a tall order. In Chapter 14, the final chapter of Part III, de Jong, de Werd and Bouwmeester argue that the role of information as a source of power in Russia’s foreign policy and military actions has received increasing attention of

Western scholars and policymakers, whilst focusing on Russian foreign policies and military operations in Georgia and Ukraine as typical case studies. This chapter aims to retrieve more insight in the nature of information operations by studying the atypical case of the 2020 Nagorno-Karabakh War between Armenia and Azerbaijan, in which Russia proliferated herself as a mediator. De Jong, de Werd and Bouwmeester argue that the Russian narrative is tailored to various national and international audiences and fits with Russian interests.

Finally, NL ARMS 2022 offers an epilogue. In Chapter 15, Baudet and de Jong provide a historical overview of the quantitative use of data, especially in measuring effects, or even success, during warfare. Baudet and de Jong discuss the idea that quantitative data can help manage and predict the course of a war, elaborating on the case of Robert McNamara whose technocratic statistical approach guided the war effort during the Vietnam War. In spite of the fact that the United States lost that war, the underlying idea has had a lasting influence that can be traced to the conduct of contemporary wars. The authors argue that technocratic approaches often disregard the complexity and imponderabilia of unique historical wartime contexts and advocate the integration of quantitative-generalising and qualitative-historicising approaches to understand past and contemporary warfare.

Notes

[1] Netherlands Ministry of Defence, "Defence Vision 2035: Fighting for a Safer Future," 2020.

[2] Netherlands Ministry of Defence. Annex p. XII

[3] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020).

[4] Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses*, 2018.

[5] Ann Rogers and John Hill, *Drone Warfare and Global Security*, 2014.

[6] Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online manipulation: hidden influences in a digital world," *Georgetown Law Technology Review* 4, no. 1 (2019): 1–52.

[7] Thomas Paterson and Lauren Hanley, "Political warfare in the digital age: cyber subversion, information operations and 'deep fakes,'" *Australian Journal of International Affairs* 74, no. 4 (2020): 439–54.

[8] James A Green, Christian Henderson, and Tom Ruys, "Russia's attack on Ukraine and the jus ad bellum," *Journal on the Use of Force and International Law*, 2022.

[9] Robert Lee, Michael Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS Industrial Control Systems Security Blog*, 2016.

[10] United Kingdom Government, "UK Assess Russian Involvement in Cyber Attacks on Ukraine," 2022.

[11] United Kingdom Ministry of Defence, "Latest Defence Intelligence Update on the Situation in Ukraine – 8 April 2022," Twitter, 2022, https://twitter.com/DefenceHQ/status/1512284278813597702.

[12] Holger Möldera and Vladimir Sazonovb, "Information warfare as the Hobbesian concept of modern times — the principles, techniques, and tools of Russian information operations in the Donbass," *Journal of Slavic Military Studies* 31, no. 3 (2018): 308–28.

References

Green, James A, Christian Henderson, and Tom Ruys. “Russia’s attack on Ukraine and the jus ad bellum.” *Journal on the Use of Force and International Law*, 2022.

Lee, Robert, Michael Assante, and Tim Conway. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” *SANS Industrial Control Systems Security Blog*, 2016.

Möldera, Holger, and Vladimir Sazonovb. “Information warfare as the Hobbesian concept of modern times — the principles, techniques, and tools of Russian information operations in the Donbass.” *Journal of Slavic Military Studies* 31, no. 3 (2018): 308–28.

Netherlands Ministry of Defence. “Defence Vision 2035: Fighting for a Safer Future,” 2020.

Paterson, Thomas, and Lauren Hanley. “Political warfare in the digital age: cyber subversion, information operations and ‘deep fakes.’” *Australian Journal of International Affairs* 74, no. 4 (2020): 439–54.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. London: Profile Books, 2020.

Robinson, Linda, Todd C Helmus, Raphael S Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva. *Modern Political Warfare: Current Practices and Possible Responses*, 2018.

Rogers, Ann, and John Hill. *Unmanned. Drone Warfare and Global Security*, Pluto Press, London, 2014.

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. “Online manipulation: hidden influences in a digital world.” *Georgetown Law Technology Review* 4, no. 1 (2019): 1–52.

United Kingdom Government. “UK Assess Russian Involvement in Cyber Attacks on Ukraine,” 2022.

United Kingdom Ministry of Defence. “Latest Defence Intelligence Update on the Situation in Ukraine -8 April 2022.” Twitter, 2022. https://twitter.com/DefenceHQ/status/1512284278813597702.