NATO DECISION-MAKING IN THE AGE OF BIG DATA AND ARTIFICIAL INTELLIGENCE

EDITED BY

SONIA LUCARELLI

ALESSANDRO MARRONE

FRANCESCO N. MORO

(Photo credit: European Pressphoto Agency, Peter Steffen)

NATO DECISION-MAKING IN THE AGE OF BIG DATA AND ARTIFICIAL INTELLIGENCE

ACKNOWLEDGMENTS

This publication is the result of the Conference "NATO Decision-making: promises and perils of the Big Data age", organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. The Conference, held online on 17th November 2020, is part of a long-term cooperation among the three institutions and it represents the seventh iteration of ACT's Academic Conference series. The success of the event was due to the joint efforts of the three institutions, and the editors want to acknowledge the ACT's Academic Outreach Team, in particular Mr. Dick Bedford and Lt. Col. Romano dell'Aere, as well as Karolina Muti and Francesca Paganucci from IAI. Opinions, conclusions, and recommendations expressed or implied within this report are solely those of the contributors and do not necessarily represent the views of ACT, University of Bologna, IAI, or any other agency of the North Atlantic Treaty Organization.

NATO ALLIED COMMAND TRANSFORMATION

UNIVERSITÀ DI BOLOGNA

ISTITUTO AFFARI INTERNAZIONALI

"NATO Decision-Making in the Age of Big Data and Artificial Intelligence"

Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro

Researcher: Karolina Muti

ISBN: 978-1-95445-00-0

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Index

WORKING GROUP III

(Photo credit: European Pressphoto Agency, ANSA)

EXECUTIVE SUMMARY

Digital revolution has substantially transformed the world we live in, providing great opportunities but also making societies more vulnerable. Technology makes external interferences cheaper, faster and all-encompassing: citizens can potentially become direct targets of information warfare, all members of a society can be part of conflicts one way or another. From advanced weaponry to command and control, most security-related domains are undergoing deep transformations as data availability and transmission increase exponentially. In this context, three interconnected aspects are explore through this publication with a view to the Alliance's evolution: Big Data and organizational challenges for NATO; hybrid threats to Allies' decision-making; the adoption of AI in the defense domain and NATO's role.

Big Data and Organizational Challenges for NATO. Basing decisions on a much larger amount of information than was previously possible could lead to a real revolution in the decision-making processes of complex organizations, especially because this information would concern different dimensions of reality and it would be constantly updated. Beside the huge quantity of information available, the high speed at which the data are generated and need to be processed is another defining factor of Big Data. Also, they will typically be acquired from diverse sources and their trustworthiness has to be carefully evaluated. Finally, any data can have different value in different phases of the decision-making process. All these features impose specific requirements on organizations that aim at using Big Data to reduce the uncertainty in which they operate. For instance, the huge volume of data compels to acquire new data storage technologies, while the high speed demands new processing tools and the variable trustworthiness and value force organizations to elaborate new methods of analysis. Accordingly, any actor that seeks to exploit Big Data should have clear goals and a well-defined strategy to delineate and implement its specific objectives.

A key issue with Big Data is providing decision makers with data that are truly relevant for their purposes, and not simply interesting. Chief data officers and senior data-related leadership positions will acquire a crucial importance in the analysis of information and in the actual decision-making process, but these positions require a special mix of talent and tools that are currently scarce in many large organizations, especially in the public sector and even more in the military one.

Another key issue lies in the emerging tension between centralization and decentralization of the decision-making process of organizations that are introducing Big Data analysis in their work. Paradoxically, while Big Data should promote widespread responsibility and tactical awareness, at the moment advanced digitalization seems to be linked to clear centripetal forces in large organizations. The centripetal tendency leads towards the de-responsibilization of the lower ranks and to a progressive loss of practice in choosing. Thus, it would be advisable to integrate Big Data in the Alliance's decision-making favoring diffused ownership and devising different tools for different branches of the organization, based on their specificities. It would also be helpful to create well-designed and reliable evaluation procedures to measure the effectiveness of organizational innovations as well as of the execution of the new decision-making processes. In particular, identifying the initial failures is especially important, to learn from them and avoid structural problems.

Hybrid Threats to Allies' Decision-Making. Hybrid threats is a broad category encompassing a variety of actors, actions and targets. As for actors, due to their actual capabilities, intentions and recent track records, China and Russia can be identified as the most gathering threats.

Concerning actions, information is key under several respects. It refers to Big Data and AI taken together, as the latter entails the use of algorithms to learn from the former with a view to exploit the target's vulnerabilities. Digital connections are the underlying infrastructure used to perpetrate hybrid threats in the information domain. Western societies rely on virtual world platforms that can be targeted by potential attackers. Since global networks defy borders and limit state jurisdiction, they are harder to defend and allow potential attackers to act below the threshold of detection and attribution. Hybrid threats also benefit from the unprecedent speed and scope of information. This is not new in principle, but it has reached game-changing levels. On the one hand, managing this massive flow of information is just prohibitive for NATO and its member states; on the other hand, high speed of circulation translates into increased operational tempo.

Hybrid threats may take aim at a variety of targets, yet particularly concerning are offensive actions that might lead to societal polarization, elite disagreement and biased perceptions of foreign actors. These actions have the potential to affect decision-making at different levels, even undermining democratic states' institutions. Accordingly, these hybrid threats could undermine decision-making process of Allies – and by reflex, NATO's too. Decision makers face in particular three main set of problems when crafting a response to hybrid threats.

1) How to respond in non-escalatory ways? Since hybrid attacks exploit the grey zone to create ambiguity, including by manipulating the threshold of detection and granting plausible deniability, decision makers are faced with the risk of overreaction.

2) How to respond in democratic ways? Potential attackers may severely impair the decision-making process of democratic systems, putting under stress, for example, the constraint to abide by domestic and international law.

3) How to get public support? Since hybrid threats are usually covered or difficult to attribute, policy makers also have to persuade the public opinion of the very same existence of the threat.

The AI Adoption in the Defense Domain and NATO's Role. In discussing what AI will mean for allied militaries and the Alliance as such, a basic question should be addressed: is AI a technological revolution or is it an instance of technological evolution? Different pieces of evidence can support both interpretations. It would probably be hard for Allies, from a political perspective, to adapt swiftly to a rapid technological revolution. NATO approach, because of the consensus characterising its procedures, will have to be more evolutionary, granular and nuanced. In any case, it is unlikely to see in the next future AI making decisions for the North Atlantic Council (NAC) or the Nuclear Planning Group (NPG). There are psychological, cultural, organizational, political as well as technical reasons for this. The journey to AI is likely to be rather troublesome. Agile software development, for instance, enables the development of superior software but, at the same time, also calls for different procedures, organizational structures and processes, touching upon organizations' identities, missions and culture.

Another topical issue is the private-public partnership on AI. This is key in the AI race between the US and China – possibly leading to disadvantages for Allies vis-à-vis China – and in the relations between NATO and major civilian companies working on AI and Big Data. There is also the fundamental need to ensure interoperability in a fragmented scenario in terms of the Allies' adoption of AI technologies. NATO has

historically been an important player in the processes of standardization and could be such also in this case. In this context, some creativity may be needed: for instance, should NATO provide cloud computing services, namely enablers, the same way it provides air-space management or ground surveillance? Could the Alliance envision an integration of nationally-owned AI assets as it does for the integrated air and missile defense? These are important questions which, however, highlight the fact that defense is a sovereign issue and most decisions are taken by national governments, not by NATO as such.

The Alliance could play a prominent role in the AI domain. For instance, NATO could establish an AI champion to help Allies understand, adopt and integrate AI. Such champion could start with small projects aiming at validating the effectiveness of the solution, and then it could help Allies in training. A key, related issue in this regard is education and training. Similarly, the importance of wargames, simulations and experimentations is going to grow, and NATO has a role to play here, as the unique avenue to convene allied military and political bodies.

TECHNOLOGICAL CHANGES AND A TRANSFORMED INTERNATIONAL SECURITY ENVIRONMENT

Sonia Lucarelli, Alessandro Marrone and Francesco N. Moro[1]

Digital revolution has substantially transformed the world we live in, providing great opportunities but also making societies more vulnerable and transforming the meaning of state borders. Technology makes external interferences cheaper, faster and all-encompassing: citizens can potentially become direct targets of information warfare, all members of a society can be part of conflicts one way or another. From advanced weaponry to command and control, most security-related domains are undergoing deep transformations as data availability and transmission increase exponentially. This is especially true as the emergence of so-called hybrid tactics contributes to universalize the battlefield. Also, attackers may lose control of their offensive cyber weapons, and 'collateral damages' across the private sector and the public worldwide might be more and more difficult to contain. Less visible, yet important challenges connected with Information Communication Technologies (ICTs) also exist. For instance, data overload can create problems for decision-makers that are unable to detect important signals. Losing sight of how machines make their calculations – a somewhat inherent feature of Artificial Intelligence (AI) – can hinder deeper understanding of phenomena as well as learning, besides having dense ethical implications.

A crucial question for Western societies and governments is how to deal with technological changes by exploiting their many benefits while managing to limit their risks. Broadly speaking, observers have long noticed the potentialities of technologies in the security domain: better situational awareness, early warning against threats and risks, the ability to prevent and/or stop attacks to happen, the use of technology against the adversaries' own technologies, and eventually deterrence of high-end hybrid warfare or, at least, the increase of resilience against it. In particular, in order to harness the potential of new technologies, higher levels of security are needed. While internet is unfortunately not secure by design, it has to be somehow retrofit to guarantee a certain level of protection – for instance by avoiding a single point of failure, developing better firewalls, etc. Ultimately, the digital revolution poses challenges to decision makers both as potential users of new technologies and as leaders of targeted societies. Learning to achieve political aims through the support of technological innovations and at the same time acquiring the ability to prevent and manage interferences, if not attacks, have become paramount.

However, achieving such results is not only about engineering. Technologies need ad hoc governance, organizations and skilled users to properly function. Actually, history is full of examples of good technologies that were improperly used and/or unable to provide the expected gains. Therefore, a joint, multi-disciplinary efforts is needed to think and manage technologies in a more comprehensive and secure way across various domains. For instance, the very same design of AI needs exchanges with social scientists in order to limit

[1] Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus.

analytical biases and increase the quality of data that will then be processed through Machine Learning (ML). Moreover, many public policies involve technologies with a strong security dimension. This is one of the main reasons security standards should be harmonized across individual government's policies as well as among Allies: this is what has been leading NATO's renewed efforts on standardization beyond the strictly military perimeter, for instance towards the 5G domain.

While digital technologies continue to dramatically increase in scope and relevance, they are deeply embedded into the broader geopolitical framework, with the re-emergence of multipolarism and looming great power confrontation. This connection has to be discussed and understood as it affects not only security but also economic and technological domains. The globalized supply chain of technology building block entails vulnerabilities and dependencies on unreliable suppliers. Foreign Direct Investments (FDIs) in high-tech companies, Small and Medium Enterprises (SMEs) and critical infrastructures are guided not only by an economic rationale but also by a politico-military one, and have to be monitored accordingly. Cyber space and, partly, outer space are de facto unregulated global commons where the ability to set regulations and standards could be a matter of competition and/or cooperation among major countries worldwide. The notions of 'whole-of-government' and 'whole-of-society' approaches confirm that these problems should be dealt with comprehensive strategies.

Great and middle powers increasingly rely on stand-off weapons, both physical and cyber ones, able to create damages rapidly, worldwide and on a large scale. This trend is going to be accelerated by AI. Some countries are adopting principles on responsible use of AI, including in terms of control and accountability. However, a vacuum remains in international law. And such vacuum is more difficult to fill because of the aforementioned interaction between geopolitics and technologies. Different powers conceive technology – and what it can bring them in terms of benefits – in different ways, and they are unwilling to regulate internationally this field of competition and warfare.

In such a rapidly changing security environment, NATO and allied activities directly or indirectly defend citizens' daily life. In the age of Big Data, AI and the pervasive use of internet, the challenge is to defend the ever-expanding information environment while maintaining all its functionalities.

Against this backdrop, in the post-Cold War period NATO somehow missed the opportunity to involve Allies and partners in a debate on how defense technologies and norms have been changing with the ICT revolution. The result is that the web is not secure by design, and both private and public actors struggle to mitigate risks and threats in an unregulated environment where attackers are structurally advantaged over defenders. Today, the Alliance should not miss the opportunity twice vis-à-vis Big Data, AI and, broadly speaking, the current and future (r)evolution of ICT. The aim of the 2020 Academic Conference was precisely to explore some fundamental aspects of the challenges and opportunities posed by technological change to the security environment in which NATO works. Below follows a brief introduction to NATO, cyber defense and three sets of issues investigated in closer detail: Big Data and decision-making; hybrid threats to allied decision-making; AI adoption by allied armed forces.

NATO, Cyber Defense and Emerging Disruptive Technologies

NATO begun to focus on cyber defense already in 2008, and over time it built up institutions and frameworks to deal with it from a well-limited military perspective. Allies recognized a cyber attack could lead to the activation of Article 5 of the Washington Treaty on collective defense. In that case, there is a clear procedure

where NATO authorities take the military lead. Article 5 does not prescribe a clear procedure factoring in new technologies. On a regular basis, headquarters and the Secretary General cabinet carry on exercises on situational awareness, whereby they receive intelligence and military advice and are immersed in an information space with blue and red teams. Moreover, every two years, there is a large-scale exercise involving national governments. These efforts aim to build familiarity with the technology-related security challenges. However, further evolution of AI-based cyber attacks can constitute an increasing threat for data-reliant organizations such as NATO.

Beyond cyber defense, the Alliance started to work on the broader issue of Emerging Disruptive Technologies (EDTs) only in 2019, by setting up an innovation board co-chaired by the Deputy Secretary General and the Supreme Allied Commander Transformation. Moreover, a dedicated unit was created in the Emerging Security Challenge Division. Two White Papers were produced, respectively on AI and on autonomous weapons, to provide inputs for Allies' decisions in this regard. The current NATO approach is based on the motto "adopting and adapting", entailing five complimentary goals: (1) better understand emerging disruptive technologies; (2) properly look at their implications for defense; (3) decide about their use; (4) mitigate their risks; and (5) exploit their advantages.

Noticeably, the traditional defense industrial ecosystem entails long planning, oligopolistic supply and monopsonic demand. Over time, it was characterized by substantial technology transfers from the military to the civilian domain (the so-called 'spin offs'), including the very same embryonic Internet. In recent years, several new technologies with relevant implications for security and defense have been emerging from a different ecosystem, marked by bottom-up innovation, a rapid development-to-market cycle, and a technology transfer from the civilian to the military domain. As a result, with the relevant exception of certain space assets and hypersonic technologies, the civilian sector is increasingly developing into the innovation driver, and defense one has become quite dependent. Such a shift implies that priority setting for current and future technology development is not substantially driven by states anymore. In the US, the Pentagon's Defense Advanced Research Projects Agency (DARPA) struggles to develop a dialogue with the private sector gravitating around the Silicon Valley to embrace certain research lines. The NATO Industry Partnership on the cyber domain serves as platform for Alliance's officials and industrial representatives to exchange notes, yet major ICT players do not seem very interested in having such a structured dialogue. Moreover, investments in these technologies require venture capitals and the acceptance of the risks to fail – something which usually states, and particularly Ministries of Defense, cannot afford. The US, the UK, France, Germany, the Netherlands and other Allies made certain steps to adapt their defense innovation models in these domains, but this is only the beginning of a long transformation process.

As a matter of fact, adapting to emerging and disruptive technologies is harder for some Allies than others. The related risk is moving towards a multi-layer Alliance, with some member states holding new technologies, and others not having such advantage. Ideally, the solution would be to collectively adopt certain new technologies, but this represents a challenge for the NATO Defence Planning Process, military procurement, common funding, etc. A technology group of experts has been appointed to reflect upon issues including but not limited to these, and the Secretary General will probably present a report to the next summit of Heads of state and governments.

In this rapidly evolving context, at the 2020 Academic Conference the first Working Group (WG) took a comprehensive view on changes, risks and opportunities related to Big Data and decision-making. The second WG focused on hybrid threats, allied decision-making and possible responses by the Alliance and its members. The third WG was dedicated to AI adoption by allied armed forces, and on NATO's possible role in

this regard. Accordingly, the publication is structured in three sections. Each section is devoted to a specific WG and encompasses two papers that have been presented during the Conference as well as the report summarizing the subsequent debate. As a whole, as for publications resulting from previous Academic Conferences, it aims to offer the reader a complimentary ensemble of thought-provoking views, favor an intellectual exchange between the policy-making and academic communities, and move forward the international debate on these topics.

(Photo credit: European Pressphoto Agency, Felipe Trueba)

WORKING GROUP
I

OPPORTUNITIES AND CHALLENGES IN THE MANAGEMENT AND GOVERNANCE OF BIG DATA

George Christou - University of Warwick

Abstract

The digitalization of 'everything' and subsequent proliferation of data that is available to organizations across different sectors presents major opportunities, but also brings along greater complexity and challenges in relation to the effective governance of Big Data Analytics (BDA). This chapter seeks to explore how organizations have strategically adapted and innovated to manage their BDA approach. Moreover, it assesses how they have navigated the challenges of Big Data analysis in order to harvest its potential power in gaining insight and adding value and advantage, whether in the market place or in relation to the battlefield. It posits that whilst responses and approaches are still very much formative, governance lessons can be gleaned from available experiences in different sectors. This, in turn, can inform the evolution of good practice in the security sector domain as a complement to internally developed responses that are also emerging in organizations such as NATO to ensure BDA provides commanders, intelligence analysts and strategic communicators with clear insight and data on which critical decisions can be taken.

Introduction

The evolution and availability of Big Data is dramatically redefining the opportunity landscapes across and within many sectors – whether business, healthcare, pensions, energy or indeed, government, security and defense. Big Data, in this sense, is understood as "a collection of large data sets that contain massive and complex data" and "data that exceeds the processing capacity of conventional database systems" (Al-Badi, Tarhini and Khan, 2018). In the new governance ecosystems that are emerging to manage Big Data, commercial industry has been at the forefront of innovating to harvest and exploit the advantages and benefits that Big Data can bring; not surprising, given that the Big Data Analytics (BDA) market is projected to be worth USD 103 billion by 2023. Commercial industry then has led the way in in providing examples of the organizational pathways, processes and strategies that are needed to ensure effective and efficient use of the data revolution. As is noted in one report "Companies with good data analytics capabilities…are twice as likely to be in the top quartile of performance within their industries" (PwC, 2019: 3). This, however, does come with one caveat, as other leading industry reports indicate that 'whilst it may come as no surprise that data and analytics are reshaping industry competition…the persistently lacklustre response to this phenomenon by most companies should raise some eyebrows" (McKinsey and Company, 2019: 2).

What the evolving literature points to on BDA is that no strategy will be the same, and that whether an organization is in the business or military sector, strategic adaptability and flexibility are important factors in shaping an approach that is unique to the requirements of its specific goals and objectives (for an overview of key debates and issues see Morabito, 2015; Espinosa and Armour, 2016; Günther et al., 2017; Sivarajah et al., 2017; Ladley, 2020). It is also evident that there are contrasting models being developed for the

governance of BDA, which can be characterized broadly, within a centralized to decentralized spectrum. If commercial industry gets its data analytics management right, there are gains in terms of getting ahead of the competition and increased revenue; for security sector organizations, it can mean gaining a tactical advantage in identifying and responding to threats, predicting the behavior of adversaries, optimising logistics and protecting military networks from attack.

The purpose of this chapter is to show how BDA practices developed in the private and public sectors can provide valuable lessons for those in the military and security sector. It is argued that governance lessons can be gleaned from available experiences in different sectors and that this can inform the evolution of good practice in the military and security sector domain; and this, of course, as a complement to internally developed responses that are also emerging in organizations such as NATO to ensure BDA provides commanders, intelligence analysts and strategic communicators with clear insight and data on which critical decisions can be taken.

The chapter is structured in the falling way: the first section will discuss how organizations across different sectors, in particular the commercial sector, have innovated to manage their BDA approach. The second section will provide an overview of the challenges and pitfalls related to BDA. The third section will then assess what sort of governance lessons can be adapted from the available experiences in other sectors that can inform the evolution of good practice in the military and security sector domain. The final section will provide concluding thoughts on challenges and opportunities going forward in relation to BDA in the military and security sector.

Organizational Innovations and Revolutions in Big Data Analytics

To fully comprehend evolving strategies for governing Big Data, it is first necessary understand what it is – what are its main features and what are the common challenges. Big Data is associated with massive data sets “having larger, more varied, and complex structures that are difficult to store, analyse, and visualise using traditional data processing technologies” (Yang et al., 2019: 2). To this end, when discussing Big Data, it is not just the large volume of data that is important (see Table 1; Yan, 2018: 112). Big Data, according to Mauro et al. (2016), “represents information assets characterised by…high volume, velocity, variety, and veracity” with others having added further important pillars and characteristics such as the virtual, variability and value (Priyadarshy, 2019; see also Van Puyvelde et al., 2017; Moorthy et al., 2015). What most general definitions point to is the need for specific, innovative technologies and governance methods that will allow the transformation of Big Data in to value.

Table 1: *Pillars of Big Data*

Pillars of Big Data	Definition
Volume	The huge quantity of data that is generated and needs to be stored and where new data storage technologies are required accommodate the Big Data.
Velocity	The speed at which the data needs to be generated and processed in order to meet demands and objectives. Particularly important is the ability to process and action data in real-time.
Variety	It refers to the fact that data can come from a number of formats and sources, with three typical types: structured (sensor data, machine data, financial models, etc.), semi-structured (XML documents, emails, etc.) and unstructured (text, videos, audio files, images, etc.).
Veracity	It refers to the truth in and trustworthiness of data. That is, the extent to which any data can be used to make critical decisions by any organization.
Virtual	It addresses the data duplication and lost in transformation related problems whilst enabling better data governance.
Variability and Value	They are inter-related with variability cutting across the other pillars. Variability, in this sense, refers to the different value of data within different phases of the Big Data cycle.

What then, are the main ways in which organizations across different sectors have sought to create governance frameworks that are fit for purpose when it comes to the management of BDA? It can be argued that the public sector and private sector face common but also very different questions and challenges when it comes to Big Data governance. Common, in the sense that data security, data integrity, data quality, data accessibility, data availability and data consistency are generally important within any governance framework for Big Data. Different, because commercial motives for pursuing a Big Data strategy are primarily driven by competition, market advantage, revenue generation (and cost reduction), whereas public sector strategies must consider broader questions beyond the benefits of commercialization, in particular in relation to public interest and societal benefit (Kim & Cho, 2017: 384). Whilst Big Data frameworks are being developed by various governments for a variety of purposes, from crime prevention and healthcare to counterterrorism

and public administration,[1] commercial industry is most advanced in how to exploit data availability and management. It is thus possible to argue that there is much to learn from the commercial sector in terms of organizational innovation and indeed revolution when it comes to developing and implementing Big Data management and governance strategies. How then, have businesses transformed themselves in order to be able to effectively exploit the opportunities of the Big Data era?

There is a general consensus that any organization that seeks to exploit Big Data should have a clear strategy and goals that helps them to understand, define and implement their Big Data objectives (McKinsey and Company, 2019: 3). Similarly, others have argued that "for benefits to be sustainable over time and provide strategic advantage to an organization, the BDA effort will require coordinated…and effective governance" (Espinosa and Armour, 2016: 1117). To this end, any major organizational innovation in terms of Big Data insight must be linked to a holistic consideration of the component parts of any business organization to create an agile architecture and strong governance that will allow the full exploitation of Big Data in the context of ever changing regulatory, technology, business and customer environments – as well as data trends. An important starting point and innovation in this regard then, is to develop a data insights strategy that is collaborative, to ensure buy-in from key stakeholders across the organization more easily. It is argued that by moving away from siloed data-management approaches, stakeholders across an organization become more accountable for how data is used, thereby reducing the risks associated with potential data misuse (Deloitte, 2018: 1).

Beyond this general consensus there are a series of other inter-related issues on creating an effective Big Data strategy that can be found in the existing literature. That is, innovations that move organizations beyond traditional data management methods to governing Big Data through new organizational structures, new skills and new roles.

First, in terms of organizational structure for data ownership, findings show that centralized, decentralized and hybrid forms can work effectively as long as certain conditions are met; the most important being that of establishing a governance framework that allows the various units to work in an integrated rather than siloed manner. Here it is argued that whilst a siloed approach may have worked in the past to improve, for example, information security, such an approach becomes more complex, costly and less effective, in a Big Data environment where external and internal data sources grow, and where for such data to have value to the organization as a whole, it must be of high quality and be in presented in a single, consistent format. Big Data in this sense, must be normalized appropriately to be read by Machine Learning (ML) or Artificial Intelligence (AI) algorithms (Deloitte, 2018: 5). What should also be borne in mind when considering the type of structure for any data ownership is that any organization should have the ability to adapt according to its needs (or level of maturity in BDA) and the changing data environment; to this end, companies may start with a decentralized model but may transition to a centralized model over time or centralize in the first instance and transition to a hybrid model. Additionally, it is argued that whilst data ownership should not be

[1] According to the World Bank Group the "United Kingdom, the United States, Singapore and Korea are among many that have adopted high-level Big Data strategies" – with France, New Zealand, Australia and Japan among others that have developed Big Data strategies (2017: 1). Some examples of successful ways in which BDA have been used include public security and public utilities. In terms of public security, Predpol, a predictive policing application has been used in 50 US cities and which analyzes basic data, such as crime type, dates and location, to help law enforcement agencies make better policing decisions; with Brazil, the UK and the Netherlands using similar approaches. Similarly, in terms of public utilities, Shanghai's municipal government has installed sensors throughout the city's 3.300-kilometer water pipe network. These sensors allow the authorities to identify precise locations of issues such as leaks, dramatically reducing response times, infrastructure damage, maintenance costs and service disruption (World Bank Group, 2017: 4-6).

centralized, data governance should, with top performing companies "often having data centralized within business units" (McKinsey and Company, 2019: 3). Indeed, the evidence suggests that in locating a BDA unit, organizations should ensure that it is cross-functional, integrated and accessible to ensure it can break through inertia and enable transformation (McKinsey and Company, 2019: 3-4). Whether in the public or private sector, locating a BDA unit with an information or business intelligence unit (e.g. a Centre of Excellence - CoE) is a more productive organization-wide strategy than trying, for instance, to locate it in specialized units such as IT, where staff might not possess the requisite ability to manage agile BDA functions.

Another important organizational innovation relates not just to the overall nature and location of BDA in an organization but leadership and data culture (PwC, 2019: 13). There are several aspects to this, including new roles, skills and education. For example, within the financial services sector there is evidence to suggest that in order to maximize the strategic use of their data – including Big Data – Chief Data Officers are required to provide "strategic guidance and execution support, and also to assure access to and the quality of critical data". It is argued that senior data-centric leadership positions are crucial to both manage and govern data, but importantly in a Big Data environment, leverage the data using emerging technologies "that can generate actionable analytical insights and tangible business benefits" (Deloitte, 2016: 2). Evidence also suggests, more broadly, that another key ingredient for a successful BDA strategy is creating a data culture through organizational leadership. This incorporates "a set of practices that brings together data talent, tools, and decision-making so that data becomes the default support for company operations" (McKinsey and Company, 2019: 5).

Key differentiators in high-performing companies in this regard are data leadership, the accessibility of data tools to frontline employees, an organizational culture that supports rapid iteration and tolerates failure, education (ensuring that employees trust Big Data, understand its value, its strengths and limitations), the ability to attract and retain talent, and an underlying technology that can adequately support Big Data exploitation and analytics. To this end, and in terms of talent, it seems that companies are in most need of 'translators' – or those that can bridge the gap between any BDA unit and other parts of the business. Indeed, even though many data-management processes are now automated (from sourcing and cleaning data, to ensuring data quality, reporting and visualization), management of such data is still reliant on human activity – and therefore talent – not just in terms of translators that make sure sophisticated models are translated into simple, visual tools for supporting front-line staff, but also data scientists, engineers and analysts that support them. The companies that have managed to retain talented staff successfully are those that have constructed clear opportunities and career paths that can ensure transitioning to other roles and learning from those within the data analytics team with different roles. To fill any remaining gaps, such strategies have often been accompanied by strategic partnerships with other organizations to access skills and talent required (McKinsey and Company, 2019: 5-7; McKinsey and Company, 2018: 4-6).

Finally, in terms of success in a data-centric culture, technology infrastructure has been seen as critical for achieving organizational objectives in data analytics; indeed, it is ranked second only behind BDA strategy as the most difficult challenge for an organization. Here, the evidence suggests that traditional data architectures that are characterized by technology that is inflexible and complex (and often more costly) with data stored across a variety of dispersed technologies, are not fit for purpose when it comes to BDA. Surveys show that more agile and robust data architecture "allows you to add more applications or new technological enhancements as needed, and makes it easier to cohesively manage data" stored in a variety of locations (Deloitte, 2018: 5). It also allows companies to support the rapid collection and sharing of data, access and

use of that data, and high levels of data quality; the latter being particularly important in driving data analytics adoption across an organization (McKinsey and Company, 2019: 8).

The type of organizational and technological structure within an organization is also important in relation to another critical issue in BDA – that of data privacy and security across the management and governance life-cycle (Yang et al., 2019: 6-10; see also Espinosa and Armour, 2016: 1113); that is, from data collection, storage and processing, to data classification, visualization and use. A critical question for many organizations has then been how the potential of Big Data can be realized whilst effectively managing and mitigating security risks. The evidence suggests that this is a real and growing problem as companies increasingly gain value from BDA; indeed, 4.1 billion records were reportedly stolen or exposed through cyber attacks in the first six months of 2019. To this end, it is suggested that organizations fare better when they adopt and implement a data-centric security strategy that can protect information that is sensitive within a BDA ecosystem and that does not impact on the ability of organizations to use data in existing applications and systems (Rosbach, 2020; see also Gupta, 2016). To elaborate further, such an approach should also be compliant with any regulatory requirements to ensure that any data used that contains sensitive information is protected and privacy ensured (Kim & Cho, 2017: 385).

Furthermore, the European Union Network and Information Security Agency (ENISA), in its report on Big Data security across the use cases of Telecoms, Energy and Finance, identified a series of challenges, but also best practices, including: strong and scalable encryption to ensure data confidentiality and integrity; high levels of application security including regular security testing procedures; compliance to standards and certification to help ensure interoperability between applications and maintain good levels of security; secure use of the Cloud including clear risk assessments, Service Level Agreements and resource isolation and exit strategies; robust source filtering (security of endpoints); access control and authentication (relating to authorized users and entities); and finally, Big Data monitoring and logging (ENISA, 2015).

Avoiding the Pitfalls of Analyzing Big Data

Given that Big Data and BDA are valuable to those in the public and private sector, and there exists a plethora of organizations that are still in the construction phase of a BDA strategy, this section will seek to outline and discuss challenges and common pitfalls that should be avoided in the planning and implementation phases. To this end, such challenges continue to evolve as BDA develops within a dynamic data and digital technology environment, and thus must be understood in this context; with strategies for analysing Big Data being agile and flexible enough to adapt to changing needs across data process, management and governance aspects.

Within the commercial world, analysts have pointed to a number of pitfalls that companies should try to avoid when seeking to develop BDA for the purpose of maximizing insights and benefits from Big Data.

The first is to ensure that there is a clear understanding of where an organization can create more value and what data assets are needed for that end, so that there is a clear idea of the investments that will need to be made in terms of data, and in particular their processes, management and governance. Any additional investment in this context must then be consistent with strategy and goals – whether in the business or the public sector. Evidence suggests that organizations which do not undertake a clear assessment of the value and strategic use of Big Data can often find that such opportunity turns out to be costly, ill-defined and poorly implemented, falling short of any initial expectations. From a commercial perspective, any assumption about the value of BDA must be well-informed, linked to all elements of the business and customer need, and it

must have a clearly defined case on how it would enhance overall business (PwC, 2019: 4-5; Krishnan, 2014; McKinsey and Company, 2018: 5). Similarly, from a public sector perspective, there must be clear strategic goals and criteria in relation to the purpose and value of using Big Data, and the benefits – governmental and societal – that this might bring over and above traditional sources of data collection, use and outcome.

The second pitfall consists in ensuring that any technological solution for BDA is sufficiently thought through in terms of data integrity and data architecture and more broadly, in relation to organizational preparedness in the introduction of any new technologies so that risk can be appropriately mitigated (Kim & Cho, 2017: 387). There are several elements to this. First, the question of how and at what speed any new technology should be introduced. Some companies have gone for 'revolution' and full transformation technology through replacement of their existing software, hardware and analytics stacks simultaneously, instead of replacing each aspect incrementally. According to McKinsey and Company, however, those that have pursued this strategy – purchasing top end technology for each function – have often found a lack of interoperability between them so "that none of them 'talks' to each other" (2018: 5). Others have also pointed to the need to ensure that the maturity of any technology introduced is fully understood and fits with the organization and for the purpose that it is needed, to ensure maximum benefit (Krishnan, 2014). Overall then, and given that technologies can become obsolete within a matter of a few years, organizations should consider taking a more functional approach to building systems with any new innovations deemed fit for purpose being integrated at a later date.

The third difficulty relates to change management, integration and ensuring the right skills are available to process and implement a successful BDA strategy. This very much pertains to two points made in the previous section. First, on data culture and creating this all the way through the organization with a commitment from the very top to the very bottom of any structure. Second, on the integration of any data analytics strategy and team into the rest of the organization, rather than being isolated and detached from overall organization goals and objectives. The important lesson learned from industry experience suggests that first all stakeholders must commit on BDA and, second, processes of accountability should be built in BDA in order to in order to ensure its proper delivery over time. To this end, there must be equal consideration to people and process as well as technology; ensuring the right people are in place with the right skills (and talent) is critical for an effective BDA strategy, as is putting the right incentives and mechanism in place to train and retain the talent needed (Krishnan, 2014; McKinsey and Company, 2018: 5; McKinsey and Company, 2019: 7-8; Expert Panel, Forbes Technology Council, 2015; PwC, 2019: 13).

The fourth pitfall concerns the various attributes of Big Data and the ways in which organizational processes are put in to place to avoid problems relating to data preparation, relevance, quality, granularity, context and complexity (Krishnan, 2014). This is very much related to ensuring that organizations think clearly about the data life cycle, creating clear guiding principles for challenges not only related to the characteristics of data itself, but also to Big Data processing techniques and challenges concerning risk, security and privacy (including regulatory compliance) (see Rahul and Banyal, 2020). To this end, there must be robust and well-defined governance and infrastructure frameworks for Big Data which, whilst inevitably varying across organizations according to their needs, will enable effective achievement of BDA strategies and goals (Yang et al., 2019: 10-11; Kim & Cho, 2017: 389).

The fifth difficulty relates to execution, testing and learning. Once there is a clear goal connected to an organizational strategy, it is also essential to think about where and how this can work and, in critically, why it might not. For the latter 'fail' scenario in particular, it is important to create processes that allow a thorough evaluation of implementation and execution procedures based on measurable criteria for success. This way,

the organization can determine whether and how any identified problems can be solved, and how it is possible to learn from any initial failure. Here it is once again important that, in implementing the test process, there are clearly defined responsibilities and roles for personnel with the implementation team, and that they have the requisite skills to provide an informed view of successes and failures in BDA strategy – i.e. if and how the latter can be remedied, and how the former can be built on to ensure further success going forward (PwC, 2019: 11).

In conclusion, the above is not an exhaustive list of pitfalls encountered by all organizations in relation to Big Data, but draws from recent literature and research on private (and certain public) sector organizations in their development of BDA strategies. They are therefore some of the most important common difficulties which, if avoided, will allow organizations to develop their own strategies through important lessons learnt across sectors – and in particular from commercial leaders – that have engaged and sought to implement effective BDA strategies.

Good Governance Practices in the Security Sector Domain

This final section of the chapter will reflect on how far practices in the public and in particular commercial sector discussed thus far might be transferable to the security sector domain – and indeed, how far security sector organizations and governments have started to develop their thinking regarding the use and challenges of BDA. What are the main lessons that can be transferred to the security sector and what has the security and defense sector learnt thus far in relation to constructing effective BDA strategies fit for purpose? It can be argued here that whilst there are fundamentally different rationales for developing BDA strategies between the commercial (monetization, profit, etc.) and security and defense sectors (strategic and tactical advantage, real-time field and operational intelligence, etc.) – the general issues to consider remain similar if any such strategies are to be successful in relation to the pillars of Big Data and indeed the technological architecture (software, hardware and analytics stacks), organizational process, culture and models of governance.

Just like with the commercial and public sector, then, technological progress has allowed militaries and security sector professionals to gather large amounts of data, and a number of countries (governments and armed forces) are in the process of constructing and implementing governance models to ensure the benefits of Big Data in terms of real time intelligence, enhanced decision-making, situational awareness and overall competitive edge against increasingly capable opponents. The synergy between Big Data, ML and AI is particularly important in this context when it comes to all aspects of combat readiness, with experts agreeing that AI and its application in the armed forces is “present in all domains…and all levels of warfare” (Svenmarck et al., 2018) with the potential to have a transformative impact on national security technology (Allen and Chan, 2017; see also Tonin, 2019). Many, however, are at an early stage in the development of any BDA strategy. Thus, the lessons from other sectors – and indeed leading governments and security organizations – can provide guidance on best practice as they move from their ‘data’ governance models to ‘Big Data’ governance frameworks that will give them the ability to ensure maximum value and advantage is extrapolated from the BDA life-cycle.

The first lesson or best practice relates to having a clear rationale, goals and guiding principles in place to ensure effective governance of Big Data in the organization. This includes strategically assessing the type of model required, based on current capabilities, resources and future needs, i.e. decentralized/centralized/hybrid. More importantly, governments and security organizations need a clear

understanding of the value of Big Data across different domains (land, sea, air) and landscapes (human, physical, information) so that high quality, usable, real-time information can be delivered through AI and ML at strategic, tactical and operational levels. This is certainly recognized in the NATO context, with a Dutch Position Paper highlighting that, in terms of Big Data and AI, "the focus should be on assessing and…demonstrating the added value that innovations can provide to NATO military theatres" (Smallgange et al., 2018). This is critical, so that the full possibilities of influencing the three landscapes – through situational awareness and effective command and control – can be developed in a broader way than that offered by traditional military means. This way, there is also a recognition that in order to take full advantage of the data-centric technologies (BDA and AI), a data-centric methodology is required, so that effective support can be offered at different levels (Blunt et al., 2018).

In the second place, related to the first lesson learned, in a military and security context where there is often a unified command in combination with tiered formal hierarchy that tends towards specialization, there can also be structural inefficiencies in the flow of information; operating jointly can thus often come at a high cost (Zelaya and Keeley, 2020). When considering any data-driven methodology, then, much thought has to be given to the organizational data management life cycle – including how to integrate the use of BDA and new technologies (e.g. AI, ML) with human decision-making, control and communication of information. Indeed, it has been argued that whilst BDA and associated technologies offer significant advances in rapidly collecting, processing and deciphering complex forms and varieties of data for the purposes of action, the human element is still critical in contextualizing any such data and offering insights on the complexity and "shades of grey" that might be missed by BDA (Van Puyvelde et al., 2018: 1414; see also Desclaux, 2018: 9). To this end, thought has already been given to the implementation of the Observe, Orient, Decide, Act (OODA) loop to determine the type of decision support required and how meaningful human control can be enabled. The OODA perspective or approach, it is argued, represents "the life cycle from data acquisition to decision making and also reflects how sophisticated a technology should be in order to provide value" (Smallgange et al., 2017: 6). An important element within this loop is giving full consideration to any legal, ethical and moral questions that arise in relation to action and particularly the use of lethal autonomous weapon systems (LAWS).

The third best practice relates to buy-in from the organization as a whole. That means not just having the technology, tools and mechanisms in place within a data driven environment that ensures access to and use of Big Data for all team members, but also:

a) Leadership from those at the top (Commanders) and within the different echelons of command within and across domains, landscapes and levels through to data engineers, analysts, assessors, translators – and the ability of the various communities of interest to use data communicated to them in an effective way;
b) The creation of an organizational (big) data-driven culture and data-centric paradigm – including ensuring that all relevant staff are data literate, have the requisite skills, literacy and readiness, and are provided with the education, training and skills to operate effectively.

To this end, NATO has identified a key capability gap when it comes to literacy and readiness and has also recognized that in terms of recruiting AI specialists, engineers and data scientists the pool of talent is shallow and it can be difficult to compete with Big Tech companies.

Here, leading national governments in developing their Big Data strategies have sought to ensure the requisite investment is in place going forward for developing a (resilient, secure and trusted) technology

architecture and recruiting the right talent. They have also, alongside leading security organizations such as NATO, recognized that partnerships (in particular with industry) and contracted services, as well as in-house expertise, that will be needed to deliver and sustain the necessary skills and understanding for assessing, interpreting and communicating information in an effective way (Tonin, 2019; Blunt, 2018; Defence IQ, 2020; Big Data for Defence, 2019). Finally, the non-defense commercial/industry sector will not just be important in terms of the skills and expertise element, but also for technological adaptation and integration, given that many innovations stem from commercial companies; the UK government, for example, has awarded IBM a GBP 3.8 million deal for the development of an AI-powered military software platform prototype (Defence IQ, 2020). More broadly, governments and security sector organizations will have to overcome certain hurdles – organizational, cultural, and incentive structures – to ensure that new technologies are adapted so they can bring advantages across strategic, tactical and operational levels (Kostopoulos, 2019: 9) and allow efficient and effective decision-making when needed.

Conclusions

This chapter has highlighted the central ways in which commercial organizations have been successful in constructing and executing a BDA strategy, and discussed the main pitfalls that organizations should seek to avoid in embarking on any such strategy. In this context it is clear that there are many lessons to be learnt and best practices that can be adapted by the security sector in relation the integration of BDA into existing strategies. Indeed, a cursory look at the leading nations with regards to Big Data strategies – and security organizations such as NATO – demonstrate that their central objectives have been developed (and appropriately adapted) with commercial best practice in mind in relation to data management, governance and analytics.

To this end, there are general principles for success that are underpinned by a need for a clear rationale, goals and strategy, a strong leadership, an agile, resilient, secure and adaptable technical infrastructure, a data-centric approach and methodology, and a data culture that permeates the whole organization. Of course, this chapter did not have the space or scope to discuss the micro-level BDA requirements within the security sector in relation to all dimensions, and in particular innovative hardware and software architectures or indeed process techniques and challenges.

What is clear going forward, however, is that the security sector will face challenges of a technical and non-technical nature that will require financial investments in AI systems and human talent, as well as cooperation and collaboration with industry and leadership, if BDA strategies are to deliver the advantages expected to those engaged at strategic, tactical and operational levels. In this, lead nations and organizations, whilst not starting from scratch, have clearly started to negotiate the steep learning curve when it comes to Big Data and decision-making (Street et al., 2019). They are at a formative phase of development with regards to constructing and implementing strategies and governance frameworks, and indeed modelling and simulation environments, tools and techniques to allow them to derive maximum value from Big Data. The journey ahead, however, whilst entailing certain risks, is also an opportunity – if objectives and goals are clearly defined, strategies grown and adapted according to ever-changing needs, data and technological environments, and data governance and management practices enabled by strong leadership are underpinned by a philosophy of date-centric methodology, technology and clear legal and ethical code of conduct. Testing (through exercises, simulations, etc.), failure and the ability to reflect are important components of evolving and (re)defining BDA governance so that real value can be extracted in real time,

with trustworthy and accurate data, and systems, technology and skills required to exploit data all the way through the decision-making process are sustained.

References

Allen, Greg & Taniel Chan (2017). "Artificial Intelligence and National Security". In Belfer Center for Science and International Affairs.

Al-Badi, Ali, Ali Tarhini and Asharul Islam Khan (2018). "Exploring Big Data Governance Frameworks". In Procedia Computer Science 141, pp. 271–277.

Big Data for Defence (2019). 2019 Trends Report.

Blunt, Richard, Chris Riley and Marc Richter (2018). "Using Data Analytics and Machine Learning to Assess NATO's Information Environment". In NATO Science and Technology Organization.

Defence IQ (2020). "2020 Market Report: Programmes and Investments for Big Data in Defence".

Deloitte (2019). "Developing a Data Insights Strategy: How to extract value from your data".

Deloitte (2016). "The evolving role of the chief data officer in financial services: From marshal and steward to business strategist".

Desclaux, Gilles (2018). "Big Data and Artificial Intelligence for Military decision-making." Keynote speech, NATO IST 160 Specialists' Meeting.

Espinosa, J. Alberto & Frank Armour (2016). "The Big Data Analytics Gold Rush: A research Framework for Coordination and Governance". In Hawaii International Conference on System Sciences, IEEE.

ENISA (European Network and Information Security Agency) (2015). "Big Data Security: Good Practices and Recommendations on the Security of Big Data Systems".

Expert Panel, Forbes Technology Council (2015). "Don't Make These 14 Common Big-Data Mistakes at Your Business". In Forbes.

Günther, Wendy Arianne, Mohammad H. Rezazade, Mehrizi Marleen Huysman and Frans Feldberg (2017). "Debating big data: A literature review on realizing value from big data". In The Journal of Strategic Information Systems, Vol. 26, No. 3, pp. 191-209.

Gupta, Vinhor (2016). "The benefits of Big Data Analytics in security". In City Security Magazine.

Kim, Hee Yeong & June-Suh Cho (2017). "Data Governance Framework for Big Data Implementation with a Case of Korea". IEEE International Congress on Big Data, pp. 384-391.

Kostopoulos, Lydia (2019). "The Role of Data in Algorithmic Decision-Making". In UNIDIR (United Nations Institute for Disarmament Research).

Krishnan, Krish (2014). "10 mistakes Enterprises Make in Big Data Projects". In IBM Big Data & Analutics Hub.

Ladley, John (2019). Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program. Amsterdam: Elsevier.

Madsen, Anders Koed, Mikkel Flyverbom, Martin Hilbert and Evelyn Ruppert (2016). “Big Data: Issues for an international political sociology of data practices”. In International Political Sociology, Vol. 10, No. 3, pp. 275-296.

McKinsey and Company (2019). “Catch them if you can: How leaders in data and analytics have pulled ahead”.

McKinsey and Company (2018). “Building an effective analytics organization”.

Moorthy, Janakiraman et al. (2015). “Big Data: prospects and challenges”. In Vikalpa, Vol. 40, No. 1, pp. 74-96.

Morabito, Vincenzo (2015). Big Data and Analytics: Strategic and Organizational Impacts. Switzerland: Springer.

PwC (PricewaterhouseCoopers) (2019), “Creating Value from Data: Why you need to take a strategic approach to maximise the value of your data”.

Priyadarshy, Satyam (2019). “Big Data Play in Oil and Gas”. In CIO Review.

Rahul, Kumar and Rohitash Kumar Banyal (2020). “Data Life Cycle Management in Big Data Analytics”. In International Conference on Smart Sustainable Intelligent Computing and Applications under (ICITETM2020).

Rosbach, Felix (2019). “Big Data is everywhere, and security isn’t…but it can be!”. In ITProPortal.

Sivarajah, Uthayasankar, Muhammad Mustafa Kamal, Zahir Irani and Vishanth Weerakkody (2017). “Critical analysis of Big Data challenges and analytical methods”. In Journal of Business Research, Vol.70, pp. 263-286.

Smallgange, Antoine, Harrie Bastiansen, Auke Venema and Adalbert Bronhorst (2018). “Big Data and Artificial Intelligence for Decision Making: Dutch Position Paper. In NATO Science & Technology Organization.

Street, Michael, Peter Lenk, Ivana Ilic Mestric and Marc Richter (2019). “Lessons Learned from Initial Exploitation of Big Data and AI to Support NATO Decision Making”. In NATO Science & Technology Organization.

Svenmarck, Peter, Linus Luotsinen, Mattias Nilsson and Johan Schubert (2018). “Possibilities and challenges for artificial intelligence in military applications”. In: Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists’ Meeting, NATO Science & Technology Organization.

Tonin, Matej (2019). “Artificial intelligence: Implications for NATO’s armed forces”. In NATO Parliamentary Assembly, Science and Technology Committee, Sub-Committee on Technology Trends and Security (STCTTS).

Van Puyvelde, Damien, Stephen Coutlhart and M. Shahriar Hossain (2017). “Beyond the buzzword: big data and national security decision-making”. In International Affairs, Vol. 93 No. 6, pp. 1397-1416.

World Bank Group (2017). “Big Data in Action for Government: Big Data Innovation in Public Services, Policy and Engagement”.

Yang, Longzhi et al. (2019). “Towards Big Data Governance in Cybersecurity”. In Data-Enables Discovery and Applications, Vol. 3, Article No. 10, pp. 1-12.

Yan, Zheng (2018). “Big Data and Government Governance”. In International Conference on Information Management and Processing, IEEE, pp. 112-114.

Zelaya, David & Nicholas Keeley (2020). “The Input-Output Problem: Managing the Military’s Big Data in the Age of AI”. In War on the Rocks.

DIGITALIZATION IN MISSION COMMAND AND CONTROL: FRAGMENTING COORDINATION IN MILITARY OPERATIONS

Paolo Spagnoletti & Andrea Salvi - LUISS University

Abstract

Does digitalization hinder the implementation of Mission Command? This chapter investigates how the doctrine of Mission Command reacts to the centripetal force exerted by the growing use of digital technologies in military High Reliability Organizations. Uncertainty is a systemic feature of military operations and organizations needed to devise practices and tools which possess suitable capabilities to address environmental constrains and ensure reliability. In this context, military organizing has been successfully centered on Mission Command: a doctrine that emphasizes diffused leadership to attain strategic objectives. Nonetheless, the advent of digitalization and the deployment of digital systems may challenge this doctrine. Remote-controlled technologies, automatic arms systems and data analytics tools have seen a widespread application in modern warfare. Such advancements favor Command and Control approaches whereby commanders can obtain an intimate awareness of the battlefield. This scenario may progressively lead towards task-oriented organizing that heavily relies on control over the structure, rather than on more flexible, agile and mission-oriented organizing. This shift, in turn, may have consequences for the entire command pyramid as: (1) it may cause a progressive lack of accountability in subordinates, (2) it may reduce practice in decision-making in operative functions, and (3) it may decrease trusts between higher level decision-makers and frontline operators. This chapter evaluates the tension between the centripetal force of digitalization and the diffused leadership of Mission Command, proposing avenues for balancing stances. Mission Command can, in fact, benefit from the affordances of digital tools that points towards fragmented coordination.

Introduction

Military organizations have always needed to account for 'the unexpected', as they operate in systemically uncertain environment. Clausewitz (1982) highlighted the relationship between war and chance. Such systemic uncertainty posits the need for military organizations to devise practices and tools which possess suitable capabilities to address environmental constrains and ensure resilience. Military organizations can be framed as High Reliability Organizations (HROs) with regards to the aspects that pertain their operative and their front-line organizing. In this case, there are many similarities with HROs that had been widely researched and investigated (Fraher et al., 2017; Weick & Roberts, 1993; Weick & Sutcliffe, 2006) . Because of the high potential magnitude of errors, these organizations face longer "crises": they are considered as processes rather than single points in time (Williams et al., 2017). For these organizations, resilience is not considered as a goal – or an endpoint – but as a continuous operational process. It requires a special 'mindset', to which the literature refers as "collective mindfulness" (Fraher et al., 2017; Weick & Roberts, 1993; Weick & Sutcliffe, 2006). It substantiates in the efficient capacity of detecting and correcting errors originated from uncertainty through a series of heedful processes (Mohun & Sagan, 1995; Salovaara Lyytinen

and Penttinen, 2019). Mindfulness is achieved through the cultivation of five hallmarks chronic preoccupations: failure, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise (Weick & Sutcliffe, 2006).

This chapter looks at Mission Command as a manifestation of collective mindfulness for HROs. Mission Command (*Auftragstaktik*) is a doctrine born to address these environmental constraints through diffused leadership to attain strategic objectives set by the higher ranks. In other words, in a Mission Command framework, the goal is identified and indicated at the top of the command chain – how to reach said goal is delegated to lower ranks and to specialists. Decisions in this context are a by-product of a thorough situational analysis that encompasses evidence from the battlefield, condensed in tactical decisions and abiding the strategic address laid out by high-rank decision makers. Such a course of action requires high levels of cooperation and trust at multiple levels. In first place, lower units – at all levels – need to be aware of the strategic goals set by the commanding officers and – most importantly – they need to embrace and share their rationale. Secondly, horizontal coordination is required: the operating units need to trust each other. Thirdly, lower officers need to fully embrace the logic of mission command and take initiative to accomplish the mission.

Such doctrine is in stark contrast with the so-called "managerial approach" adamantly adopted and renown among the ranks of the US Army almost until the Vietnam War (Shamir, 2010). The latter was heavily reliant on traditional "business oriented techniques": decisions were taken from above, making use of large volumes of data. As Shamir (2010: 649) puts it: "the managerial approach is characterized by centralization, standardization, detailed planning quantitative analysis and aspires for maximum efficiency and certainty". In other words, the command chain promoted and enforced a purely vertical doctrine of command, rewarding compliance with meticulously detailed orders and discouraging deviance from the established pathway.

Starting from the eighties, both the British and American Army progressively turned into a more decentralized philosophy of command (Farrell, 2008; Shamir, 2011), better suited "to contend with the demands, uncertainties and frictions of command in war" (Yardley & Kakabadse, 2007; British Army, 1995). Said management methodology has been codified in doctrinal documents (see e.g. US Department of the Army, 2014; NATO, 2010; UK MoD, 2014), and most military organizations have adapted to it and took measures to implement it in manoeuvre warfare. These measures include extensive training and leadership programs as well as renewed tactical practices. Empirical and anecdotal evidence suggests that Mission Command increases operative efficacy (Yardley & Kakabadse, 2007). Moreover, it fosters widespread engagement and diffused ownership. Given that "no plan survives the first contact with the enemy" (Hughes, 1995), flexibility and freedom of action are values to be actively pursued: "This requires understanding your superior commanders' intentions, flexibility of mind, rapid decision-making, good organisation and good communications" (UK MoD, 2014: 31). Despite this promise of success, the literature argues that modern military theory is grounded on Mission Command, but the extent to which extent it has been implemented at various levels is rather unclear (Shamir, 2010).

Yet, the growing use and the organizational implementations of real-time control system technologies have led to the renaissance of direct supervision and micro-management practices (Storr, 2003). Given the availability of fine-grained and detailed data, commanders have an incentive to centralize the decision-making process pushing towards a more task-oriented approach. The new wave of digitalization has brought cutting-edge remote-controlled technologies, automatic arms systems and data analytics tools that have seen a widespread application in modern warfare and in recent campaigns. High-rank officers can de-facto

monitor and control the battlefield from afar, providing platoons with real-time orders. This approach led to the resurgence of Command and Control (C2), deemed a re-emergent doctrine mainly in Western and technology-intensive armies (Connor, 2002). In principle, these systems are able to provide commanders with clear insights from the operative ground and with a level of "intimacy previously reserved for the men in the trenches" (Shamir, 2011: 166). As a result, according to the critics of this system, flexibility and initiative will be hampered with the result of a progressive de-responsibilization of subordinates (Bateman, 1996). Thus, digitalization seems to be intrinsically in contrast with Mission Command, as "C2 leaders" would be prone to establish a more direct control over the structure. This is problematic for the entire command pyramid: "remote commanders" are less likely be warranted trust from the lower ranks.

This chapter conceptualizes the tension between the centripetal force of digitalization and the diffused leadership underlying Mission Command. It critically reviews the main contributions in the field and concludes that digital tools may be shaped in such a way to favor Mission Command, instead of contrasting its core principles. In other words, Big Data, and other advanced data-driven coordination tools, can be used as means to foster widespread responsibility and tactical awareness in extreme contexts. Therefore, the goal of the analysis is to discuss affordances and constraints of digitalization in command and control of military operations.

The first part of this chapter reviews the concept of Mission Command and presents evidence of its applications and adaptations in contemporary military organizations. The second part will discuss the limits of Mission Command vis-a-vis the digitalization. Furthermore, the study will present the main feature of the C2 approach that supposedly better fit a digitized army. Lastly, it will evaluate the co-existence of digital tools and Mission Command exploring avenues for a balancing stance. This work aims to make a contribution to the field of organizational studies and to that of military studies. It constitutes the first step of a broader project that will test the authors' claim, empirically resorting to interviews and focus-groups.

Mission Command

As recounted above, Mission Command is a doctrine that rests upon the concept of diffused leadership in order to create flourishing grounds for initiative and flexibility. Decision are therefore a by-product of the situational awareness of field officers in harmony with the intent provided by the commanding officers. Responsibility, intent and trust are key elements for this doctrine to yield increases in efficacy (Storr, 2003). Its theoretical foundations root in the framework of the manoeuvrist approach (Bungay, 2005; Hooker, 1993; Pech & Durden, 2003; Yardley & Kakabadse, 2007). According to the Joint Doctrine Publication 0-01 (2014: 29):

> "The manoeuvrist approach to operations applies strength against identified vulnerabilities, including predominately indirect ways and means of targeting the intellectual and moral component of an opponent's fighting power. Significant features are momentum, tempo, and agility which, in combination, aim to achieve shock and surprise."

Its origin can be traced back to the Prussian Army at the wake of the Nineteenth Century.[1] The harsh defeat in Jena had proven the Prussian rigid model of command obsolete (Shamir, 2010 and 2011), particularly

[1] Other countries' organizations provided virtuous examples of diluted leadership as well. Storr (2003), for instance, recounts examples from the British Navy. Among others, Admiral Horatio Nelson made use of a similar model in battle of Trafalgar.

against the flexible and "more utilitarian" French Army (Bungay, 2005; Yardley & Kakabadse, 2007). Bungay (2005) uses McGregor's (1960) theoretical framework of X and Y organizations applied to the two belligerents' forces (Yardley & Kakabadse, 2007). In particular, the Prussian Army embodies "Theory X": an organization based on direct management and a C2 tactical warfare. This implies that soldiers de facto need precise directions. The Republican French Army, conversely, made a manifest example of "Theory Y": highly utilitarian, strongly self-controlled and actively engaging with responsibilities. A similar parallel in Yardley's review encompasses the work of Cameron and Quinn (2011) on visions of leadership. In this context, the Prussian Army embodied the "traditional hierarchy" in terms of organizational culture. On the other hand, the French Army had been labelled as an adhocracy – a system that rewards bold, innovative and creative leaders.

Helmuth von Moltke capitalized the changes at the middle of the Nineteenth Century to propose and implement deep changes that resulted in a new form of leadership (Widder, 2002): the *Auftragstaktik*. The mantra was initiative, aggressiveness, and subordinate freedom of action (Echevarria & Antulio, 1986). This model had been progressively incorporated in the military apparatus, becoming a pillar of the formative process of officers in the Kriegsacademy (Shamir, 2010).

The footprint of such a paradigmatic shift can be found even in the World Wars: the Wehrmacht performing at high levels of tactical effectiveness (Storr, 2003).[2] Conversely, the American and British forces on average tended to adopt a more centralized and managerial structure of command. In fact, "the hunger for information at the top produced an information overload resulting in long lead times needed in order to prepare and launch operations" (Shamir, 2010: 652). Constant communication was a dogmatic approach in this organizational structure based on vertical command (Van Creveld, 1985). This model was further exacerbated by the Americans during the Vietnam War. Higher ranks not only ruled on the strategic dimension, but on the tactical domain as well: decisions were taken based on daily fine-grained statistics.[3] In sum, across the major war, the US Army relied more on numbers, attrition, massive firepower and vertical control than on tactical brilliance (Boot, 2003; Shamir, 2010). As often happens, there were some deviant cases. The tactical acumen and the spirit of initiative of some units emerged in extreme situation where the 'fog of war' rendered the managerial model impracticable. Among others, it is possible to remember the deeds of Sergeant Alvin York in the Argonne Offensive – worth a Medal of Honor – and those of the first United States Navy Sea, Air, and Land Teams (US Navy SEALs) in South Vietnam. Yet, these actions were hardly representative of a systematic trend.

From the eighties, both the British[4] and the American Army progressively turned toward a more decentralized philosophy of command (Farrell, 2008; Shamir, 2011), better suited to engage with contemporary security challenges. It is well documented how Mission Command allows for a more flexible and effective engagement, with asymmetric warfare such as peacekeeping operations and counterinsurgency (US Army and Marine Corps, 2010). It is not a case that the manoeuvrist approach and – more specifically – Mission Command has seen a resurgence in contemporary doctrinal documents (US Department of the Army, 2014; NATO, 2010; UK MoD, 2014). Its use has been highly beneficial in recent counterinsurgency campaigns, and has become the go-to course of action for Special Operations forces (see e.g. Willink & Babin, 2017).

[2] Among others, the battle of Caporetto (1917) constitutes a prime example of *Auftragtaktik*.
[3] See for instance the data on the Hamlet Evaluation System (HES) (Kalyvas & Kocher, 2009).
[4] The British Joint Doctrine was developed under General Bagnall at the end of the seventies (Storr, 2003).

Yet, the application of Mission Command requires a shared understanding of the 'why' behind any given operation. Once the strategic objectives – or the 'commanders' intent' – is known, diffused leadership is used to circumvent environmental constraints, seize the momentum and obtain a favorable outcome. This course of action is grounded on high levels of trust. More specifically, subordinates – at all levels – need to be aware of the strategic goals set by the commanding officers and – most importantly – they need to embrace and share their rationale. Secondly, horizontal balance is required: the operating units need to trust each other. Thirdly, lower officers need to fully embrace the logic of mission command and take initiative to accomplish the objectives. How to achieve such unity then? As Yardley, Kakabadse and Neal (2012: 74) note, "the glue that holds mission command together is the culture and values of the organization". The latter is the catalyst for trust that is fully realized through Mission Command.

Another crucial element of Mission Command is situational awareness. Delegating tactical decision to subordinates requires them to responsibly take ownership of actions and choices on the field to execute the mission and maximize the outcome in accordance to the superiors' intent. Similarly to what recent works on coordination of first-responders suggest (Wolbers et al., 2018), specialists need to act with relative independence to achieve broader cooperation. Specific knowledge is thus a key factor to allow them to take informed decisions. The work of Bungay (2005) and Yardley and Kakabadse (2007) in particular, illustrate the decay curve of a plan's effectiveness over time, illustrating the concept presented.

In a neutral scenario, a plan developed through Mission Command decays in a slower way if compared to a vertically-imposed course of action. The reason for that is that Mission Command makes plans that are more flexible and fluid. Yet, as time passes, even Mission Command suffers from loss of effectiveness when situational awareness is not present. That is, even a flexible plan flickers when the operative conditions on the field change: a plan developed at t0 will inevitably not be as effective at t1 and even less so at t2. Conversely, the presence of situational awareness allows to organize a more agile Mission Command. The vertically-imposed plan will perform exactly as in the previous case, since it is not possible to update it 'spot on'. A second vertically-imposed plan can be developed, but it will inevitably decay over time when conditions change. Instead, Mission Command – in a space of situational awareness – enables the actors to adapt the plan over time, correcting for contingencies and striving for the 'higher intent' as conditions change.

Due to this peculiar feature of Mission Command, several authors have analyzed its feasibility as an organizational theory for businesses and the private sector (Pech & Durden, 2003; Yardley et al., 2012; Yardley & Kakabadse, 2007). This approach might be helpful to better equip private actors against contingencies and unexpected threats. As Yardley and Kakabadse (2007: 76) argue, "competitive advantage is often to be found in narrow margins and innovative solutions rapidly developed and brought to market". Accordingly – as per the military counterpart – leaders should be trained to what the literature defines as "controlled risk-taking" and wide-spread empowerment.[5]

All in all, Mission Command is one of the most though-provoking organizational doctrines, and provides a viable solution to respond to contemporary security threats.

[5] Although behind the scope of this chapter, a particularly interesting case is that of Echelon Front, a consulting company founded by two former Navy SEAL officers. They offer leadership programs based on multilevel decision-making and diffused ownership, with a methodology drawn from their experience in the Navy and on the battlefield (see Willink & Babin, 2017).

C2 and Mission Command: the Pitfalls of Digitalization

As briefly outlined above, several military organizations have a tradition of managerial approaches "inspired primarily by the scientific and quantitative school represented by Frederick Winslow Taylor (1856-1915) and Henry Ford (1863-1947) among others, as well as by the theories of operations research and system analysis" (Shamir, 2010: 646). These theories strongly influenced the organizing and the governance of military organizations even in crisis management: Robert McNamara as US Secretary of Defense provides an example of that. The US Army used this model extensively, which is starkly different from Mission Command. As Shamir (2010) notes, such difference is immediately evident when looking at the training facilities of the commanding body. Academies prompted officers to strive for efficiency through a centralized control process without attaining the levels of independent tactical prowess of German officers, forged in the mission command-oriented environment of the Kriegsakademie (Van Creveld, 1990). This tendency has been further exacerbated by the World Wars (Gabriel & Savage, 1979), with increased centripetal efforts inspired by the private sector.

As recounted in the previous section, the debacle in the Vietnam War posited the need for a change, and Mission Command slowly gained prevalence. Nonetheless, digitalization posits several challenges to this doctrine. Remote-controlled technologies as well as automatic arms systems and real-time data intelligence have been seeing a widespread application in military organizations. These devices and techniques provide higher ranks with a virtually unlimited control over their subordinates. Being able to see, hear and evaluate what a platoon experiences, commanders may have an incentive to give tactical directions transcending the original intent-setter role. The archetypal scenario would be that of a circle of officers sitting in a control-room, overseeing and leading a unit on the other side of the globe. As an anecdotal example, in 2011, during Operation Neptune Spear that led to the killing of Osama bin Laden, the President of the United States was able to receive live updates from the battlefield in the White House Situation Room. The risk – or the promise – is that of a renaissance of micromanagement (Storr, 2003). This approach has brought some authors to announce the re-emergence of a C2 doctrine typical of technology-intensive armies (Connor, 2002). This is further reinforced by the widespread use of semi-automated firepower: drones and tele-guided artillery strikes have become a frequent complement to the activity of soldiers. Despite their effectiveness, these tools are managed from the center of the command structure and risk to eliminate the discretion of soldiers on the ground to decide when and where to use them based on sheer necessity. As mentioned in the introduction, technological advancements provide high officers with more intimacy, with the battlefield tempting them to "impose their preferences on tactical units" (Augier et al., 2014: 1430).

This is inherently a risk for the Mission Command model. The centripetal effect of this technologies may hamper initiative and frustrate flexibility. As Augier et al. (2014) argue, changes brought by the implementation of technological systems may have consequences on an organization's ability to learn and adapt. In turn, subordinates will have an incentive towards de-responsibilization (Bateman, 1996).

While this is not an automatic process, the lack of 'practice in choosing' may lead to a progressive desensitization to contingency. Furthermore, the introduction of these new technologies does not entirely dissolve the risk of the fog of war. As it was outlined in the very opening of this piece, uncertainty is hardly eliminated from a 'boots on the ground' scenario. Data may be inaccurate or discontinued due to technical issues: in that case, the cost in human capital may be conspicuous. It follows that "if the confidence of senior leaders outpaces the efficacy of the technology" (Augier et al., 2014: 1430), the space for tactical adaptation may be severely reduced.

In other words, taking away the power to make decisions from the operational level inevitably decreases situational awareness. In turn, as shown in the figures above, this will impact the plans' effectiveness in the long-run, in cases whereby the flow of information is interrupted or erroneous. Furthermore, this approach makes trust harder to establish, as servicemen would be asked to follow vertically-imposed orders. Empirical examples of this phenomenon include the implementation of the Below-Blue Force Tracker (BFT). Among other functions, it provides the command center with the GPS coordinates and real-time tracking of the movements of troops. The original rationale behind this system is allowing a more agile manoeuvring at the tactical level, vis-à-vis the fine-grained disaggregated data. Conversely, the command center can use the aggregated data to provide units with strategic directions (Augier et al., 2014). The estimated marginal effect of its implementation translated in a reduction of Blue-on-Blue events between 24% and 12% in the Gulf War, increasing situational awareness of commanders not only towards enemy forces, but especially towards movement of allied ones (Augier et al., 2014).

Yet, having more trust in technology than in the lower levels of the organization is highly problematic. In 2003, General Franks of the United States Central Command (CENTCOM) made use of BFT to push forward idled units that did not adopt an aggressive advancement as seen fit to higher strategic goals (Gordon & Trainor, 2006). Furthermore, empirical evidence from surveys suggest that most of the times BFT was used to issue direct orders from the headquarters to Marine platoon commanders, with a progressive centralization of the tactical decision-making (Dreier & Birgl, 2010).

Digitalization and Fragmented Coordination in Military Operations

The review of previous studies on data technology in military operations sheds light on the tensions between the centripetal force of digitalization and the diffused leadership principle underlying Mission Command. It is then possible to conclude that digital tools may be shaped in such a way to favor Mission Command, instead of contrasting its core principles. In other words, Big Data, and other advanced data-driven coordination tools, can be used as means to foster widespread responsibility and tactical awareness in extreme contexts. Technical advancements can be used to better support coordination in Mission Command, and do not intrinsically threat the applicability of the doctrine. This chapter thus claims that digitization does not automatically imply a C2 structure. The implementation of new technologies should be adapted to the decentralized nature of a Mission Command environment. A catch-all product indeed has a centripetal effect, while a carefully tailored one may be able to foster diffused ownership. Equipping different branches of the organization with ad hoc tools based on their operative needs and requirements would further their capacity to take initiative, increase situational awareness and act in accordance with the commanders' intent.

This analysis shows how C2 decisions are embedded in the institutional context of military operations, and highlights affordances and constraints of digital technologies in this specific domain (Orlikowski & Barley, 2001). Since fragmentation has been recognized as a suitable coordination mode in the fast-paced environment of extreme contexts (Wolbers et al., 2018), this chapter claims that combat units in military organizations can achieve flexibility, sensitivity to operations, and improvisation by designing C2 systems that support fragmentation more than integration. By focusing on digital technologies' role in supporting working around procedures, task delegation, and expertise, further studies can develop a design theory for digital tools effectively supporting the fragmentation paradigm (Wolbers et al., 2018).

In addition to fragmentation in coordination, the present study suggests looking into other affordances of data technologies, such as those emerging in their application to training and simulations tools. Military

organizations operate under special conditions characterized by extreme events with a high potential magnitude of consequences for both organizational members and often hostile and non-hostile actors at risk. As military organizations engage in extreme events less frequently than other organizations (e.g. trauma organizations), they may require more extensive collective training and simulations. Due to chance of casualties, such training requires redundancies and cross-functional exercises to ensure flexible job rotation and contingency-driven substitutions. In military organizations, since they often operate under austere conditions or time constraints do not allow personnel replacements, team members must be ready to step up and take the role of other team members, or assume formal leadership positions if leaders are lost. This requires a balance between generalization and specialization – necessitating advanced training and simulations tools for leader-development across combat units. Therefore, future studies can apply a contingency approach to investigate the fit between data technologies and leadership development in extreme contexts (Hannah et al., 2009).

Finally, this study revitalizes the long-standing centralization and decentralization debate in organization studies (Bloomfield & Coombs, 1992), revising it in light of new digital trends. The analysis instantiates the contradiction between data-processing capabilities seen as both centralized hierarchical control systems and as decentralized internal control and interfaces supporting semi-autonomous units. Further empirical investigations on the mechanisms and conditions under which Big Data capabilities can lead to organizational performance in extreme contexts can contribute to work through this dilemma (Mikalef et al., 2018 and 2020).

References

Augier, Mie, Thorbjorn Knudsen and Robert M. McNab (2014). “Advancing the field of organizations through the study of military organizations”. In Industrial and Corporate Change, Vol. 23, No. 6, pp. 1417–1444.

Bateman, Robert L. (1996). Force XXI and the death of Auftragstaktik. In US Defense Technical Information Center.

Bloomfield, Brian P. & Rob Coombs (1992). “Information Technology, Control and Power: the Centralization and Decentralization Debate Revisited”. In Journal of Management Studies, Vol. 29, No. 4, pp. 459–459.

Boot, Max (2003). “The new American way of war”. In Foreign Affairs, Vol. 82, No. 4, pp. 41–58.

British Army (1995). British Army Doctrine Publication, Volume 2, ‘Command’, Army Code No. 71584.

Bungay, Stephen (2005). “The road to mission command - The genesis of a command philosophy”. In The British Army Review, Vol. 137, pp. 22-29.

Cameron, Kim S. & Robert E. Quinn (2011). Diagnosing and changing organizational culture: Based on the competing values framework. New Jersey: John Wiley & Sons.

Connor, William M. (2002). “Emerging Army Doctrine: Command and Control”. In Military Review, Vol. 82. No. 2.

Dreier, Matthew J. & James S. Birgl (2010). “Analysis of Marine Corps Tactical Level Command and Control and Decision Making Utilizing FBCB2-BFT”. In Naval Postgraduate School.

Echevarria, Antulio J. & John Bates (1986). “Auftragstaktik: In Its Proper Perspective”. In Military Review, Vol. 66, No. 10.

Farrell, Theo (2008). “The dynamics of British military transformation”. In International Affairs, Vol. 84, No. 4, pp. 777–807.

Fraher, Amy L., Layla Jane Branicki and Keith Grint (2017). “Mindfulness in Action: Discovering How U.S. Navy Seals Build Capacity for Mindfulness in High-Reliability Organizations (HROs)”. In Academy of Management Discoveries, Vol. 3, No. 3, pp. 239–261.

Gabriel, Richaed A. & Paul L. Savage (1979). Crisis in command: Mismanagement in the army. New York City: Macmillan.

Gordon, Michael R. & Bernard E. Trainor (2006). Cobra II: The Inside Story of the Invasion and Occupation of Iraq. New York City: Pantheon Books.

Hannah, Sean T., Mary Uhl-Bien, Bruce J. Avolio, Fabrice L. Cavarretta (2009). “A framework for examining leadership in extreme contexts”. In Leadership Quarterly, Vol. 20, No. 6, pp. 897–919.

Hooker, Richard D. (1993). Maneuver warfare: An anthology. Aldershot: Gower Publishing Company, Limited.

Hughes, Daniel J. (1995). Moltke on the art of war: Selected writings. New York City: Random House.

Kalyvas, Stathis N. & Matthew Adam Kocher (2009). “The dynamics of violence in Vietnam: An analysis of the hamlet evaluation system (HES)”. In Journal of Peace Research, Vol. 46, No. 3, pp. 335–355.

McGregor, Douglas & Joel Cutcher-Gershenfeld (1960). The human side of enterprise. Volume 21. New York City: McGraw-Hill.

Mikalef, Patrick, John Krogstie, lias O. Pappas and Paul Pavlou (2020). “Exploring the relationship between big data analytics capability and competitive performance: The mediating roles of dynamic and operational capabilities”. In Information and Management, Vol. 57, No. 2.

Mikalef, Patric, Ilias O. Pappas, John Krogstie and Michail Giannakos (2018). “Big data analytics capabilities: a systematic literature review and research agenda”. In Information Systems and E-Business Management, Vol. 16, No. 3, pp. 547–578.

NATO (2010). AJP-01 (D): Allied Joint Doctrine. Brussels: NATO Standardization Agency.

Orlikowski, Wanda J. & Stephen R. Barley (2001). “Technology and institutions: what can research on information technology and research on organizations learn from each other?”. In MIS Quarterly, Vol. 25, No. 2, pp. 145–165.

Pech, Richard J. & Geoffrey Durden (2003). “Manoeuvre warfare: a new military paradigm for business decision making”. In Management Decision, Vol. 41, No. 2.

Shamir, Eitan (2010). “The long and winding road: the US Army managerial approach to command and the adoption of Mission Command (Auftragstaktik)”. In The Journal of Strategic Studies, Vol. 33, No. 5, pp. 645–672.

Shamir, Eitan (2011). Transforming command: the pursuit of mission command in the US, British, and Israeli armies. Stanford: Stanford University Press.

Storr, Jim (2003). “A command philosophy for the information age: The continuing relevance of mission command”. In Defence Studies, Vol. 3, No. 3, pp. 119–129.

Van Creveld, Martin (1985). Command in war. Cambridge, MA: Harvard University Press.

Van Creveld, Martin (1990). The training of officers: From military professionalism to irrelevance. New York City: Free Press.

Von Clausewitz, Carl (1982). On war. Volume 20. London: Penguin UK.

Weick, Karl E. & Karlene H. Roberts (1993). “Collective Mind in Organizations: Heedful Interrelating on Flight Decks”. In Administrative Science Quarterly, Vol. 38, No. 3, pp. 357–381.

Weick, Karl E. & Kathleen M. Sutcliffe (2006). “Mindfulness and the quality of organizational attention”. In Organization Science, Vol. 17, No. 4, pp. 514–524.

Widder, Werner (2002). “Battle Command: Auftragstaktik and Innere Fuhrung: Trademarks of German Leadership”. In Military Review, Vol. 82, No. 5.

Williams, Trenton A. et al. (2017). “Organizational response to adversity: Fusing crisis management and resilience research streams”. In Academy of Management Annals, Vol. 11, No. 2, pp. 733–769.

Willink, Jocko & Leif Babin (2017). Extreme ownership: How US Navy SEALs lead and win. New York City: St. Martin’s Press.

Wolbers, Jeroen, Kees Boersma and Peter Groenewegen (2018). “Introducing a Fragmentation Perspective on Coordination in Crisis Management”. In Organization Studies, Vol. 39, No. 11, pp. 1521-1546.

Yardley, Ivan & Andrew Kakabadse (2007). “Understanding mission command: a model for developing competitive advantage in a business context”. In Strategic Change, Vol. 16, No. 1.2, pp. 69–78.

Yardley, Ivan, Andrew Kakabadse and Derrick Neal (2012). From Battlefield to Boardroom: Making the difference through values based leadership. London: Palgrave Macmillan.

UK MoD (United Kingdom Ministry of Defence) (2014). “Joint Doctrine Publication 0-01, UK Defence Doctrine”. In Development, Concepts and Doctrine Centre.

US Army and Marine Corps (2010). Counterinsurgency Field Mannual. Issues 3–24. New York City: Cosimo Reports.

US Department of the Army (2014). ADP 6-0, Mission Command.

WORKING GROUP REPORT

DATA AND DECISION-MAKING: CHANGES, RISKS AND OPPORTUNITIES

Stefano Costalli - University of Florence

Introduction

Uncertainty is a typical factor of military operations and Clausewitz, already in the Nineteenth Century, posited that chance had an essential and unavoidable role in determining the development and outcome of war. As a result, military organizations have always devoted extreme care and huge efforts to create organizations and procedures that could guide action through the fog of war based on available information. Nowadays, the evolution and availability of Big Data, conceived as collections of datasets that contain massive and complex data exceeding the processing capacity of current analytical systems, are promising private and public organizations, including armed forces and NATO, to reduce the role of chance in their spheres of operations. Basing decisions on a much larger amount of information than was previously possible, could lead to a real revolution in the decision-making processes of complex organizations, especially because this information would concern different dimensions of reality, previously unexplorable, and it would be constantly updated. The available literature on this topic suggests that strategies of business companies and military organizations will change considerably as a result of this revolution.

However, in order to fully take advantage of the opportunities provided by the Big Data revolution, organizations have to change their governance and their operational procedures substantially. In particular, while strategic adaptability and flexibility seem to emerge as crucial factors to win the Big Data revolution, achieving these goals and undertaking these deep changes also represent serious challenges for complex organizations that developed over time and have their own histories and organizational cultures. Severe tensions are to be expected, and to an extent are already operating, on a centralization to decentralization continuum. It is not easy to define where the information provided by Big Data should go and which decision-makers should use them.

For these reasons, Working Group (WG) 1 began its works considering the available knowledge on the organizational needs required to exploit the Big Data revolution and trying to understand whether organizational innovations and models that are emerging in private companies can provide useful guidelines for NATO. Subsequently, WG1 tried to define the possible organizational challenges NATO will have to face as a result of the Big Data revolution.

Organizational Innovations for Decision-Making in the Big Data Age

First of all, the WG defined the main features of Big Data, which set the terms to evaluate any possible organizational innovation and decision-making method. The first and most apparent characteristic of Big Data is the huge quantity of information available. The high-speed at which the data are generated and need to be processed is another defining factor that needs to be taken into account, in addition to the fact that

data will typically be acquired from diverse sources and will have different formats. Moreover, the trustworthiness of the data has to be carefully evaluated, and finally any data can have different value in different phases of the decision-making process. All these features impose specific requirements on organizations that aim at using Big Data to reduce the uncertainty in which they operate. For instance, the huge volume of data compels organizations to acquire new data storage capabilities, while the high-speed demands new processing tools and the variable trustworthiness and value compel organizations to elaborate new methods of analysis. Most importantly, all these innovations must be implemented together, because otherwise the Big Data could not be fruitfully exploited and, on the contrary, could create new problems to the organizations, exposing them to dangerous short circuits.

Considering the available literature and exchanging views among the members of the WG, a general consensus emerged according to which any organization that seeks to exploit Big Data should have clear goals and a well-defined strategy to delineate and implement their specific objectives concerning these tools. This is essential to have a clear understanding of the domains and levels where the organization could profit most from the use of Big Data, which types of data are needed, and what investments will have to be made in order to achieve the organization's goals. Founding the organization's decision-making process on the use of Big Data will require important investments, and these have to be guided by a clear strategy. According to the emerging evidence, organizations that invest in Big Data analysis without a clear appraisal of the type of data needed and without carefully defined strategies, are bound to failure, wasting precious resources and possibly ending up in suboptimal situations.

Private companies have adopted diverse organizational structures to work effectively with Big Data, ranging from highly centralized to remarkably decentralized models and including hybrid solutions. However, developing forms of governance that allow the different units of the organization to share data and work together seems fundamental. Before the advent of Big Data, such an approach would have raised problems of information security, and the various units would have been advised to limit data circulation. Conversely, some members of the WG observed that in a Big Data environment, security should be recommended for the outcome of the analysis, not for the data source. Otherwise, organizations would risk obtaining "security through obscurity". In private companies that use Big Data analysis, no attention is given to individual data, but rather to the overall amount of data, which is the real added value. In any case, while data ownership should not be centralized, the available evidence indicates that data governance should, and the Big Data Analytics (BDA) unit should be carefully located. It needs to be placed where it is most needed, easily accessible by core units, cross-functional and integrated. Relatedly, some members of the WG stressed that a key issue with Big Data is providing decision-makers with data that are truly relevant for their purposes, and not simply interesting.

A key requisite for all organizational innovations to occur and for Big Data analysis to be effective is the development and incorporation of a Big Data culture. Chief data officers and senior data-related leadership positions will acquire crucial importance in the analysis of information and in the actual decision-making process, but these positions require a special mix of talent and tools that are currently scarce in many large organizations, especially in the public sector. The organizations that are implementing big data analysis seem especially in need of 'translators' – professionals that can ensure effective communication between the Big Data analysis unit and other parts of the organization, where workers are not data scientist and may not be ready to work directly on complex models. However, organizations willing to use Big Data are also in need of real data scientists and analysts, because sophisticated techniques and data analysis tools eventually rely on talented humans who know how to manage the tools and interpret data. As a result, attracting new types of

talented young workers and retaining them creating new career paths and opportunities will represent both an essential organizational innovation and an important challenge.

In fact, some members of the WG highlighted that it will not even be easy to find many workers with the appropriate knowledge and skills to perform the new tasks in old and complex organizations. It is possible to find computer scientists, but sometimes these individuals do not seem to fit well with large organizations whose main core business has not much to do with computer science. At the moment, it is even more difficult to find translators, since in principle these workers should be social scientists with an expertise in Big Data analysis, but most academic institutions are not ready to forge these profiles. For what concerns NATO and national armed forces, this educational task is not even performed by military academies, even though some experiments are emerging. The ideal profile would include technical awareness, quantitative analytical skills, broad vision, flexibility and open-mindedness – and this explains why it is not easy to produce it.

Organizational Challenges for NATO in the Big Data Age

After having analyzed the main organizational innovations NATO will have to take into account in the age of Big Data, the WG tried to identify the main challenges. Most of these challenges are strictly linked to the organizational innovations mentioned above, representing the other side of the coin, as in the case of finding and retaining talented workers with new professional profiles.

The first challenge is embodied by an emerging tension between centralization and decentralization of the decision-making process of organizations that are introducing Big Data analysis in their work. As stressed by various members of the WG, a key issue in the use of Big Data for decision-making is that the data, once analyzed, need to reach critical decision-making levels, and not only (or simply) the top level. Nonetheless, it is apparently quite difficult to translate this principle into concrete organizational forms and procedures. Paradoxically, while Big Data should promote widespread responsibility and tactical awareness, at the moment advanced digitalization seems to be linked to clear centripetal forces in large organizations. So far, technologies such as remote-controlled arms systems and intelligence activities based on real-time data collection have produced strong incentives to micromanagement and to a re-centralization of decision-making in military organizations that have implemented these tools. As a matter of fact, these technologies are managed from the center of the command structure, and provide higher ranks with an increased possibility to control their subordinates as well as the expectation of increasing such control with the adoption of additional technologies. This powerful tendency risks to threaten initiative and reduce the flexibility of military organizations, decreasing their overall capacity to learn and adapt. While the full exploitation of Big Data and the optimization of their use would require the information to reach the most relevant levels, the centripetal tendency leads towards the de-responsibilization of the lower ranks on the ground and to a progressive loss of practice in choosing. This process is not only inefficient for the reasons mentioned above, but also potentially dangerous because Big Data do not fully eliminate uncertainty: in specific occasions, the data can be inaccurate or not available due to technical problems and, in these cases, the personnel on the ground has to be ready to adapt and react basing their decisions on their experience. Thus, various members of the WG recommended NATO to integrate Big Data in the organization's decision-making, favoring diffused ownership and devising different tools for different branches of the organization, based on their specificities. The implementation of Big Data can and should be used to increase flexibility, situational awareness and action in accordance with the center's intent but without centralizing all decisions and producing the illusion of complete control.

Some members of the WG suggested that it is crucial for NATO – and for all big organizations engaged in the use of Big Data – to create well-designed and reliable evaluation procedures to measure the effectiveness of organizational innovations as well as of the execution of the new decision-making processes. Identifying the initial failures is especially important, to learn from them and avoid structural problems. This issue is linked to other potential challenges highlighted during the discussions of the WG. For instance, some members pointed out that when adopting Big Data, certain member countries will probably do better than others, and this could cause problems of interoperability, but also learning opportunities. Finally, a well-designed evaluation system will also help avoid some deep risks that automated decision-making could represent for the values of NATO. In fact, some members of the WG stressed that what distinguishes democracies from authoritarian regimes or tech dystopias run by robots is that, ultimately, citizens make the rules that have to be implemented. Moving towards automated decision-making as a result of Big Data analysis in matters of war and peace, life and death, is extremely risky, and the implementation of Big Data cannot decrease human control and responsibilities. Some of NATO's authoritarian adversaries are already facing smaller legal and normative obstacles in the use of Big Data, but NATO will have to carefully check the impact of next generation's technologies on the democratic values and legal frameworks of its members.

Conclusion

The availability of Big Data is promising to revolutionize the business of private companies, the work of public administration and the bases of decision-making in military organizations. The possibility to collect immense dataset on multiple dimensions on reality and update them constantly and in real time could greatly reduce the uncertainty that dominates many environments, including military affairs and actual combat operations.

However, organizations that aim at exploiting this possibility effectively will have to change their governance and their operational procedures substantially. For this reason, WG1 started its works reviewing the available knowledge on the organizational innovations required, seeking to identify useful lessons for NATO. Subsequently, WG1 tried to detect possible organizational challenges for NATO as a result of the Big Data revolution, suggesting ways to tackle them.

First of all, any organization willing to exploit Big Data must have clear goals and strategies to implement their objectives concerning Big Data. This is essential to produce a clear assessment of the areas and levels where the organization could profit most from the introduction of Big Data analysis. As a matter of fact, it is crucial to understand that, in order to be fully effective, the information collected through Big Data needs to reach the points where it is more relevant. Moreover, a key requisite for all organizational innovations to take place and produce results, is the development of a Big Data culture. The new positions will require special talents and expertise that are currently scarce in many military organizations. WG1 highlighted that it will not be easy to attract these talents and retain them in military organizations, if not by creating new career paths and opportunities.

As regards the main organizational challenges, the members of WG1 found that a major challenge is represented by an emerging tension between centralization and decentralization of the decision-making process in military organizations that are introducing Big Data analysis in their work. Somehow paradoxically, while Big Data should promote widespread responsibility and tactical awareness, at the moment advanced digitalization seems to be linked to clear centripetal forces in large organizations. This is not an inevitable path – flexibility and shared ownership of information are compatible with the introduction of Big Data, but big organizations have to be aware of this tension and set up evaluation systems to control the effectiveness of the innovations adopted.

(Photo credit: European Pressphoto Agency, Jim Hollander)

WORKING GROUP
II

HYBRID THREATS TO ALLIED DECISION-MAKING

Hanna Smith - Hybrid CoE

Abstract

This chapter discusses the challenges to decision-making in Western countries brought by hybrid threats in relation to China and Russia. The first section looks respectively at Chinese and Russian strategic thinking, by underlining a number of similarities between the two authoritarian states. Their approach is directly connected with the five main characters of hybrid threats analyzed in the chapter: usage of multiple synchronized tools; ability to create ambiguity; deliberate threshold manipulation; exploitation of the seams of democratic societies; use of decoys. In the second section of the chapter, those features are related to Western decision-making by following David Omand's model of Situation awareness, Explanation, Estimate and Strategic notice (SEES). The third section discusses the characteristics of current information environment which amplify the hybrid threats impact on the SEES model: speed of information, volume of information, Artificial Intelligence, and degrading expert opinions and official voices. Finally, this chapter draws some conclusions and recommendations relating to allied decision-making.

Introduction

Recent digital and technological developments have enabled many completely new tools, which have given rise to new virtual platforms that fall outside current norms and rules. These new tools have also brought unprecedented speed to all kinds of action. Interconnectivity and globalization have created new possibilities for network-based action, lowered borders, changed geopolitics and made sure that there is more data around us than ever before. New actors have emerged in international politics, who are looking to enhance their status. Authoritarian and democratic states appear to be entering into a new form of ideological battle. In this situation one can ask: what are the rules of the game? An important weapon in this new battle is hybrid threats. Hybrid threats constitute a shadow policy for authoritarian states that supports their strategic aims and is based on their strategic culture traditions. The clear dividing lines, unwritten rules, players and goals of the Cold War are history. This situation is challenging for planners, decision-makers and foresight building.

The concept of hybrid threats has entered into political normality by appearing in the discourses and documents of the EU, NATO and their member states. The concept has been examined through many different disciplinary lenses: international relations, strategic studies, security studies, military studies, history and political science – to name a few. This multidisciplinary analytical mosaic also blurs the picture of what hybrid threats really are. The Report "The Landscape of Hybrid Threats: A Conceptual Model", issued by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) together with the European Union (EU) Commission's Joint Research Center, uses hybrid threats as an umbrella concept, under which different types of activity occur: interference, influence, operations, campaigns and even warfare (Giannopoulos, Smith and Theocharidou, 2020). The approach adopted would enable a comprehensive

analysis including civilian, political, military and academic thinking. This chapter will take the report's conceptual model as its starting point for hybrid threat analysis.

Hybrid threats are still difficult to define, which on the one hand complicates the adoption of strategies to counter them, common positions and a holistic approach, but on the other hand gives flexibility, greater freedom to be creative and possibility to combine different disciplines and backgrounds. Consequently, the characterization of hybrid threats will help to identify real threats, potential threats and also those aspects that might look like threats but are not. Too tight definition might, in the worst case, point in the wrong direction and also tie one's hands when it comes to responding.

There is still an ongoing debate regarding the usefulness of the concept of hybrid threats. Those saying that hybrid threats are mostly "old wine in new bottles" mean that perhaps we do not need a new concept, and we could just adjust the old ones to current circumstances. To this Frank Hoffman, who is often seen as the man behind the 'hybrid warfare' concept, answered in the following way: "New language and new terms aid us in thinking differently and characterizing what is truly new, hopefully without overlooking what is enduring in war. A new lexicon captures the changes better than hanging on to old terms with new meanings" (Hoffmann, 2010).

The 'old' in the concept of hybrid threats lies in the fact that interference and influence have always been part of international politics. Also, the technique of combining different domains like social, political, informational, military and legal ones has been part of the strategic thinking behind influence, interference and military operations. This thinking is also present in today's activities that constitute hybrid threats. What is new, then – although anchored to traditions in the authoritarian strategic thinking – is related to today's security environment and how it is different compared to the Cold War's, for example. The battle between democratic and authoritarian state systems today is not as clear-cut as the division between communist and capitalist countries was during the Cold War. Furthermore, digital and technological developments have provided new platforms for influencing, new tools for both interference and influence, and have extended the domains where action happens – from the traditional military domains like land, air and sea, to cyber and space, to more comprehensive domains like culture and administration. These are all connected and, through hybrid threats activities with a targeted approach, even the best prepared states and alliances can be challenged.

The logic of interference found in hybrid threats is substantially based on authoritarian strategic culture. Strategic culture itself as a concept has been contested, but in recent years it has found its way back into security studies. It is worth noting that the Cold War juxtaposition, the bipolarity of the superpowers, crucially downplayed the relevance of national aspects relating to cooperation, competition, conflict, and war. In that way, the 'national character' of the enemy, which was very important before the Second World War, was downplayed during the Cold War years (Miklossy & Smith, 2020: xiii). Post-Cold War studies started to pay attention again to different domestic processes and their effects. As Glenn observed, "[t]he mid-nineties witnessed the emergence of a new school of realists that sought to move beyond the basic insights of Waltzian neorealism by investigating the interaction of systemic pressures and domestic processes in the foreign policy decision making process, thus providing a much richer explanatory account of why states choose certain foreign policies over others" (2009: 523-551). From examining national strategic cultures, the theory can also be extended to cover strategic cultures of a particular state system. Here the concept of authoritarian strategic culture comes from the studies that produce characterizations of authoritarian and totalitarian regimes (Linz, 2000; Svolik, 2012; Brooker, 2014). There are national specificities when it comes to behavior, and there are specificities that are linked to the state system. The national specificities are more

difficult to define due to the fact that culture as a concept is complex. A state system is relatively easier. A state system often defines the regime type as well as its relationship to civil society, opposition and the military.

This chapter begins by presenting the characteristics of hybrid threats, as identified in the authoritarian strategic thinking specifically in relation to Russia and Chinese traditions. Those characteristics are then put into the context of decision-making following David Omand's Situation awareness, Explanation, Estimate and Strategic notice (SEES) model. In the third part, the challenges that the new information environment presents us are considered, and finally the chapter draws some conclusions relating to allied decision-making.

Hybrid Threats and Strategic Thinking

As mentioned in the introduction, this chapter takes as its starting point the report "The landscape of Hybrid Threats: A conceptual model". The report does not claim to be an exhaustive source for the description of all the characteristics that hybrid threats might have, and there might be many more that have to do with the changing nature of the phenomenon. However, the report does identify five characteristics deemed to be the most important with respect to the challenges they pose to decision-making:

- Usage of multiple synchronized tools, used to create linear and non-linear effects;
- Ability to create ambiguity with plausible or implausible deniability and to hide true intent;
- Deliberate threshold manipulation and the use of grey zones like borders between war and peace, friend and enemy, virtual and real, internal and external, etc;
- Exploitation of the seams of democratic societies and the different jurisdictions (local, state, international);
- Use of decoys.

These five challenges are all related to Russian and Chinese interference and influence traditions, which will be presented in the following sections. In turn, they are part of wider strategic culture, which is the product of a centuries-long dialogue between a people and its history (Gray, 2006: 15). Strategic culture is closely interlinked with the idea of national interests in a spatial context that is defined by potential threats, perceptions of friends and foes, traditions of alliances, and institutional linkages (Miklossy & Smith, 2020: 263).

Traditions of Chinese strategic thinking

Since uncovering strategic culture is beyond the scope of this chapter, the approach is to present some dominant ideas that are still present today in Chinese thinking relating to interference, influence and winning conflicts and wars. The Chinese thinking presented here is based on three books; *On Strategy Studies* (2006) published by the People's Liberation Army (PLA), *Political Work Guidelines of the People's Liberation Army* (2003), where the "Three Warfares" concept is introduced, and *The seven military classics of Ancient China* (2017), which presents seven texts from different times seen as cornerstones of Chinese military tradition. This is particularly relevant since President Xi Jingping has forbidden the use of foreign theory books in education and has mandated turning back to their own classics including those on strategy (Nojonen, 2019). Therefore, Chinese practitioners of strategy are actively studying their own classics in building a professional

identity and practices based on the particular traditional conceptualization of the Chinese strategy work (Nojonen, 2019).

The book *On Strategy Studies*, published in Chinese, introduces the concept of "supraplanning": a dynamic process towards a goal – and not a rigid adherence to a sequence of steps that is forever fixed and precisely worked out in advance. The authors outline three factors that determine the strategic behavior of the Chinese military: strategic thinking, strategic environment and military capacity. The book makes a point that the aim is "to lure the other side into developing misperceptions…and to [establish for oneself] a strategically advantageous position by producing various kinds of false phenomena in an organized and planned manner with the smallest cost in manpower and materials" (Detweiler, 2009: 10).

In analyzing Chinese strategic behavior, the authors argue that the tradition, understanding and practice of stratagems is the dominant pattern of Chinese strategy thinking. Based on the book, the characteristics of Chinese supraplanning are:

a) resourcefulness and decisiveness;
b) deep stratagems and distant deliberations;
c) comprehensive planning and preparations;
d) flexibility and ingenuity.

It is important to note that different concepts found in traditional Chinese strategic thinking are presented in a dialectic way, such as "weakness and strength", and "clandestine manoeuvres and open operations". This means that concepts are not strictly defined, but rather remain borderless and ambivalent, creating ambiguity. Also, these concepts can be nouns and verbs at the same time; in other words, they can be both abstractions of cognitive processes as well as actual practices. This means that a solid picture of each given situation might be very difficult to form without a profound knowledge of Chinese language (Nojonen, 2019).

Also, the more well know Chinese concept of "Three Warfares", in the book *Political Work Guidelines*, comprises three different components: Psychological Warfare, Public Opinion Warfare and Legal Warfare. The Three Warfare concept was first made official in the revisions of the PLA's Political Work Regulations in 2003.

- *Psychological Warfare* is defined as operations that achieve political and military aims by influencing a target's psychology and behavior through the distribution of specific information. Situational awareness can be blurred with informational manipulation, and different biases can be supported. In this respect, the 'targets' are practitioners and decision-makers. Psychological Warfare methods include deterrence, coercion, deception, instigation, seduction, bribery, inducement and confusion. These methods are part of both theoretical and doctrinal descriptions.

- *Public Opinion Warfare* is defined as operations aimed at influencing both domestic and international support with the use of selective information delivered through different media. This is different from psychological warfare in the way that it aims to control the masses. The main channels for this type of activity are the internet and traditional media sources, such as broadcasting and newspapers. Towards the public opinion, warfare concept channels also include international organizations and academic forums that can be used from within under a tailor-made approach.

- *Legal Warfare* is used to attain legal superiority by using domestic and international law to gain a political initiative or military advantage. Rather than viewing law as a method of rational order-

making, legal warfare looks for ways to use legal advantage to influence targets by delivering the effects of interference, response, defeat, deterrence, or defense via legal means, including through national or international channels.

The third book, *The seven military classics of Ancient China*, gives a comprehensive picture from a historical perspective of how Chinese rulers and generals have analyzed the best ways to keep power, get power, conquer land, defeat the enemy and gain control. The book includes Sun Tzu's famous "Art of War", and Huang Shigong's "Three Strategies", which discusses the Art of War. In the latter text, for example, the line "Follow their (enemy) trends in order to break them. Be wild with your words in order for them to make mistakes. Surround them with your net in order to catch them", could be applied to today's security environment, where the manipulation of information is based on the assumption that decision-makers will make mistakes that favor the actors providing misinformation. All these texts have psychological elements, search for weaknesses and look for ways to covertly succeed.

This snapshot of Chinese strategic thinking already shows that it will be very hard from outside China to identify actions that are seen and planned by Beijing to be borderless and ambivalent. Furthermore, different levels of decision-making are the main target. The various tools are designed to work in the way that situational awareness is blurred and context is lost, which means that estimates, warnings and preparedness in the target are incomplete.

Traditions of Russian strategic thinking: reflexive control

Russian and Chinese traditions of strategic thinking have similarities on several points, although naturally there are also differences. The Russian concept of reflexive control is designed to manipulate the target's information-processing and decision-making in such a way that it inadvertently promotes Russian interests at the expense of the target's own interests. This effect-driven approach may be aimed as narrowly as at an individual, or as broadly as at a political organization or cultural milieu. There is a similar idea in Chinese strategic thinking, involving mechanisms for controlling both individuals and masses. The process can be characterized as 'reverse psychology': prompting the opponents to do something that they will perceive as being harmful to the manipulator, while actually making a decision that has been prepared before-hand by the manipulator. "Do whatever you want with me, just don't throw me into a thorny bush", said the rabbit to the fox. The fox did just that and the rabbit was saved in the thorny bush. The opponent is manipulated into believing that the decision was made of his own free will. This type of manipulation is very characteristic of today's hybrid threats.

Reflexive control bases large part of its effectiveness on informational influence and requires the study of human consciousness and will (Smoljan, 2016). Preparations of reflexive control include playing out scenarios of potential reactions and anticipating certain responses and outcomes. This means that active testing is part of the technique. The theory of reflexive control is a very well-known part of Russian strategic thinking (Lefebvre, 1984; Thomas, 2002 and 2004; Vasara, 2020), and has been designed especially under authoritarian regimes.

Based on current literature, the following characteristics of reflexive control are identified are particularly relevant:

- *Pressure*: demonstrations of military might, sanctions, ultimatums, provocations, military intelligence, raising defense readiness, etc.;

- *Deception*: appearing strong where weak, covert operations, bluff, provocations in irrelevant areas, hiding critical connections and links between operations, creating false distractions, leading the target out of a conflict in a way that benefits the manipulator, etc.;
- *Surprise*: always acting unexpectedly and against the common logic;
- Distraction: creating a real or imaginary threat, using decoys, acting in one place but target somewhere else;
- *Overload and Exhaustion*: the target is continuously provided with conflicting information and it is then forced to carry out useless actions so that it will be gradually weakened;
- *Provocation*: making the target act in a manner advantageous to the actor behind the action;
- *Synchronization of action*: Valery Makhnin developed the concept further and made an argument that the reflexive approach makes use of reflexive methodology on the basis of which the techniques, instruments and phases using information and psychological influence are planned and put into effect (Vasara, 2020: 52).

The theory of reflexive control has been evolving since the 1960s but has played an important role in Russian strategic thinking both at the political level and on the military side. In his very comprehensive study of reflexive control theory, Antti Vasara from the Finnish National Defence University argues that, by looking at the combined outputs of several Russian authors who have been working on the theory, today "the end result is a comprehensive theory of exerting influence over the enemy" (2020: 61).

Reflexive control theory is only one – although very influential – theory. Ofer Fridman lists Messner's subversive war theory, Dugin's net-centric war theory, and Panarin's theory of information warfare, as Russian theories presenting characteristics and techniques which are seen in the landscape of hybrid threats (2018).

In the following section, the five major characteristics of hybrid threats identified in this chapter will be examined closer.

Five characters of hybrid threats

The accounts of Chinese and Russian strategic thinking traditions, which are very much part of their interference and influence playbook today, show many similarities. Here, five characteristics have been chosen based on the literature that was examined in the previous part of this chapter.

The first characteristic is the use of multiple synchronized tools to create linear and non-linear effects which are also identified in the Multinational Capability Development Campaign (MCDS) work on hybrid warfare (Cullen & Reichborn-Kjennerud, 2017). This is the cornerstone that brings the word 'hybrid' into the picture. This feature, however, is common to most military studies. Warfare has always included multiple domains. The way this tactic expresses itself in the landscape of hybrid threats today is that most of the activities look very unconnected, they are mostly legal, and they happen inside our societies, using the systemic vulnerabilities of democratic systems. The Chinese texts emphasize the coordination of different techniques, while the Russian texts talk about a combination of techniques, instruments and phases.

The second characteristic is the ability to create ambiguity with plausible or implausible deniability, and to hide the true intent. This is central to the success of hybrid threat activities. As Andrew Mumford has pointed out, "The key aim of ambiguity is not necessarily to hide the true actor behind the activity, but ultimately to

stymie a legitimate response" (2020: 3). In Mumford's view, the ambiguity is calculated and the implausible deniability is not an unintended consequence. This ambiguity aims, in the first place, to hide the true intention of the action rather than to hide the actor. This type of ambiguity creates difficulties for any kind of response. Hiding the true intent is talked about and used throughout the Chinese and Russian texts.

The third characteristic is the deliberate threshold manipulation and the use of grey zones like the border between war and peace, friend and enemy, virtual and real, internal and external, etc. Thresholds and red lines are often created or stated for the purpose of deterrence. They are also a sign of collective readiness to react with hard power. Thresholds are in international treaties, like Article 5 of the North Atlantic Treaty and Article 222 (Solidarity clause) or 42.7 (Mutual Defense clause) of the Treaty on the Functioning of the European Union (TFEU). From the perspective of hybrid threats, this threshold manipulation has the purpose of breaking any unity inside a country or alliance and of delaying any response. Furthermore, indecision can also be used as an example of weakness.

The fourth characteristic is something very specific to today's hybrid threats. Since the activities relating to hybrid threats focus on democratic states' systemic vulnerabilities, all grey areas and seams can be seen as target areas. Therefore, the fourth feature consists in the exploitation of these vulnerabilities. It can relate to different jurisdictions (internal to an institution, local, state, international), it can be gaps or restraints in the legal system, or a way that democratic values are used as tools – like freedom of speech, for malign action. By targeting the seams, clear definitions and divisions of labor can be seen as limiting factors for effective responses. This implies that, from a compartmentalized way of thinking, we need to move more towards a comprehensive approach.

The fifth and final characteristic is the way actors use decoys. It is very typical to create actions in one place while the real target is somewhere else. This way, the actor can also hide its real goals and possibly even escape attribution. Decoy and deception have been part of the tactics of warfare, therefore are less common when talking about interference and influence in peace time, especially if the target is a civilian population. Also due to the concept's unfamiliarity in civilian contexts, it can be very effective.

Intelligence, Decision-Making and the Challenge of Hybrid Threats

All decision-making depends on information, data, expertise and, in some cases, also on algorithmic calculations. In a situation where decisions need to be made quickly, there is a risk that correct information is not trusted or considered. Case studies show that, in a time of crisis, early decisions were based on advice that turned out to be faulty or inaccurate, due to either a deficit in knowledge or wrong information sources, and therefore led to non-optimal decisions (Dokos, 2014). Other studies underline that long-term disinformation activity reinforces existing divisions in a society, and plays these division against each other with the aim of activating individual-level decisions, which might result in unhealthy polarization (Jamieson, 2018; Kent, 2020).

Information based on professional intelligence gathering, let alone on secret intelligence, is only available to a small number of those that need to make significant decisions (Omand, 2020). The secret piece of information is the information our adversaries want to keep away from us while we want to keep our secrets away from them. A piece of information that has been obtained through covert intelligence can make all the difference from a national security perspective, either confirming the open-source intelligence or bringing new insights, which will affect the decision-making.

Here, the focus will be on state-level decision-making, which comes closest to decision-making mechanisms in alliances. For that purpose, David Omand's model, which he calls the 'SEES model', is used for categorizing the decision-making process relating to intelligence production. Omand's argument is that, through the SEES model, it would still be possible to make solid evidence-based decisions. He reminds us that our knowledge of the world is always fragmentary and incomplete, and sometimes wrong. So, even if we have a lot of information, we might never have all the details, therefore we need models to help us construct situational awareness, explanations, estimates and strategic notice – like the SEES model (Omand, 2020).

The SEES model

The first 'S' of the model stands for 'Situational awareness'. This answers the sort of factual questions that start with 'what, when, and where?'. Situational awareness is a cornerstone for decisions, functioning cooperation and effective response. If situational awareness is not in place, it will be very difficult to start cooperating and/ or finding effective responses. For this reason, we need reliable information sources, which is not so easy in the current information environment. There is also a need for constant monitoring, to be able to track continuity and change. Situational awareness can go wrong if the knowledge of the world is wrong, either because someone unconsciously selects out material, or because somebody sends some false messages that are believed to be truthful, or if someone gets the details wrong. This first part of the model is clearly a target of hybrid threat activity as shown in the above account of Russian and Chinese interference and influence thinking.

The first 'E' in the model is for 'Explanations' of the information that has been received. Here, the necessary questions are 'how and why?'. One needs access to background knowledge, foreign language skills, history, geography, anthropology, psychology, and current affairs to provide the correct context to link the information. Furthermore, it is rather important that those who do analysis come from different backgrounds and have different ages, so that there is historical memory present to give context but also a solid knowledge of current affairs. The explanations can go wrong if there is no understanding of the psychology of the adversary. The assessments of motivations and rationales are important in explanation. It is very easy to get

explanations wrong if they are based on mirror imaging[1] thus assuming that the thinking is the same in both sides. Since explaining requires several different skills, including both long-term and current situational contextual understanding, this is strongly targeted by hostile actors through long-term activities that consist in repeating the story that they want to be perceived as the dominant one. If situational awareness is challenged by different active campaigns using Artificial intelligence (AI) as an aid and amplifier, then explaining is challenged by a long term, gradual build-up of strategically important connections and dependencies.

The second 'E' stands for the 'Estimation' of impact to answer vital questions about 'what is likely to happen next if we do – or do not – adopt a particular policy or act in a particular way?'. This is not a prediction, but rather an estimation of the likelihood, for example, of national security threats rising for terrorism. Estimates need an explanatory model, sufficient data and explicit assumptions, and having a good explanation allows to model possible outcomes. This 'estimate' part is the one in which most decision-makers are interested. Based on these estimations, many decisions have been made and will be made without any certainty. Here

[1] Mirror-imaging means that an analyst may perceive and process information through the filter of personal experience. Mirror-imaging imposes personal perspectives and cultural background on incomplete data, undermining objectivity.

there is also a great danger of getting things wrong, since explanatory models need data, solid explanations and explicit assumptions. Making assumptions when trying out different 'what ifs' in a model can lead to errors. Here, many 'what ifs' need to be taken into account, therefore it is important to detect as many linkages as possible. The estimation phase in the model can be targeted by trying to feed wrong information on which assumptions could be based. If a digital platform is used in the modelling of estimation, it can be targeted by cyber tools. This part of the process is also of high interest to intelligence, therefore decoys to create distractions are used in the attempt to push the estimates along the wrong tracks.

Finally, the second 'S' is about 'Strategic notice'. Strategic notice helps the military to answer important questions of the 'how could we best prepare for whatever might appear next?' type, or even 'how could we pre-empt this risk so that it never comes to test us?'. The strategic notice helps decision-makers to address media attitudes and public resilience – both necessary to counter any potential threats (Omand, 2010: 220). Interestingly, the information that is needed to provide strategic notice can in fact be provided entirely from open sources. This means, for example, that academics and long-term experts might be as relevant and good observers as intelligence officers. The possibility of getting the strategic notice wrong arises from the inability of imagining the unimaginable and looking beyond the horizon. Strategic notice can be considered as an area of imagination competition where both sides try to water down their opponent's observations.

The impact of hybrid threats on the decision-making processes is amplified by the current information environment, as discussed in the next section.

The SEES Model and the Current Information Environment

Today's information environment makes the way in which that intelligence and information are handled more complicated than before. Big Data can distort rational analysis. Online information has a particular character compared to information sources like newspapers, magazines and TV. The internet has largely reshaped the information environment. The SEES model shows how important and comprehensive are different types of information. Yet, in today's interconnected and globalized world, simple and clear facts are not so easy to establish. The situation has created an environment where it is very hard to distinguish between changing, maybe contradictory messages which emanate from governments and expert communities, from the mass of fake news. Some characteristics that make today's information environment challenging for the SEES model, and particularly prone hybrid threat activities, are speed, volume, AI and degrading expert opinions and official voices.

Speed

The viral spread of (dis)information forms the context of what is today called the 'infodemic'. It is the viral spread of fake news, misinformation and disinformation, using the possibilities afforded by social media. On social media, individual users are not only consumers, but also producers and spreaders of content. Social media platforms have become message-amplifiers. The effect of this triple role – consumer, producer and spreader – is very difficult to contain. Data travels fast and is amplified. When a consumer produces and spreads information, it means that facts and rationality often risk being lost. When information produced in social media starts to penetrate into the mainstream media, false information can also end up on the decision-makers' table and/or decision-makers are influenced in other ways.

Finally, when information travels fast and is amplified, the inaccurate or false facts get more space. There is a risk that mainstream media, ethical journalistic work and real subject experts' voices become just one voice among many. This situation makes fact checking very challenging and gives rise to deception in the domain of information.

Volume

Speed is followed by volume. The volume of information that exists becomes a source for blurring situational awareness, while also being a tool to this end. It is possible to flood the information domain with all kinds of information, which offers something for everybody, so that truths and facts become buried under many other explanations. A good example here is how during the Skripal case, in the spring of 2018, Russian state-led media circulated over 30 alternative explanations of the case. Some of the explanations verged on the absurd, such as the following ones:

- *It was Theresa May because she's a friend of Gina Haspel, director of the CIA* (Zvezda - 13 March);
- *The UK poisoned Ivan the Terrible and therefore also Skripal* (Komsomolskaya Pravda - 26 March);
- *It was a drone* (Zvezda / Russian MoD - 18 March);
- *It was the "mother-in-law to be"* (MK.RU - 14 March);
- *The UK did it to justify high military spending because "they need a major enemy"* (Deputy Foreign Minister Alexander Grushko, quoted in The Guardian - 3 April);
- *Ukraine did it: "to frame Russia"* (Russia 1 - 13 March);
- *Accidental Overdose* (RIA Novosti - 8 March).

This flow of explanation is not believable for most observers, but it seemed that this was not accidental. In the end, the pile of ridiculous narratives also discredits fact-based explanations. And since a lot of information was based on intelligence which cannot be shared, there was also a perfect opportunity to cast the shadow of ambiguity through an information campaign that was coordinated and synchronized from the Kremlin. So, with volume, ambiguity can be created and true intents hidden.

Artificial Intelligence

The mass collection of personal data also enables another mechanism, namely micro-targeting along with developments in online surveillance and behavior-tracking. AI and machine learning (ML) support the emergence of highly-targeted information operations – or what can be best called 'Hyper-Personalized Influence Targeting' (HPIT) – to achieve political, economic, military and geopolitical objectives. This technique was employed by the Russian Internet Research Agency (IRA) to send messages via Facebook, Twitter and Instagram (and other social media platforms) to US citizens, leading up to and during the 2016 presidential campaign, largely in an attempt to amplify social discontent, provoke violence and undermine the electoral process (Lauder, 2019). This means that, through micro-targeting, it is possible to reach out to users individually and show them carefully-cultivated content based on their likes, dislikes, beliefs etc. in order to influence them and lead them to amplify the message.

Degrading

If speed and volume are products of the new information environment, then the degrading of expert opinions and official voices is one of the impacts that they have created. From the hybrid threat point of view, a distrust of official communications can provide a platform for outside interference by creating a source of power inside of a target's internal space for the external actor; it can trigger destabilization in the form of riots (note the difference from democratic demonstrations); and it can deepen an ongoing crisis or have negative effects on future crises. This type of 'power' can be used to influence decision-making (EU-HYBNET, 2020).

Conclusion: the Challenge to Decision-Making

Putting together the five characteristics of hybrid threats (use of multiple synchronized tools, ability to create ambiguity and to hide true intentions, deliberate threshold manipulation, exploitation of the seams of democratic societies, and use of decoys); the SEES model (situational awareness, explaining, estimating, and strategic notice); and the new challenges of today's information environment (speed, volume, AI, and degrading expertise), they result in a mix that can influence decision-making algorithms and, in Omand's words, "it is our own demons that are most likely to mislead us" (2020).

Since hybrid threats are designed to interrupt effectiveness of the SEES model at some point, by trying to create cognitive errors such as those arising from group thinking,[2] mirror imaging or applying unconscious confirmation bias, they can challenge organizations like the European Union (EU) and NATO even more than a state. The multilateral setting – with several, connected national interests – can be more vulnerable to hybrid threat activities. The things that can go wrong in the SEES model are especially vulnerable in a multilateral setting, unless there is a comprehensive approach, willingness to exchange information, joint understanding on resilience, and mechanisms to counter and respond in place.

The way Moscow and Beijing think about interference and influence is different from countries with a democratic system. For the EU and NATO, both Russia and China are difficult states to deal with. China is seen in the EU as a global partner, competitor and systemic rival. It has not been on NATO's radar before the 2019 London Summit, but the Report "NATO 2030" delivered by the Group of Expert appointed by the Alliance's Secretary General states that "NATO must devote much more time, political resources and action to the security challenges posed by China" (2020: 12). Russia has been viewed by the West as a systemic rival for much longer, but it has also been considered part of the European cultural heritage in the EU. For NATO, Russia has been the greatest military power in the East, which has conflicts of interest with NATO. For the moment, open military conflict is not viewed as very likely neither for Moscow nor for Beijing, although it is not excluded. This leaves the door open to hybrid threats, a mechanism that has roots in authoritarian strategic culture but also has national specificities. The things that can go wrong in the SEES model are challenged by the new information environment being manipulated according to the tactics of hybrid threats. Even if the EU is not a military alliance, while NATO is, both organizations are challenged in similar ways by hybrid threats. Given several factors, including overlapping membership, it is clear that weakening one will also weaken the other. Therefore, in the landscape of hybrid threats, the EU and NATO are considered as a united target by hostile actors – and they can also best counter and respond to these threats if working together.

[2] Group thinking is a phenomenon that occurs when a group of well-intentioned people makes irrational or non-optimal decisions spurred by the urge to conform or the belief that dissent is impossible.

Against this backdrop, here follow some recommendations aimed to policy-makers and expert communities in both NATO and EU countries:

- The importance of analysis is growing. Too much effort has been put into collecting data, and not enough into training analysts. Older analysts need to be trained about the new information environment and its functioning. In turn, the younger generation needs to be trained on history, context and connections. Central elements in training are understanding the psychology of the adversary, the assessments of motivations, and rationales.

- The cultural context of information is lost in the volume of information. International cooperation, especially on the part of an alliance like NATO, needs to be lifted to a new level. This does not only concern joint situational awareness about hostile actors, but also involves understanding partners and their perspectives. Without that mutual understanding among allies and partners, divergences can become over politicized and decision-making paralyzed, which is what the actors behind hybrid threats want.

- There is a need for more effective training in the use of open-source intelligence, focusing on the sources and tools for finding information, including the biases they may have. In addition, more knowledge is needed to be able to detect linkages between actions. Hybrid threat activities start in a settled way, often on a very legal basis, and the potential for such activities to turn into hostile acts needs to be recognized.

- Military communities should reach out more often to non-military expert communities. To counter hybrid threats, a multidisciplinary approach needs to be taken, which really means combining different disciplinary fields and expertise coming from practitioners, academics and the private sector.

- Sharing the vocabulary is important when building situational awareness. Civil-military cooperation is needed here. The civilian side uses different words than the military and sometimes, even if the understanding of a concept would be shared, actors do not understand due to the use of different terms, and discussions can turn into an unnecessary battle of words.

References

Brooker, Paul (2014). Non-Democratic Regimes. Basingstoke: Palgrave Macmillan.

Cullen, Patrick J, & Erik Reichborn-Kjennerud (2017). “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare”. In Multinational Capability Development Campaign (MCDC).

Detweiler, Christopher (2009). “An Introduction to the Modern Chinese Science of Military Supraplanning”. In University of Freiburg, Faculty of Philosophy.

Dokos, Thanos (2014). “The Ukraine Crisis: A Story of Misperceptions, Miscalculations & Mismanagement Is There Still Time to Avoid Permanent Damage to the European Security Order?”. In Hellenic Foundation for European and Foreign Policy (ELIAMEP), ELIAMEP Thesis.

EU-HYBNET (2020). Deliverable, for internal use only.

Fridman, Ofer (2018). Russian Hybrid Warfare - Resurgence and Politicisation. London: Hurst&CO.

Giannopoulos, Georgios, Hanna Smith and Marianthi Theocharidou (2020). "The Landscape of Hybrid Threats: A Conceptual Model". In European Commission.

Glenn, John (2009). "Realism Versus Strategic Culture: Competition and Collaboration?". In International Studies Review, Vol. 11, No. 3, pp. 523-551.

Gray, Colin (2006). "Out of the Wilderness: Prime Time for Strategic Culture". In United States Nuclear Strategy Forum, Publication No. 0004.

Hoffman, Frank G. (2010). "'Hybrid Threats': Neither Omnipotent Nor Unbeatable". In Orbis, Vol. 54, No. 3, pp. 441-455.

Jamieson, Kathleen Hall (2018). Cyberwar - How Russian Hackers and Trolls Helped Elect a President. Oxford: Oxford University Press.

Kent, Thomas (2020). Striking Back Overt and Covert Options to Combat Russian Disinformation. Washington, DC: Jamestown Foundation.

Lauder, Matthew A. (2019). Expert view, non-public. In The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Lefebvre, Vladimir A. (1984). Reflexive Control: The Soviet Concept of Influencing on Adversary's Decision Making Process. Englewood, CO: Science Applications, Inc.

Linz, Juan J. (2000). Totalitarian and Authoritarian Regimes. London: Lynne Rienner Publishers.

Miklossy, Katalin & Hanna Smith (2019). Strategic Culture in Russia's Neighbourhood - Change and Continuity in an In-Between Space. Lanham: Lexington Books.

Mumford, Andrew (2020). "Ambiguity in Hybrid Warfare". In The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), Hybrid CoE Strategic Analysis, No. 24.

NATO (2020). "NATO 2030: United for the New Era".

Nojonen, Matti (2019). Expert view, non-public. In The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Omand, David (2020). Interview with the author

Omand, David (2010). Securing the State. London: Hurst & Co.

Svolik, Milan W. (2012). The Politics of Authoritarian Rule. Cambridge: Cambridge University Press.

Thomas, Timothy (2002). "Reflexive Control in Russia: Theory and Military Applications". In Reflexive Processes and Control, No. 2.

Thomas, Timothy (2004): "Russia's Reflexive Control Theory and the Military". In Journal of Slavic Military Studies, Vol. 17, No. 2.

Vasara, Antti (2020). "Theory of Reflexive Control Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy." In Finnish National Defense University.

HYBRID THREATS TO ALLIED DECISION-MAKING: MERGING WHACK-A-TROLL TACTICS WITH WHOLE-OF-SOCIETY DEFENSE CONCEPTS

Franz-Stefan Gady - Institute for International Strategic Studies

Abstract

This chapter seeks to offer preliminary answers to two questions. First, to what degree will Artificial Intelligence (AI)-enabled information warfare exacerbate hybrid threats to NATO decision-making? Second, what can NATO countries do to alleviate the threat? To narrow the research scope, this chapter will principally look at threats posed by Russian AI-enabled information warfare operations under the concept of *gibridnaya voyna*. The study argues that given that AI-enabled information warfare has the potential to amplify societal polarization, elite disagreement within domestic politics, and reshape the perception of the "Russian threat" in NATO member countries, it can have a direct negative impact on national and NATO decision-making. Such operations, however, only amplify existing symptoms of polarization and disagreement found within NATO member states and are not their root causes. The chapter concludes that NATO must better integrate tech-centric so-called "whack-a-troll" tactics with a whole-of-nation strategy to better safe-guard NATO decision-making and alliance cohesion. Renewed discussion of whole-of-society defense concepts to inform national security strategies may be useful in this regard.

Introduction

NATO defines hybrid threats as threats that "combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces" (2019). Such hybrid methods are used to blur the line between war and peace and "attempt to sow doubts in the minds of target populations." NATO further emphasizes that "[t]he speed, scale and intensity of hybrid threats have increased in recent years." The latter can partially be traced back to various technological advances including in the fields of Artificial Intelligence (AI) and offensive cyber capabilities, utilized in conjunction with deliberate attempts by competitor nations to undermine the political cohesion of NATO member states from within.

Hybrid threats pose a number of unique challenges to political decision-making within both NATO member states and the Alliance's various deliberative bodies, where decisions are based on the principle of consensus preceded by consultation processes (NATO, 2020). In particular, meddling by outside powers in political processes by means of influence operations, broadly defined as "organized attempts to achieve a specific effect among a target audience," is one of the top concerns of NATO leadership (Thomas et al., 2020). In particular, Russian tactical-operational influence operations under the concept of *gibridnaya voyna* ('hybrid warfare') have been receiving a great deal of attention since 2014. As Ofer Fridman notes, such operations target society at large, seeking to undermine political cohesion in an adversary state by employing methods that amplify the divisions and polarizations among its citizens (2018).

Definitional confusion has plagued the discussion on hybrid warfare. Fridman, who sketches the conceptual evolution of the term in both the West and Russia, points out that at least three different phenomena have been described as hybrid warfare in past years with no agreed upon definition. Indeed, the term 'hybrid warfare' itself may at this point obfuscate rather than clarify modern conflict characteristics. As Fridman argues:

> "Despite the political usefulness of the term hybrid warfare, it would appear that Russian and Western military professionals now recognize that the term is next to useless for describing the real nature of contemporary conflicts, leading them to promote more specific definitions, such as information warfare, cyber warfare, which are now prevalent in the West, or new-generation-warfare, which is currently prevalent in Russia" (2018: 157).

Indeed, the Russian Chief of the General Staff, General Valery Gerasimov, has publicly aimed to draw a distinction between new-generation warfare and hybrid warfare with the former – given its emphasis on military capabilities – being the main focus of the Russian Armed Forces (Fridman, 2018).

Nonetheless, it is evident from a review of Russian military literature that hybrid warfare focused on weakening societal cohesion of an opponent still retains a prominent spot in Russian national security thinking. For example, a 2015 article on future warfare published in the widely-read journal of the Russian Ministry of Defence stated in strong terms the centrality of information to the Russian understanding of future war, asserting that "it is precisely the information-psychological struggle which will, in the main, create the preconditions for the achievement of victory [in future warfare]". The article, authored by two frequent contributors on future warfare, continued:

> "…the achievement of strategic objectives in future wars will be impossible without the establishment of information dominance over the enemy. In future wars, special disinformation operations and [operations for] misleading the military-political leadership of the other side will include a system of interconnected and carefully-agreed upon large-scale measures according to the plan of new-type war ('hybrid war'), including the use of various means of actions upon the personnel of the armed forces and population of the state with the objective of creating internal tension (schism) in society. Information-psychological operations in future war will pursue by non-forceful means the objective of achieving the significant weakening of the military potential of the enemy by means of affecting his information processes, misleading [him], demoralizing the population and the personnel of the armed forces" (Bogdanov and Chekinov, 2015: 45)

As part of such future Russian *gibridnaya voyna* campaigns, the effective integration of AI with cyber capabilities that enable faster and more precise weaponization of information has the potential to compromise and undermine NATO decision-making at multiple levels. This chapter consequently seeks to offer preliminary answers to two questions in this regard. First, to what degree will AI-enabled information warfare[1] exacerbate hybrid threats to NATO decision-making? Second, what can NATO countries do to alleviate the threat?

To narrow the research scope, this chapter will principally look at threats posed by Russian influence operations under the concept of *gibridnaya voyna*.

[1] Henceforth, the term 'AI-enabled information warfare' will be used to describe the integration of AI with cyber capabilities for the purpose of influence operations.

Factors Influencing NATO Decision-Making

In order to answer to the above questions, it is first necessary to outline the various influences that impact allied decision-making within NATO. According a recent RAND study, member states' decision-making processes on their own participation in NATO operations can be broadly divided into three categories:

- Domestic politics;
- Perception of the Russian threat;
- Alliance dynamics (Binnendijk and Priebe, 2019).

Notably, RAND finds that domestic politics and perceptions of the Russian threat have the larger impact in decision-making processes involving an unconventional (i.e. hybrid) attack on a NATO country. In the future, such an attack would undoubtedly feature AI-enabled information warfare as part of *gibridnaya voyna* embedded within a new-generation warfare campaign. Consequently, this chapter will primarily focus on domestic politics and perceptions of the Russian threat to illustrate Russian tactical-operational AI-enabled information warfare.

According to the RAND study, domestic political considerations that influence decision-making regarding support or opposition to NATO military action in an unconventional environment are impacted by a number of factors, including the proximity of public elections, general public support for a particular course of action, elite agreement or disagreement (coalition governments can be particularly vulnerable in this case), and a centralized or decentralized foreign policy decision-making structure. Perceptions of the Russian threat in turn are also subject to a number of factors including perceptions of Moscow's aims and motivations, escalation risks, vulnerabilities to Russian economic sanctions as well as military retaliations, and competing national security demands (Binnendijk and Priebe, 2019).

Most relevant for this chapter is that in both instances – domestic politics and perceptions of the Russian threat – AI-enabled information operations have the potential to influence factors in favor of Russia. For example, such operations could expand the audience reach of NATO-skeptical parties during election seasons, or in advance of a parliamentary vote in order to undermine elite consensus on anti-Russian actions. Alternatively, with the help of a carefully crafted 'what aboutism' narrative employed part of a wider disinformation operation, Moscow could amplify disagreement over aggressive Russian actions within a target country by emphasizing online that Russia, like any other country, is merely pursuing legitimate self-interest.

AI-Enabled Information Warfare

AI-enabled information warfare entails the use of algorithms capable of processing and learning from big data to execute attacks against specific targets autonomously or semi-autonomously in order to achieve a desired effect in the information space.[2] The terms 'autonomously' and 'semi-autonomously' describe respectively the ability of the algorithm without or with (limited) human intervention to learn from vast amounts of data in order to execute polymorphic attacks on multiple fronts in the information space (for example, simultaneous attacks on a microblogging site synchronized with emails phishing attacks), in which

[2] This is an expansion of a definition of AI found in Wright (2019: 317): "AI can be used for offensive and/or defense purposes; it can take many forms but essentially AI comprises algorithms capable of processing and learning from vast amounts of data and then taking decisions autonomously or semi-autonomously."

the algorithm is capable of changing its identifiable features (for example, by creating multiple malicious online identities fitted with unique malware packages). The most relevant media for AI-enabled information warfare are audio, text and video (Giles and Hartmann, 2020). Furthermore, AI-enabled information operations target all interrelated dimensions of the information environment – physical, informational, and cognitive/emotional. Herbert Lin and Jaclyn Kerr define the information environment as, the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (2019: 4).

AI-enabled information warfare methods may plausibly be deployed in various other ways. For example, AI-enabled algorithms permit the building of realistic simulations of individuals "to test every individual's reaction to events (both virtual and real), advertising, political campaigns, and psychological operations, and even to guess what might go viral through person-to-person interactions" (Libicki, 2017: 52). Such simulations could be created by deploying an algorithm capable of pattern recognition to study the social media behavior of a select target group of individuals in a specific country. This in turn could be used to create personalized phishing emails for social engineering attacks, but also to create so-called 'deepfakes' to gain access to sensitive systems or to facilitate the spreading of disinformation. Another example is the use of bots in order to 'hijack' public perceptions: "Bots, trolls, and sock puppets can invent new 'facts' out of thin air leading to a polarized society and a culture of mistrust" (Wright, 2019: 318). The main objective behind creating alternate facts would not be to create a convincing alternative narrative – which is an objective of strategic communications – but rather to erode the solidarity of groups facing the same threat by playing on the fears and anxieties of individuals (Libicki, 2017).

In sum, AI-enabled information warfare differs from 'regular' information warfare in four crucial areas:

1. Speed: AI can accelerate the pace of operations by, for example, faster identifying targets due to the expedited operationalization of cyber intelligence, surveillance and reconnaissance (ISR) data as a result of increased pattern recognition capabilities of algorithms.
2. Scope: AI can expand the scope of information warfare operations by semi-autonomously or autonomously executing polymorphic attacks on multiple platforms with the help of bots, trolls, or sock puppets.
3. Scale: AI can increase the chances of a particular message or narrative going 'viral' in the information space by, for example, self-learning algorithms 'wargaming' the potential impact of specific content online, or AI-enabled facial recognition software that is capable of recognizing emotional states of individual humans.
4. Sophistication: AI can not only increase the sophistication of microtargeting processes, but also facilitate the creation of ever more convincing synthetic media products (such as 'deepfakes') with the support of Generative Adversarial Networks (GANs) where it is increasingly difficult to separate real from synthetic identities (Rocca, 2019).

Since AI is both scalable and effective, it is likely to be of significant utility to those seeking to undermine Western democracies because it will permit adversaries to avoid making tradeoffs between scale and effectiveness. In particular, AI will likely allow adversaries to expand exponentially the scale and rate of attacks, while also increasing the number of targets (Rocca, 2019). In addition, the following factors are all likely to enhance the utility of AI in information warfare: societies' growing dependence on cyberspace as a news source; citizens' increased reliance on social media; the difficulties individuals face in distinguishing between fake and genuine news sources; the unprecedented levels of access to information; and the speed at which information can be spread between individuals (Giles and Hartmann, 2020).

AI, however, is no panacea for influence operations. The impact of AI-enabled information warfare will largely depend on the quality of input data on the one hand, and continue to be contingent on analogue factors that may be too difficult for algorithms to effectively process on the other (for instance, various cultural and historical factors that may impact a society's reaction to a particular event).

Furthermore, an overreliance on AI-enabled technology, in particular for conducting information warfare operations in cyberspace, may be misguided given the uncertainty surrounding the degree to which AI will favor the offense or defense (Dafoe and Garfinkel, 2019b). Building on the literature analyzing 'regular' or conventional cyber attack and defense operations (given that AI-enabled information warfare operations will mainly be conducted through this domain), broad generalizations on the subject are misplaced. As one analysis regarding the offense-defense balance in cyberspace puts it: "Sweeping claims about the offense-defense balance in cyberspace are misguided because the balance can be assessed only with respect to specific organizational skills and technologies" (Slayton, 2016: 72).

Nevertheless, there is some evidence that certain methods appear to favor the offensive. As a digital forensics expert notes regarding deepfake technology, "the adversary will always win, you will always be able to create a compelling fake image, or video, but the ability to do that if we are successful on the forensics side is going to take more time, more effort, more skill and more risk" (Giles and Hartmann, 2020: 236). Another analysis notes that scaling effects will likely be an important factor in determining the offense-defense balance (Dafoe and Garfinkel, 2019a). Nonetheless, it is unclear whether, for example, increased automation alone will ultimately favor the attacker or defender. Given that AI-enabled information warfare will be carried out principally through cyberspace, the uncertainty surrounding presumed technical solutions should therefore be kept in mind by policymakers.

If no discernible offensive advantage can be achieved, there is the risk of an information war of attrition with no clear winner but with excessive collateral damage sustained by society overall. The series of Chinese-backed Covid-19 disinformation campaigns executed in 2020 are a good example of this, having inflicted lasting damage on the information spaces of a number of Western democracies despite the adoption of successful countermeasures by governments (Ha & Cho, 2020). As these campaigns have shown, an information warfare stalemate would likely be more harmful to democratic societies that assume the presence of free speech as a norm than to authoritarian societies where the flow of information is under tighter control, and where consequently a disruption of the information space will have fewer consequences.

AI-Enabled Information Warfare Boosting Hybrid Threats

AI-enabled information warfare will likely differ from 'regular' information warfare primarily in speed, scope, scale and level of sophistication. In the context of *gibridnaya voyna*, its ultimate aim will be to weaken societal cohesion by non-military means. Although Russia is actively developing AI-enabled information warfare tools (including cyber warfare weapons) which may well produce "game-changing strategic effects" (Miron & Thornton, 2020: 12), all known Russian information warfare campaigns carried out against NATO countries to date have been regular ones.

A.) Domestic Politics

The Russian operation to influence the US presidential elections of 2016 remains a prime example of Moscow's use of information warfare methods to interfere in Western politics. An influence operation, spearheaded by Unit 26165 of the Russian military intelligence agency (GRU) and the

Russian Internet Research Agency (IRA), compromised the US information space (Nakashima & Troianovski, 2018). Russian efforts included a deliberate doxing campaign to discredit the Democratic leadership via the release of information from hacking the network of the Democratic National Committee (DNC) and the spread of tailored disinformation on social media channels (Rid, 2020). The effort consumed significant manpower and financial resources and was conducted over a number of years. Inmid-2016, the IRA's US unit had a staff of around 80 and a monthly budget of USD 1.25 million (Jankowicz, 2020). The IRA's 67,502 organic Facebook posts are known to have been shared and liked tens of millions of times and to have generated almost 3.5 million comments. While the precise impact of the Russian operation remains unclear, as Nina Jankowicz observes: "[B]y creating and tending to trusted communities of hundreds of thousands of individuals over the course of several years, Russian operatives were able to encourage some Americans to show up to protests. They changed behaviour [emphasis added]" (Jankowicz, 2020: 9).

B.) Perceptions of the Russia Threat

Though it was not ultimately successful, the Russian influence operation executed in the opening stages of the 2008 Russia-Georgia war provides an excellent case study of an attempt to alter threat perceptions of Russia: Georgia is believed to have acted as a "training ground" for Russian information warfare (Jankowicz, 2020: 57). Although it remains unclear whether Russia or Georgia initiated hostilities, Moscow attempted to use information operations to cultivate a narrative blaming the opponent for beginning the war. Georgia faced a wave of Distributed Denial of Service (DDoS) attacks that took down the websites of government agencies, media outlets and other institutions that would be critical to counter a Russian disinformation campaign, followed by Russian disinformation effort, including the dispatch of a large number of state-sponsored journalists South Ossetia to report on the war from a Russian perspective. Russia's government officials and television personalities resorted to terminology including "genocide", "ethnic cleansing" and "humanitarian catastrophe" in relation to Georgia, and "peace enforcement" in relation to Russian operations, driving the narrative that Moscow had acted as a guarantor of peace and not an aggressor (Jankowicz, 2020).

Nevertheless, the Georgian leadership was able to mount an effective campaign of counter measures in the international media. The inefficacy of the Russian attempts to control the narrative internationally are thought to have provided the impetus for the rebranding of state-controlled media outlet in RT: in particular, the poor English language skills of Russian commentators is widely understood even amongst RT employees to have significantly diminished Kremlin's efforts. As the editor-in-chief of RT later put it, "Russia looked so pale compared to the Georgians, it broke my heart" (DFRLab, 2018; Jankowicz, 2020). As the head of the Russian Military Forecasting Center lamented in an op-ed in the Russian government newspaper Rossiyskaya Gazeta: "For Russia the informational war has become World War III. It was lost by Russia in 2008, during the first five days of the hostilities in the Caucasus" (Jankowicz, 2020: 66).

Neither cases mentioned above offers particularly conclusive evidence that Moscow achieved what it set out to do: in Georgia, it is obvious that there were serious shortcomings on the Russian side; in contrast, in the US, Russian information warfare operations probably changed behavior but the assessment of success remain debatable. Overall, however, it appears that the Russian information warfare campaign in the US was more successful than Russian operations in Georgia.

AI might change that, if left unchecked. Based on the framework outlined in the previous section, AI-enabled information warfare would presumably be capable of achieving better effects within a shorter time frame and with less manpower, while widening the scale, scope, and sophistication of such an operation. In particular, it could help establish a dominant narrative based on disinformation that would be difficult to counter, although the Georgia case is also illustrative of the inherent limits of information warfare when other basic skill sets are lacking – for example, the ability to communicate convincingly in a foreign language or other cultural influences missing from Big Data. Noticeably, there has been noticeable progress in the creation of audio deepfakes as a result of improvements AI-generated synthesized voice capabilities (Giles and Hartmann, 2020).

Miron and Thornton's analysis of Russian military thinking on AI notes that the latter in combination with information operations at the grand strategic level has received considerable attention (2020). In particular, the AI-enabled spread of disinformation has been the focus of discussion. Confusion as a result of disinformation would "have a deleterious effect on an adversary state's decision-making as there would be very little reliable information to base it on" the analysis notes summarizing the conclusions of Russian sources. It continues:

> "Fundamentally, faith would be undermined in everything from government announcements to the accuracy of GPS readings. Without faith in information, governments, societies and military organizations cannot effectively operate. State functions may collapse simply under the weight of an inability to discern truth. A 'cognitive war' would be fought and won" (Miron & Thornton, 2020: 16).

As a result, it is fair to assume that by undermining domestic political cohesion, Russian AI-enabled information warfare capabilities, given their scalability and effectiveness, would indeed boost hybrid threats to NATO decision-making.

Whack-A-Troll Tactics

To date, the efforts of NATO member states, spearheaded by platform providers such as Twitter and Facebook, to respond to information warfare campaigns have by and large focused on technical solutions built around so-called "whack-a-troll" tactics (Jankowicz, 2020: 208). US-led NATO operations in Macedonia represent an important example (Barnes & Santora, 2018). Such tactics – typically involving the deletion of fake or abusive accounts – are time-consuming and typically endless. There has been growing interest in using AI to create anti-troll software that can autonomously identify and block such accounts (Chiwhane et al., 2019). In the near future, social media companies with the help of AI could indeed be capable of identifying millions of fraudulent or malicious accounts per day. Additionally, concerted technical efforts have been made to prevent deceptive information attacks on specifically AI-enabled systems (Keller, 2020). At the same time, the United States in particular has also more actively tried to combat Russian information operations under Pentagon Cyber Command's "persistent engagement" posture, abandoning its previous focus on cyber deterrence paired with resilience (Barnes, 2020).

Researchers have also suggested a host of other technical and organizational responses. For example, Giles and Hartman outline a set of possible countermeasures (2020: 249):

- Exploring methods of technical authentication of digital material;
- Content provenance through digital signatures;

- Considering further applications of digital signatures;
- Continuing efforts to restore trust in independent media and journalism;
- Inducing social media platforms to enhance the detection of fakes and to install means to allow users to evaluate the reliability of content;
- Ensuring the availability of national or supranational authorities to which civilians can report instances of malign influence campaigns;
- Following the example of Singapore, forcing social media platforms to mark fake or false content (including any repost or shared post of the initial material).

However, as outlined in the previous section, technical countermeasures and responses at the tactical and operational level will only go so far in responding to AI-enabled information warfare.

Whole-of-Society Defense Concepts

As a result, responding to AI-enabled information warfare that could compromise allied decision-making will require a more strategic response that may include military tactical-operational whack-a-troll and 'hack-back' or active defense methods,[3] yet embedded within a whole-of-society defense concept. Such 'total defense' concepts are slowly being reintroduced by NATO partner countries such as Sweden and Finland, as well as by member states like Denmark, Estonia, Latvia, and Lithuania (Kepe & Osburg, 2017). Not only could these concepts inform national security strategies of Allies and provide frameworks, for instance, for more effective private-public cooperation in combating malicious activities in cyberspace – they could also inform educational curriculums to provide citizens with "information warfare literacy", i.e. raise awareness of threats that could compromise a country's information environment. Latvia has already introduced such a national security curriculum in its schools (Gavrilko & Leimane, 2020). Estonia has been promoting "digital competence" in its school curricula (Republic of Estonia, 2011).

Within NATO, this could be complemented by the introduction of a dedicated, annual information warfare exercise that includes civilian policy makers, military staff, representatives from platform providers, members of media organizations, as well as lawmakers. Such exercises could help build a best practice database for information operations and whole-of-society defense concepts maintained by a NATO Center of Excellence (CoE). This could ultimately contribute to a NATO-wide adaption of a set of baseline requirements on information as they already exists for resilience.[4] A good starting point for this discussion, for example, could be the "ABC" framework presented by the Transatlantic Working Group (François, 2019). This particular framework sub-divides information warfare campaigns into three broad categories – manipulative actors, deceptive behaviors, and harmful content – to facilitate cooperation between policy makers and regulators.

AI-enabled information warfare may also demand structural and organizational changes within NATO and in member countries. For example, there needs to be more serious deliberation on introducing necessary structural changes within the Alliance to enable speed and flexibility in executive decision-making in the face of hybrid threats. As one study notes, this could include delegated authority for the Supreme Allied Commander for Europe (SACEUR) "to alert, prepare and stage forces based on intelligence indicators and

[3] The Tallin Manual Glossary defines active defense as "A proactive measure for detecting or obtaining information as to a cyber intrusion, cyberattack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber counter-operation against the source" (Schmitt, 2013: 257).
[4] This idea was introduced by Eugenio Cusumano during the November 17 NATO Transformation Command workshop (Shea, 2016).

while consulting NATO civilian authorities" (Lute & Burns, 2019: 23). In the United States, there have also been discussions about creating information warfare commands that would subsume the respective cyber commands of the individual service branches to "encourage decision-makers to think of information warfare in the holistic sense that has long eluded the service and the nation" (Crane, 2019). However, the role of the Armed Forces and NATO's in combating hybrid threats overall, and AI-enabled information warfare in particular, will remain limited given that the majority of these efforts rest with civilian and not military authorities. Consequently, even if whole-of-society defense concepts are introduced, it would not automatically lead to more resilient NATO decision-making processes.

References

DFRLab (Atlantic Council Digital Forensic Lab) (2018). "Question That: RT's Military Mission". In Medium.

Barnes, Julian (2020). "U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China". In The New York Times.

Barnes, Julian & Mark Santora (2018). "In the Balkans, Russia and the West Fight a Disinformation-Age Battle". In The New York Times.

Binnendijk, Anika & Miranda Priebe (2019). "An Attack Against Them All? Drivers of Decisions to Contribute to NATO Collective Defense". Santa Monica, CA: RAND Corporation.

Bogdanov, Sergey & Sergey Chekinov (2015), "Prognozirovanie xaraktera i soderzhaniya vojn budushhego: problem i suzhdeniya" ["Forecasting the Character and Content of Future Wars: Problems and Judgements"]. In Voennaya mysl [Military Thought], No. 10. [Translations for this article by A Stronell].

Burns, Nicholas & Douglas Lute (2019). "NATO at Seventy: An Alliance in Crisis". In Belfer Center for Science and International Affairs.

Chiwhane, Shwetambari et al. (2019). "An Effective Analysis of Anti Troll System using Artificial Intelligence". In International Research Journal of Engineering and Technology (IRJET), Vol. 6, No. 12.

Crane, Conrad (2019). "The United States needs an Information Warfare Command: A Historical Examination". In War on the Rocks.

François, Camille (2019). "Actors, Behaviors, Content: A Disinformation ABC: Highlighting Three Vectors of Viral Deception to Guide Industry &Regulatory Responses". In Transatlantic Working Group.

Fridman, Offer (2018). Russian "Hybrid Warfare": Resurgence and Politicization. Oxford: Oxford University Press [See in particular Chapter 5 for a discussion of the term 'hybrid warfare'].

Garfinkel, Ben & Allan Dafoe (2019). "Artificial Intelligence, Foresight, and the Offense-Defense Balance". In War on the Rocks.

Garfinkel, Ben & Allan Dafoe (2019). "How does the offense-defense balance scale?". In Journal of Strategic Studies, Vol. 42, No. 6.

Gavrilko, Guna & Ilze Leimane (2020). "Can National Security be Taught?". In RUSI (Royal United Services Institute), Live Briefing.

Giles, Keir & Kim Hartmann (2020). “The Next Generation of Cyber-Enabled Information Warfare”. In Jančárková, Taťána et al. (eds.). 12th International Conference on Cyber Conflict - 20/20 Vision: The Next Decade. In NATO CCD CoE (NATO Cooperative Cyber Defence Centre of Excellence).

Ha, Matthew & Alice Cho (2020). “China’s Coronavirus Disinformation Campaigns Are Integral to Its Global Information Warfare Strategy”. In Foundation for Defense of Democracies.

Jankowicz, Nina (2020). How to Lose the Information War: Russia, Fake News, and the Future of Conflict. London: I.B. Tauris.

Keller, John (2020). “Industry asked for trusted computing shielding of artificial intelligence (AI) in information warfare”. In Military & Aerospace Electronics.

Kepe, Marta & Jan Osburg (2017). “Total Defense: How the Baltic States Are Integrating Citizenry Into Their National Security Strategies”. In Small Wars Journal.

Libicki, Martin C. (2017). “The Convergence of Information Warfare”. In Strategic Studies Quarterly, Vol. 1, No. 1.

Lin, Herbert & Jaclyn Kerr (2019). “On Cyber-Enabled Information Warfare and Information Operations”. In Oxford Handbook of Cybersecurity. Oxford: Oxford University Press [forthcoming].

Miron, Maria & Rod Thornton (2020). “Towards the ‘Third Revolution in Military Affairs’: The Russian Military’s Use of AI-Enabled Cyber Warfare”. In The RUSI Journal, Vol. 163, No. 3.

Nakashima, Ellen & Anton Troianovski (2018). “How Russia’s military intelligence agency became the covert muscle in Putin’s duels with the West”. In The Washington Post.

NATO (2020). “Consensus decision-making at NATO”. [Last updated October 2020.]

NATO (2019). “NATO’s response to hybrid threats”. [Last updated August 2019.]

Republic of Estonia (2011). “National Curriculum for Upper Secondary Schools”. In Government Regulation. [Last updated August 2014.]

Rid, Thomas (2020). Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux. [See in particular Chapter 28 for details of the DNC hack.]

Rocca, Joseph (2019). “Understanding Generative Adversarial Networks (GANs)”. In Towards Data Science.

Shea, Jamie (2016). “Resilience: a core element of collective defence”. In NATO Review.

Slayton, Rebecca (2016). “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment”. In International Security, Vol. 41, No. 3.

Schmitt, Michael N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press.

Thomas, Elise, Natalie Thompson and Elizabeth Wanless (2020). “The Challenges of Countering Influence Operations”. In Carnegie Endowment.

Wright, David (2019). “AI and information warfare in 2025”. In 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, pp. 317-322.

WORKING GROUP REPORT

HYBRID THREATS TO ALLIED DECISION-MAKING

Andrea Locatelli - Catholic University of the Sacred Heart

Scholars and analysts have been debating for decades over the features of the current security scenario. Terms like 'risk' (as opposed to 'challenge'), 'new wars', 'asymmetric conflicts', 'fourth-generation warfare', 'other-than-war operations', are just cursory examples of the richness of this debate. Seen from this perspective, hybrid threats are just the latest attempt to make sense of the security challenges that contemporary societies are asked to face. It is therefore hardly surprising that much emphasis has been placed in recent times on this term, both for analytical and prescriptive purposes. Unfortunately, as witnessed by the (at times lively) discussions in the three sessions of Working Group (WG) 2, it seems that the security scenario remains too complex to be easily captured by this concept, with the ensuing result of complicating the task of inferring policy prescriptions.

Nonetheless, benefiting from the heterogeneous composition of the WG, which included both academics and practitioners, participants in the discussion engaged in a fruitful debate. They initially focused their attention on how to understand the features of hybrid threats and identify the vulnerabilities exposed by these threats; then, they moved on to define the challenge posed by hybrid threats to decision-making; finally, they discussed policy prescriptions aimed at strengthening NATO's role in tackling the impact of hybrid threats on these vulnerabilities. In a nutshell, each session centered around one of the following questions:

1. What do we mean by hybrid threats and why are they a reason of concern?
2. How do hybrid threats exploit vulnerabilities to undermine NATO's and NATO member states' decision-making?
3. What can NATO do about it?

The next three sections of this report present a concise summary of the main conclusions reached by the WG for each of these questions.

The Meaning of Hybrid Threats

Hybrid threats is a broad category encompassing a variety of actors, actions and targets. Actors engaged in hybrid threats include states as well as private actors, being them organized groups or even individuals; actions span from propaganda up to physical violence to coerce an opponent; among targets, we can count national and supranational institutions, but also societies at large. This is hardly a novelty: as one of the participants of the WG noted, none of the above-mentioned components is new; however, their combination has actually brought unprecedented effects. So, the panellists' first task has been to identify which of the hybrid threats had to be the prime focus of attention. While some disagreement remained on the borders of the broad constellation of actions and tools underlying hybrid threats, all participants agreed on some core elements. Three in particular stood out:

- Information is key under several respects. Information refers to a variety of assets, like Big Data and Artificial Intelligence (AI). The two usually come in tandem, since AI entails the use of algorithms to learn from Big Data with a view to exploit vulnerabilities. Information Technology (IT) also includes bots and deepfakes, which are central to undermine societal cohesion.

- Digital connections are the underlying infrastructure used to perpetrate hybrid threats. Our societies rely on virtual world platforms that can be targeted by potential attackers. This is not just a matter of physical vulnerability: since global networks defy borders and limit state jurisdiction, they are harder to defend and allow potential attackers to act below the threshold of detection and attribution.

- Hybrid threats benefit from the unprecedent speed and scope of information. A consequence of the previous point is that information spreads freely – and virtually in real time – in Western societies. Again, this is not new in principle, but it has reached game-changing levels. On the one hand, managing this massive flow of information is just prohibitive for NATO and its member states; on the other hand, high speed of circulation translates into increased operational tempo.

Having defined the pillars of hybrid threats, the second task has been to identify the main features of these threats, which imposed to answer ancillary questions like: 1) Whence the origin of these threats? 2) Which tools could potential enemies employ? 3) Which targets are most likely to be affected?

1. As mentioned, various actors may perpetrate hybrid attacks. However, due to their actual capabilities, intentions, and recent record of actions, China and Russia have been identified by most participants as the most gathering threat. The latter, in particular, is considered more likely to pose the greatest challenge to NATO. Two participants raised a challenging point by noting how this line of argument may actually benefit Russia, since it leads us to overthink the enemy and potentially overreact to Russia's provocations. However, others observed how the Russia followed similar patterns of behavior during the Ukrainian crisis (2014), Brexit (2016) and the 2016 US elections. It is therefore the main reason of concern for NATO.

2. A direct consequence of the elements discussed above is the variety of means that potential attackers could employ to perpetrate attacks. The list of tools available would be overly technical and exceedingly long for the purposes of this report. For this reason, the discussion in the WG focused on info-warfare capabilities. As one of the participants stressed, a reason of concern should not be just the availability of multiple tools, but also – and most importantly – their combination to create linear and non-linear effects.

3. Hybrid threats may take aim at a variety of targets, but participants of the WG agreed that societal cohesion should take center stage in the discussion. Particularly concerning are offensive actions that might lead to societal polarization, elite disagreement and biased perceptions of foreign actors. Some participants noted how difficult it will be for NATO to tackle this kind of actions. However, as discussed in the next sections of this report, these actions have the potential to affect decision-making at different levels.

Following these considerations, at the end of the first session of the WG, convergence emerged towards a definition of hybrid threats that focuses on state-led AI-enabled information actions deliberately aimed at undermining democratic states' institutions.

Vulnerabilities and Challenges to Decision-Making

What follows from the previous discussion is that hybrid threats are so compelling due to their capacity to exploit previously unexplored vulnerabilities. Or better, to exploit built-in features of Western societies as susceptibilities. In particular, the discussion focused on three different layers of vulnerability.

- As anticipated in the previous section, the first layer hinges on Western societies' dependence on global networks – i.e. complex infrastructures that transcend state borders and are either owned or run by private companies. It is therefore possible for potential attackers to take aim at targets outside a state's jurisdiction, or to take advantage of opportunities opened by different jurisdictions. Secondly, hybrid attacks may be directed against private actors with a view to achieve strategic outcomes in the public domain. Thirdly, adversaries might use private platforms (e.g. social media) to manipulate information.

- The second layer of vulnerability concerns Western societies. To put it simply, one of the main goals that adversaries want to achieve is to inflate societal divisions. This is certainly not a novel kind of vulnerability. In fact, dividing lines (being them in the form of ideological, ethnic, linguistic, religious or economic cleavages) are an integral part of any society. However, empowered by Information Technologies, adversaries may take advantage from polarization – i.e. increased divergence among groups – and sow the seed of discord in our societies. The essence of this threat is not that different from classical subversion, but it is more problematic because it can be done covertly, persistently, and with transnational effects.

- The third layer of vulnerability concerns the foundations of democratic institutions. It is obviously related to the previous layer, but it is distinct, since it exclusively involves the political processes that lead to policy outcomes. The challenge posed by hybrid threats breaks down in turn into a procedural and an ideational component. The first one relates to the need for democratic systems to work by consensus instead of coercion, which implies public support for policy decisions; the second one boils down to the need for democratic regimes to live up to their core principles, like transparency, rule of law, and freedom of speech/thought.

Potential enemies could take advantage of these vulnerabilities and undermine the decision-making process of NATO states – and by reflex, NATO's too. The WG discussed the main problems that decision makers face when crafting a response to hybrid threats and focused on three in particular:

1. How to respond in non-escalatory ways? Since, as we have seen, hybrid attacks exploit the grey zone to create ambiguity (e.g. manipulating the threshold of detection and granting plausible deniability), decision-makers are faced with the risk of overreaction.

2. How to respond in democratic ways? In the light of previous considerations, it has emerged how potential attackers may severely impair the decision-making process of democratic systems. In

particular, the discussion focused on the democratic constraint to abide by domestic and international law.

3. How to get public support? Since hybrid threats are usually covered or difficult to attribute, policy-makers must persuade the public opinion on the very existence of the threat. This problem impairs most specifically the explanation phase of the policy-making process. This is particularly the case with Russia's attempts to manipulate its perception in Western societies.

Policy Prescriptions

The final session of the WG addressed the final and most important question: what can NATO do to defend the allied decision-making process from hybrid threats? As discussed above, the impact of hybrid threats may affect different kinds of decision-making, from the local to the supranational level. Following the logic of the argument developed so far, the main target of hybrid attacks – the weak ring of the chain – is the state level. NATO's decision-making process is not directly involved in the kind of threats included in the working definition used by the WG, but it is indirectly affected, since political consensus is the working principle of the North Atlantic Council. For this reason, in the third session participants debated several proposals, some of which clearly fall beyond the scope and purpose of the Alliance. However, for the reasons discussed in previous sections of this report, they are worth considering.

As one participant noted, most proposals can be ascribed to two different narratives: the first one is shaped around a strategic logic, while the second is based on a resilience discourse. Both allow us to infer policy prescriptions, so they can be used as a general framework to organize the conclusions reached by the WG. With respect to the former narrative, participants discussed the following proposals:

- Improve and expand NATO's intelligence capabilities. The institution in 2017 of the Joint Intelligence and Security Division (JISD) greatly contributed to increase NATO capabilities and streamline the intelligence process. The creation of a special unit devoted to countering hybrid threats is another welcome innovation. However, better coordination between the civilian and military components in the JISD, more extensive use of open-source intelligence, and improved data analytics resources would be beneficial for NATO's decision-making. In particular, strengthening the JISD might lead to better situational awareness and a clearer perception of Russia's behavior.

- Improve strategic communication: NATO Strategic Communications Centre of Excellence (StratCom CoE), set up in Riga in 2014, is NATO's main tool to harmonize member states' communication and develop original solutions to contemporary challenges. The CoE has progressively increased its activities and integration in NATO's institutions. However, its funds and staff are still limited, as well as its cooperation with other CoEs within NATO and the European Union (EU). Strengthening this body, in particular by letting more member states staff the CoE, would help forge a more effective and shared communication strategy.

- Related to the latter point, NATO can play a role as a catalyzer and promoter of best practices and information sharing. In this respect, the Joint Analysis and Lessons Learned Centre (JALLC) and the Cooperative Cyber Defence Centre of Excellence (CCDCoE) already perform a critical function in terms of training, exercises and research. By diffusing best practices and lessons learnt among Allies,

NATO may raise the quality of national defenses to hybrid threats, to the benefit of the entire decision-making process of the alliance.

In terms of measures aimed at strengthening resilience, most proposals focused on state-level prescriptions. They fundamentally called for a mix of technology-based solutions and doctrinal and organizational innovations. In the words of one of the participants, this approach evokes an analogy with the current Covid-19 pandemic: until a vaccine to hybrid threats will be available, what measures could be implemented to contain the spread and severity of info-attacks? Among the many proposals raised in the discussion, a few deserve consideration here:

- Consensus has emerged on the critical role played by digital literacy: as discussed in previous sections, hybrid threats aim to exacerbate existing societal divisions. Promoting digital literacy is then seen as an effective tool to minimize the impact of info-attacks.

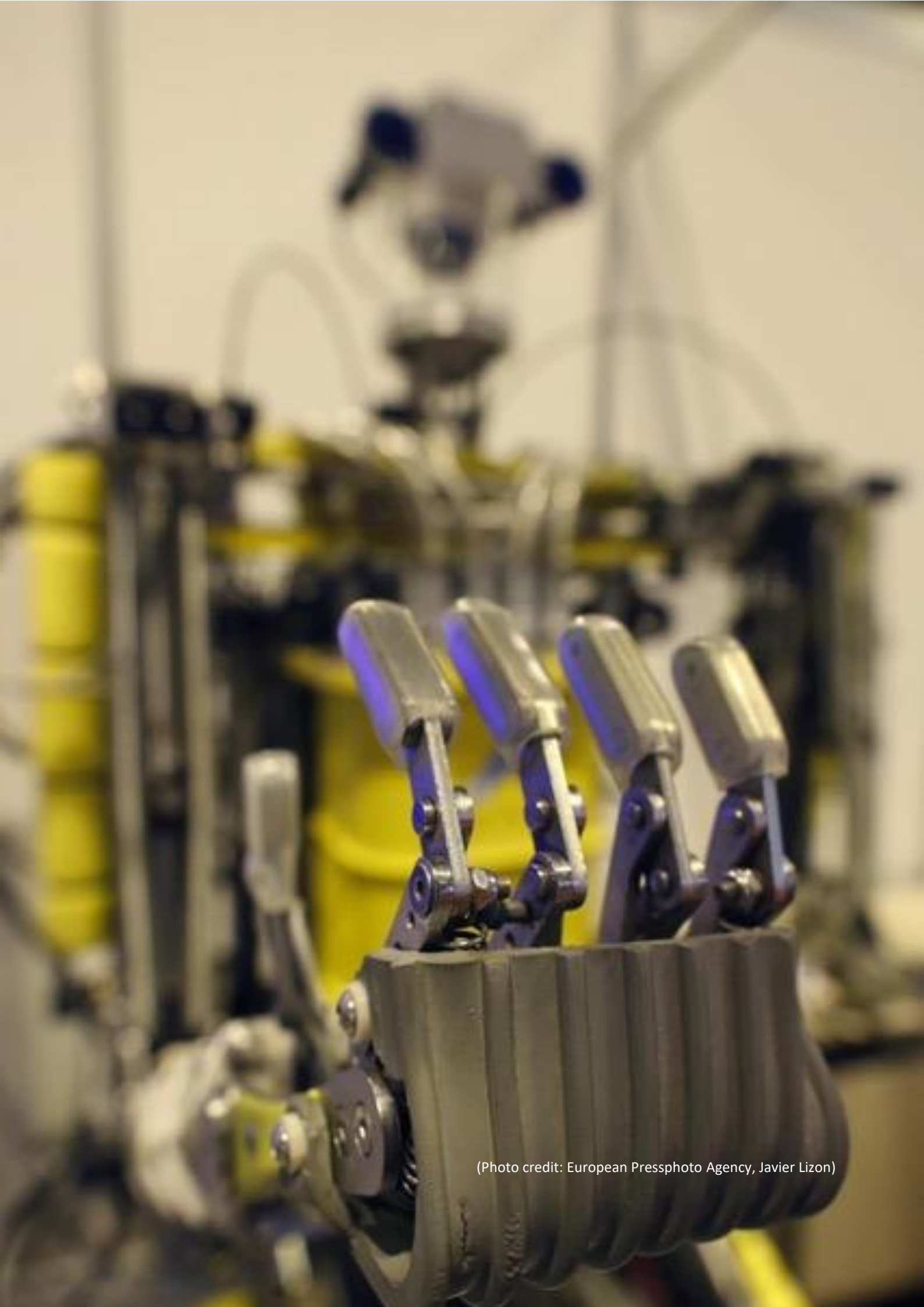
- Participants have also discussed the effectiveness of regulation authorities and other data protection measures. Related to this point, domestic and international law is another tool that may limit the impact of hybrid threats. As one of the participants noted, a clearer definition of what information actions are legitimate and what are not, could limit the opportunities for potential enemies to exploit the grey zone.

- Seen from this perspective, NATO should work more closely with third parties, in particular the European Union – for instance, with the recently appointed Hybrid Fusion Cell (HFC).

Conclusion

The concept of hybrid threats has unquestionably attracted a good deal of scholarly attention in recent years. However, the sheer complexity of the phenomenon it is supposed to capture has limited its heuristic potential. So, it is hardly surprising that the academic community has not come yet to a shared definition and widespread agreement on its utility. Most importantly, these limits have hindered its potential for generating policy prescriptions, thus raising a wall between academia and policy-making circles. Starting from these premises, the WG tried to bridge this gap and provide NATO leaders with a set of prescriptions. In their discussion, participants tried, in the first place, to frame a working definition of hybrid threats. They then discussed how hybrid threats target NATO's and NATO states' decision-making. Finally, they raised a few proposals aimed at increasing NATO's role in countering this kind of threat.

In conclusion, the WG stressed the centrality of societies and their respective governments in countering hybrid threats: being the main target of these threats, it is up to national governments to develop strategies for resilience. However, since different levels of decision-making are confronted with this challenge, NATO is also called into question. In particular, the Alliance can contribute to protect its members with its technical and diplomatic capabilities.



(Photo credit: European Pressphoto Agency, Javier Lizon)

WORKING GROUP III

NATO AND ARTIFICIAL INTELLIGENCE: THE ROLE OF PUBLIC-PRIVATE SECTOR COLLABORATION

Sophie-Charlotte Fischer[1] *- Center for Security Studies, ETH Zurich*

Abstract

NATO has recently started to explore the opportunities and risks of military Artificial Intelligence (AI) applications. One challenge that NATO and its member states face in entering the age of machine intelligence is that commercial technology companies lead in the development of AI. This chapter contributes to the emerging literature and policy debate on alliances and AI by identifying obstacles for NATO arising from the commercially driven innovation ecosystem and analyzing how the militaries of selected member states have tried to overcome them, so far. Examining the strategies of member states provides important clues about similarities and differences in Allies' approaches. Based on this assessment, this chapter also provides policy recommendations for how NATO can proactively shape public-private sector collaboration in AI across the Alliance.

Introduction

Throughout the last decade, significant progress in Artificial Intelligence (AI) and especially the subfield of Machine Learning (ML) has revealed a wide range of possible AI applications including for military purposes. Current assessments suggest that AI – defined here as "the ability of computers and machines to perform tasks that normally require human intelligence" (Sayler, 2020) – could significantly increase the speed and accuracy in areas ranging from military logistics to decision-making on the battlefield (Scharre, 2020). At the same time, security and reliability problems associated with AI systems as well as legal and ethical considerations could limit their deployment in the future (Horowitz, 2018). However, despite these uncertainties, a growing number of countries is already actively pursuing militarized AI technologies.

Recently, also NATO has started to explore developments in AI, including potential use cases and operational and strategic implications. The increasing emphasis on emerging and disruptive technologies within NATO is an attempt to ensure the continued ability of the transatlantic Alliance to "deter and defend against potential threats" (NATO Science & Technology Organization, 2020) but also "that its values, ethical stances as well as moral commitments will remain central in a rapidly changing security environment" (Gilli, 2019: 1). For example, in recent years, NATO has been paying more attention to China as a defense and security actor, whose extensive investments in and pervasive deployment of AI have not gone unnoticed (see e.g. The Reflection Group, 2020). NATO Deputy Secretary General Mircea Geoană suggested that "there are

[1] The author would like to thank the participants of the Conference "NATO Decision-Making: Promises And Perils of the Big Data Age?" for feedback on an earlier draft of the chapter. The author is especially grateful to Alessandro Marrone, Andrea Gilli, Sten Rynning and Mark Webber for their valuable suggestions, which have resulted in a much-improved version of the original manuscript.

considerable benefits of setting up a transatlantic digital community cooperating on Artificial Intelligence" (NATO, 2020). However, NATO is facing a number of challenges in entering the age of machine intelligence.

The objective of this chapter is to investigate one particular challenge to realizing NATO's AI ambitions: the commercial sectors' lead in the development of AI. In contrast to the Cold War, defense is no longer the driving force of technological developments in many emerging technology domains. Instead, commercially oriented firms driven by market forces are leading in fields like AI. Consequently, defense organizations have to increasingly rely on commercial technology companies for access to cutting-edge technology. This reliance, however, creates challenges for NATO and its member states that will be further examined in this chapter.

The structure of the chapter is four-fold. In a first step, it briefly reviews the still nascent academic and policy literature on alliances and AI. Subsequently, this chapter sketches out the structure of the global AI innovation system and identifies the resulting implications for the transatlantic alliance's pursuit of AI. Thirdly, the study sheds light on how three NATO member states – the United States, France and Germany – have so far dealt with the role of commercial AI companies in the defense space. The final part outlines a number of policy recommendations for NATO to promote partnerships with the AI industry and to prevent the emergence of technology gaps and potential interoperability problems among Allies.

Literature Review

In the discipline of International Relations (IR) and Security Studies in particular, AI has entered the scholarly discourse only during the last decade and its current state reflects the still nascent policy discourse. Within this emerging literature, most scholars have focused, so far, on the necessity for and feasibility of arms control for AI-enabled military applications (Maas, 2019). Many of these works discuss arms control specifically with regard to lethal autonomous weapons systems (LAWS), which is also the most advanced debate on AI in foreign and security policy to date (Rosendorf, 2020; Rosert & Sauer, 2020; Asaro, 2012). Yet, there is also a growing literature discussing the potential implications of AI for strategic stability and the global balance of power (Horowitz, 2018; Garfinkel & Dafoe, 2019; Horowitz, 2019; Haas & Fischer, 2017).

Although the broader discourse on alliance politics is well established in IR literature, scholars have started only recently to examine AI through this lens. The few existing works examine a range of possible implications of emerging technologies for military alliances. However, in their analyses, the authors also point to the challenges arising from the lead of commercial companies in emerging technology domains. Daniel Fiott, for example, examined the potential implications of the US defense innovation strategy and the pursuit of emerging technologies for the transatlantic Alliance. In the article's conclusion, Fiott warns that "by utilizing emerging technologies from the commercial sector to achieve greater military power the US may further open up the technology gap within NATO" (2017). In a more recent contribution, Eric Lin-Greenberg outlined AI-specific challenges for decision-making among Allies and military operations conducted by multinational alliances. As one challenge the author highlighted that the lead of the private sector in AI and the distribution of AI resources could complicate burden-sharing among Allies in the future (2020).

These concerns are also mirrored in an increasing number of policy papers discussing the intersection of alliances and AI. For example, Andrew Imbrie and his co-authors outlined a roadmap for how the US can strengthen alliances and partnerships to promote a democratic way of AI. In the report, the authors argue that as most AI research and development takes place in the private sector or academia, "the US government will need to become a "fast follower" and ready-adopter of commercial innovations" (Imbrie et al., 2020: 27).

Andrea Gilli recently developed a set of strategies for NATO to lead in AI. In the paper, he also raised the question whether NATO is "agile enough" to leverage AI technologies developed by the commercial sector (Gilli, 2020).

Building on these previous works, this chapter zooms further into the challenge of public-private sector collaboration in the context of NATO. It seeks to contribute to the emerging literature and policy debate by identifying obstacles arising from the characteristics of the AI innovation ecosystem for NATO and analyzing how the militaries of selected member states have tried to overcome them, so far. Examining the members' strategies provides important clues about similarities and differences in Allies' approaches as well as the challenges they have faced. Such an assessment also lays the ground to formulate policy recommendations on how NATO can proactively shape public-private sector collaboration in AI across the Alliance.

The AI Innovation Ecosystem: Challenges for NATO

During the Cold War, government funding was the driving force behind the development of many cutting-edge dual-use technologies (Heinrich, 2002; Lécuyer, 2006). In 1960, US defense-related Research & Development (R&D) alone accounted for more than one-third of global R&D, and the government funded approximately twice as much R&D as US businesses (Sargent, Gallo and Schwartz, 2018: 3). However, over time, the vector of dual-use innovation shifted. In today's innovation ecosystem, spin-off effects often arise from technology companies that are primarily focused on civilian markets. Major technology firms including the likes of Google and Facebook reinvest significant parts of their revenue in R&D and rapidly introduce new products to the market (Missiroli, 2020). As few areas of high-technology are still unique to the military, defense organizations have to increasingly rely on commercial technology companies and engage with these actors more systematically (Sargent, Gallo and Schwartz, 2018; Missiroli, 2020).

The history of AI illustrates this shift particularly well. AI as a discipline has a history that dates back at least to the 1950s (Press, 2016). The US Department of Defense (DoD) has had an interest in AI since the 1960s, but it was especially pronounced during the 1980s. Starting in 1983, over a ten-year time period, the US government funded research into AI and advanced computing hardware as part of the so-called Strategic Computing Initiative. Notably, the DoD invested a total of USD 1 billion into the project with limited success (Roland & Shiman, 2002). Today, however, the defense apparatus trails commercial technology companies that are spearheading the development of AI. The leadership of the commercial sector is due to its advantage in different "ingredients" that are crucial for the development of AI including Big Data, hardware, and talent (Fischer & Wenger, 2019).

However, although the private sector is leading in AI, and many technologies developed for civilian uses have potential military applications, this does not necessarily imply that they can be easily transferred to the military realm. For example, commercial technology companies have their own profit-oriented objectives and may or may not be willing to collaborate with militaries for reasons including economic considerations (McMartin, 2020; see also Olney, 2019) or moral concerns (Statt, 2018). And even if companies are willing to collaborate, some commercial AI applications may not be directly transferable but must undergo significant modification prior to being functional for the military (Sayler, 2019). Moreover, for certain defense applications of AI, there may be no commercial business case, and military research organizations or traditional defense contractor shave to develop them. Thus, market incentives in the commercial space do not necessarily produce the optimal outcome for defense (Gilli, 2020: 65-67). In a nutshell, the objectives of

commercial technology companies and the original uses of certain AI applications and market incentives create challenges for NATO and its member states to develop robust AI capabilities.

Another characteristic of the AI innovation system that poses challenges to the transatlantic Alliance is the unequal geographic distribution of AI resources. Currently, the US is still leading in AI globally according to different metrics, and many of the most successful AI companies are American.[2] However, Chinese AI firms have emerged as the greatest competitors to US companies and "the West" is no longer the uncontested leader in science and technology (Rasser et al., 2019). Looking at US allies, the landscape is scattered. Some countries, including Canada, the United Kingdom and France have advanced technology sectors and invest increasingly into AI. However, while many states have stepped up their investments in AI, it is unlikely that some NATO members, especially in Southeastern Europe, will invest in developing a competitive industry or spend a meaningful amount of their defense budgets on AI in the foreseeable future (Lin-Greenberg, 2020). Thus, the AI innovation landscape is not only characterized by a lead of commercial actors, but also by an unequal distribution of resources across NATO member states.

In summary, the commercially-driven nature of the global AI innovation system, the geographic distribution of leading AI firms and resources, and investment priorities of member states create a number of challenges for NATO. For once, the militaries of member states may be unable to access commercial AI technologies because firms are either unwilling to collaborate or because they are simply unaware of opportunities in the defense domain. Moreover, the distribution of AI resources across member states bears the risk of dividing the Alliance into AI "haves" and "have nots" and to thereby increase the technology gap among NATO member states. As a result, in the future, some Allies may lack the AI capabilities to meaningfully contribute to NATO operations and it may become even more difficult to achieve interoperability (Lin-Greenberg, 2020). In the following paragraphs, this chapter investigates how the militaries of three NATO member states with advanced AI industries have adapted to the commercially driven AI innovation ecosystem, so far.

The State of Play: NATO and Public-Private Sector Collaboration on AI

Most NATO member states have only recently ramped up their focus on AI in the military domain. The following paragraphs will briefly review the state of collaboration on AI between commercial technology companies and militaries of the US, France and Germany. The selection of these countries is based on two considerations. First, although the US industry is leading in AI globally, also France and Germany have advanced civilian AI industries. Secondly, however, all three countries have different traditions when it comes to collaboration between the military and the civil sector. While this link has been traditionally close in the US,[3] there has been a much clearer division between the two spheres in Germany since the end of the Second World War (see e.g. Anderson & Townsed, 2018). France sits on the middle of the spectrum between the American and German cases. These characteristics raise the expectation that the Allies may adopt different approaches and face different challenges in collaborating with commercial AI companies.

[2] However, several of the leading US AI companies including Facebook, Google, IBM, and Microsoft conduct AI R&D in different locations around the world (see Heston & Zweetslot, 2020).

[3] However, the relationship between the US government and technology companies was negatively impacted by different events, including the revelations by Edward Snowden that the National Security Agency (NSA) had been intercepting data from several US businesses including Google and Facebook (see Hempel, 2015).

The United States

Among NATO members, the United States was the first to emphasize the importance of AI for the competitiveness of the American military in its third offset strategy. The strategy's main purpose, first formulated around 2014, was to maintain and strengthen the US long-held military technological advantage vis-à-vis rising great power competitors including China and Russia (Ellman, Samp and Coll, 2017). At the same time, it was acknowledged by the DoD's leadership that the commercial sector had become the driving force behind many strategically important technologies, requiring the DoD to rethink how it could identify and access innovation developed by private technology companies (Carter, 2015). The 2017 National Security Strategy and the DoD's military AI strategy from 2018 re-emphasize the importance of partnering with commercial technology companies including large industrial partners, small start-ups, and venture capital firms. The authors of the latter also formulated the goal to make it easier for the AI industry to partner with the DoD, for example by lowering administrative barriers (US DoD, 2018).

The objective to collaborate more closely with commercial actors on AI is also reflected in various organizational changes that the Pentagon initiated over the last few years. Already in 2015, then US Defense Secretary Ashton Carter established the Defense Innovation Unit Experimental (DIUx) – now Defense Innovation Unit (DIU), a Pentagon outpost situated in innovation centers including Silicon Valley, Boston and Austin. The aim of the DIU is to accelerate the adoption of leading commercial technology by the military, for example, by using innovative acquisition vehicles like Other Transaction Authorities (OTA). Although the DIU is focusing more broadly on different emerging technologies, AI and ML technologies feature prominently in the unit's portfolio.[4] Apart from DIU, different services have by now established their own programs with the objective to rapidly access commercial technologies for military capabilities, among other things. These include AFWERX (Air Force), SOFWERX (Special Operations Command) and NavalX (Navy).

Moreover, in 2018, the DoD established the Joint Artificial Intelligence Center (JAIC) with the overarching aim to accelerate the delivery of AI-enabled capabilities, scale the impact of AI tools, and synchronize the Department's AI efforts. One of the JAIC's tasks is to evolve partnerships with commercial technology companies and other relevant actors (Leung & Fischer, 2018). The Pentagon is also collaborating with commercial AI actors via other avenues. For example, DARPA develops together with a number of startups the so-called OFFSET program, which has the aim of "using swarms comprising upwards of 250 unmanned aircraft systems (UAS) and/or unmanned ground systems (UGS) to accomplish diverse missions in complex urban environments" (Chung).

However, the US also faced drawbacks in its efforts to establish a closer collaboration with commercial technology companies due to economic, ethical and legal reasons. For example, former Secretary of Defense Carter had to 'reboot' the DIU shortly after it was established, as companies did not see a viable business opportunity in contracting with it. Only after the DIU's contracting procedure was adapted during an overhaul period of the organization, it began to successfully establish partnerships with technology companies (Hempel, 2015). Moreover, the US technology firm Google decided not to renew a contract with the Pentagon on Project Maven – an Air Force initiative aimed at automating the analysis of video footage gathered by drones – after an outcry of its employees due to ethical concerns with the project (Statt, 2018).[5] Lastly, the Pentagon has also faced legal challenges when awarding contracts to commercial technology

[4] Analysts have also advocated to take DIU global for the US to harness innovation more actively abroad and allow Allies to benefit from DIU in turn (see Kliman & Thomas-Noone, 2018).

[5] However, recent research by the Center for Security and Emerging Technology found that the majority of AI researchers is not principally opposed to working on defense projects (see Aiken, Kagan and Page, 2020).

companies, which have slowed project timelines. The most recent example is the awarding of the cloud infrastructure contract JEDI to Microsoft, which was challenged by its competitor Amazon (Macias, 2020)

France

France is the European country which has most openly addressed the opportunities and challenges related to AI-enabled military applications beyond the debate on autonomous weapons systems (Franke, 2019). The French AI strategy features a separate section on defense, highlighting the need for close collaboration between the public and the private sector. Like the United States, France also published a separate military AI strategy in 2019. The latter addresses the issue of public-private sector collaboration in different ways. On the one hand, the document emphasizes again the need to strengthen partnerships with commercial AI companies. However, it also refers to the geography of AI resources and the dominance of American and Chinese companies, stressing the risk of a French dependency on foreign AI firms and underscoring the need to "preserve a heart of sovereignty" (Ministère des Armées, 2019).

The French Ministry of Defense has also started to make organizational changes, aimed at enabling closer collaboration with commercial technology companies for military purposes. For example, similar to the US DIU, the French Defense Ministry has established the Innovation Défense Lab, with the aim to accelerate the experimentation, prototyping and deployment of innovation, including technology coming from commercial companies. (Ministère des Armées, 2020). While not much is known about the work of the Lab yet, it can be expected that enabling collaboration with AI companies is of particular interest to the unit, given the French government's and the Ministry's broader AI efforts.

Germany

Although Germany has an advanced civilian AI industry and a national AI strategy, it lags behind the US and France when it comes to strategic thinking concerning defense-related AI and investments (Tonin, 2019; Franke, 2019). Although the German military is already working on certain projects with AI components (see e.g. Airbus, 2020), Berlin has no military AI strategy and also its national AI strategy from 2018 does not mention the defense domain. The German Ministry of Defense made only a brief mention of AI and the need to generally seek closer collaboration between the armed forces, "startups and the entire digital economy" in its 2016 Defense White Paper (Die Bundesregierung, 2016).

Notably, in 2019, the Army's Concepts and Capabilities Development Center (Amt für Heeresentwicklung), which is subordinated to the Army Headquarters, published a Position Paper on AI in land forces. In the Paper, the authors do not only explore potential areas of action for AI development in the military, but also point to the dual-use character of AI and the necessity to collaborate with German and European industrial players and research institutes (Bundeswehr, 2019). Furthermore, the authors recommend that the Bundeswehr set up, for example, an AI Development Center, and an AI Data Center, among other initiatives. Yet, it seems as if these recommendations have not been taken up by the Ministry of Defense, so far (Bundeswehr, 2019).

However, already in 2017, the German Ministry of Defense created a novel unit, the Cyber Innovation Hub, which among other tasks focuses on establishing partnerships with commercial technology companies to leverage external innovation for the military (Weizenegger & Khadjavi, 2020: 42-45). Although the Innovation Hub does not focus solely on AI, it is particularly relevant in a NATO context as the Hub has also been serving

as a platform to collaborate with similar units in other countries. The Cyber Innovation Hub has, for example, hosted innovation challenges together with the NATO ACT Innovation Hub and the US innovation units SOFWERX and AFWERX (Capital Factory, 2018). Despite the historic separation between commercial technology development and defense in Germany, there is little publicly known about the obstacles that the Cyber Innovation Hub has faced in attracting collaborations with startups or other private players.

Discussion and Policy Recommendations

The initiatives of the previously examined NATO member states to adopt AI technologies from the commercial sector form part of broader efforts to leverage emerging technologies for military purposes. All three countries have expressed the need to partner with commercial technology companies to this end. While the United States is already slightly more advanced in this regard, also France and Germany have created organizational units that are tasked with partnering with commercial technology companies. Notably, the approaches that the states have adopted to collaborate more effectively with commercial actors look similar and seek to mimic the business practices of the private sector. Moreover, some of these new organizational units have already established ties across countries and have collaborated on selected projects.

However, the brief review of states' strategies has also revealed some obstacles. For example, the US' military has faced a number of economic, legal and ethical challenges associated with the collaboration of commercial technology companies. Moreover, in its military AI strategy France has stressed the challenge of an unequal distribution of AI resources, that could create dependencies on other countries and foreign companies. While the US and France have developed separate military AI strategies, Germany lacks a strategic approach to AI development for military purposes, so far.

Considering that NATO and its member states are all still at a relatively early stage in the development and adoption of AI for military purposes, the Alliance has a window of opportunity to proactively shape public-private sector collaboration. Recent activities of NATO representatives and NATO publications reflect the need to do so. For example, in September 2020, NATO Deputy Secretary General Mircea Geoană spoke at the HumanAIze forum on AI and public-private sector collaboration and underscored that NATO needs to engage more systematically with commercial AI firms (Geoană, 2020; see also The Reflection Group, 2020). The remainder of this chapter outlines four policy recommendations for how NATO can facilitate public-private sector collaboration in AI.

First, NATO should develop a NATO-AI Industry Partnership loosely modeled on the NATO Industry Cyber Partnership. Such a partnership on AI could serve as a key information exchange mechanism between member states and AI companies on issues including novel advances in AI development, investment gaps in technology domains relevant to the Alliance but also on governance issues arising from technical risks and ethical concerns regarding AI technologies. Considering the previous experiences of the NATO-Industry Forum, NATO Allied Command Transformation (ACT) could be an important catalyst for such an initiative.

Second, NATO should foster an exchange of personnel between selected NATO bodies and AI companies. Such an exchange could help to increase institutional knowledge about the AI innovation landscape and business practices of AI companies. Participating NATO bodies should also appoint 'bridge builders' that have a good understanding of both the military and commercial sector, and could take the lead on the implementation of selected NATO AI projects.

Third, NATO should promote regular exchanges and collaborative projects between the innovation units of different member states and encourage them to leverage the AI ecosystem across the alliance. The NATO ACT Innovation Hub could play a key role at fostering this exchange. NATO ACT could also encourage member states that do not yet have institutional mechanisms to collaborate with the private sector to consider establishing them.

Lastly, and related to the previous point, NATO should support the introduction of innovative acquisition tools that make it economically viable and attractive for technology companies to collaborate with militaries. Given the fast-moving nature of the AI innovation ecosystems and business practices of commercial technology companies, NATO Allies need to break down some bureaucratic barriers that still hinder public-private sector collaboration.

References

Aiken, Catherine Rebecca Kagan and Michael Page (2020). "'Cool Projects' or 'Expanding the Efficiency of the Murderous American War Machine?' AI Professionals' Views on Working With the Department of Defense". In Center for Security and Emerging Technology, CSET Issue Brief.

Airbus (2020). "Future Combat Air System: Owning the sky with the Next Generation Weapons System".

Anderson, Wendy R. & Jim Townsed (2018). "As AI Begins to Reshape Defense, Here's How Europe Can Keep Up". In Defense One.

Asaro, Peter (2012). "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making." In International Review of the Red Cross, Vol. 94, No, 886.

Bundeswehr (2019). "Künstliche Intelligenz in den Landstreitkräften: Ein Positionspapier des Amts für Heeresentwicklung".

Capital Factory (2018). "Defense Innovation // Startup Recon Mission // Cyber Innovation Hub".

Carter, Ashton B. (2015). "Drell Lecture: 'Rewiring the Pentagon: Charting a New Path on Innovation and Cyber'". In US Department of Defence, Speech.

Chung, Timothy. "OFFensive Swarm-Enabled Tactics (OFFSET)". In Defense Advanced Research Project Agency.

Die Bundesregierung (2016). "Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr".

Ellman, Jesse Lisa Samp and Gabriel Coll (2017). "Assessing the Third Offset Strategy". In Center for Strategic and International Studies, Report.

Fiott, Daniel (2017). "A Revolution Too Far? U.S. Defence Innovation, Europe and NATO's Military-Technological Gap". In Journal of Strategic Studies, Vol. 40, No. 3, pp. 417-437.

Fischer, Sophie-Charlotte & Andreas Wenger (2019). "A Politically Neutral Hub for Basic AI Research". In Center for Security Studies, CSS Policy Perspective.

Franke, Ulrike Esther (2019). "Not smart enough: The poverty of European military thinking on artificial intelligence". In European Council on Foreign Relations, Policy Brief.

Garfinkel, Ben & Allan Dafoe (2019). “How does the offense-defense balance scale?”. In Journal of Strategic Studies, Vol. 42, No. 6, pp. 736-763.

Geoană, Mircea (2020). “Speech by NATO Deputy Secretary General Mircea Geoană on NATO and innovation at HumanAIze, an online forum on Artificial Intelligence and public-private sector collaboration”. In NATO.

Gilli, Andrea (2019). “Preparing for “NATO-mation”: the Atlantic Alliance toward the age of artificial intelligence”. In NATO Defence College, NDC Policy Brief No. 4.

Gilli, Andrea (2020). “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence”. In NATO Defence College, NDC Research Paper No. 15.

Haas, Michael C. & Sophie-Charlotte Fischer (2017). “The evolution of targetedkilling practices: Autonomous weapons, future conflict, and the international order”. In Contemporary Security Policy, Vol. 38, No. 2, pp. 281-306.

Heinrich, Thomas (2002). “Cold War Armory: Military Contracting in Silicon Valley”. In Enterprise & Society, Vol.3, pp. 247–284.

Hempel, Jessi (2015). “DOD Head Ashton Carter Enlists Silicon Valley to Transform the Military”. In Wired.

Heston, Roxanne & Remco Zweetslot (2020). “Mapping U.S. Multinationals’ Global AI R&D Activity.” In Center for Security and Emerging Technology, CSET Issue Brief.

Horowitz, Michael C. (2018). “Artificial Intelligence, International Competition and the Balance of Power”. In Texas National Security Review, Vol. 1, No. 3, pp. 36-57.

Horowitz, Michael C. (2019). “When speed kills: Lethal autonomous weapon systems, deterrence and stability”. In Journal of Strategic Studies, Vol. 42, No. 6, pp. 764-788.

Imbrie, Andrew et al. (2020). “Agile Alliances: How the United States Can Deliber a Democratic Way of AI”. In Center for Security and Emerging Technology, Analysis.

Lécuyer, Christoph (2006). Making Silicon Valley: Innovation and Growth of High Tech, 1930-1970. Cambridge, MA: MIT Press.

Kliman, Daniel & Brendan Thomas-Noone (2018). “Now is the time to take DIUx global”. In Defense News.

Leung, Jade & Sophie-Charlotte Fischer (2018). “JAIC: Pentagon debuts artificial intelligence hub. Bulletin of the Atomic Scientists”.

Lin-Greenberg, Eric (2020). “Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making”. In Texas National Security Review, Vol. 3, No. 2, pp. 56-76.

Maas, Matthijs (2019). “How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons”. In Contemporary Security Policy, Vol. 40, No. 3, pp. 285-311.

Macias, Amanda (2020). “Pentagon says it will stick with Microsoft for $10 billion JEDI cloud contract”. In CNBC.

McMartin, Ben (2020). “Don’t Underestimate the Cost of Selling to the Federal Government”. In Public Spend Forum.

Ministère des Armées (2019). “Artificial Intelligence in Support of Defense”.

Ministère des Armées (2020). “Innovation Défense Lab”.

Missiroli, Antonio (2020). “Game of drones? How new technologies affect deterrence, defence and security”. In NATO Review.

NATO (2020). “Cooperation on Artificial Intelligence will boost security and prosperity on both sides of the Atlantic, NATO Deputy Secretary General says”.

NATO Science & Technology Organization (2020). “Science & Technology Trends 2020-2040: Exploring the S&T Edge”.

Olney, Rachel (2019). “The Rift between Silicon Valley and the Pentagon is Economic, not moral”. In War on the Rocks.

Press, Gil (2016). “Artificial Intelligence Defined As A New Research Discipline: This Week In Tech History”. In Forbes.

Rasser, Martijn et al. (2019). The American AI industry: a blueprint. Washington DC: Center for a New American Security.

Roland, Alex & Philip Shiman (2002). Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993. Cambridge, MA: The MIT Press.

Rosendorf, Ondřej (2020). “Predictors of support for a ban on killer robots: Preventive arms control as an anticipatory response to military innovation”. In Contemporary Security Policy, Vol. 42, No. 1, pp. 30-52.

Rosert, Elvira & Frank Sauer (2020). “How (not) to stop killer robots: A comparative analysis of humanitarian disarmament campaign strategies”. In Contemporary Security Policy, Vol. 42, No. 1, pp. 4-29.

Salisbury, Emma (2020). “A Cautionary Tale on Ambitious Feats of AI: The Strategic Computing Program”. In War on the Rocks.

Sargent, Josh F. Jr., Marcy E. Gallo and Moshe Schwartz (2018). “The Global Research and Development Landscape and Implications for the Department of Defense”. In Congressional Research Service, Report R45403.

Sayler, Kelley M. (2020). Artificial Intelligence and National Security. Washington, DC: Congressional Research Service.

Scharre, Paul (2020). “The Militarization of Artificial Intelligence”. In Texas National Security Review.

Statt, Nick (2018). “Google reportedly leaving Project Maven military AI program after 2019.” In The Verge.

The Reflection Group (2020). “NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General”.

Tonin, Matej (2019). “Artificial Intelligence: Implications for NATO’s Armed Forces”. In NATO Parliamentary Assembly, Science and Technology Committee, Sub-Committee on Technology Trends and Security.

US DoD (United States Department of Defense) (2018). “Summary of the 2018 Department of Defense Artificial Intelligence Strategy”.

Weizenegger, Sven & Stephanie Khadjavi (2020). “Bundeswehr Cyber Innovation Hub”. In European Security & Defence.

THE NATO ALLIANCE AND THE CHALLENGES OF ARTIFICIAL INTELLIGENCE ADOPTION

Edward Hunter Christie - NATO, Vrije Universiteit Brussel, Wilfried Martens Centre for European Studies

Abstract

This chapter adds to existing literature on how Artificial Intelligence (AI) may affect political-military decision-making in the context of an alliance, by focusing on selected technology adoption challenges. Existing analyses tend to focus on issues that derive from assuming a future state in which AI is already in place, such as compressed tactical decision-making cycles, risks to interoperability due to different future levels of technological adoption, or the need for international norms to limit the development and use of lethal autonomous weapon systems. While those considerations are fully justified, this chapter places its focus on identifiable shorter-term challenges relating to the practical adoption of AI. Four areas are discussed: iterative development, access to human capital, access to data, and engagement with civilian-oriented technology institutions. Each of these areas poses potential challenges to collective decision-making and policy coordination for NATO Allies.

Introduction

AI consists in the ability of machines to perform tasks that typically require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems (Reding & Eaton, 2020).

From a military perspective, the battlefield of the future will undoubtedly feature a greater use of, and reliance on, Artificial Intelligence (AI). The range of potential applications is at least as vast as the current range of tasks that require human cognition, e.g. analyzing and classifying visual data, organizing logistics, operating support vehicles, or tracking and engaging hostile targets.

The prospect of widespread adoption of such capabilities has led to questions regarding traditional political-military decision-making in an alliance context such as NATO. Many existing analyses focus on issues that derive from assuming a future state in which AI is already in place, such as compressed tactical decision-making cycles, risks to interoperability due to different future levels of technological adoption, or the need for international norms to limit the development and use of lethal autonomous weapon systems (LAWS). While those considerations are entirely valid, this chapter places its focus on identifiable shorter-term challenges relating to the practical adoption of AI. Indeed, the journey towards a deep and systemic adoption of AI-enhanced capabilities may prove far more challenging, complex, and disruptive, than what that journey's assumed destination may suggest at first sight. Four areas are discussed: iterative development, access to human capital, access to data, and civilian-oriented technology institutions. Progress in each of these four areas is essential to ensure successful practical adoption of AI, whether in national defense institutions or at the NATO level.

Some initial observations can be made to justify the selection of these four areas. First, the manner in which AI solutions are developed is far more dynamic and iterative than traditional military capability development. This raises a series of tensions with respect to existing approval processes, which place a premium on predictability and control. Second, although AI is intuitively associated with the prospect of job displacements, the first necessary step to adopt AI is to hire more people, namely technical experts, in relatively large numbers. Given massive demand for such skills, defense establishments have to ensure they are sufficiently attractive employers, but they often lack the flexible budgets and hiring practices to do so. Third, access to data is essential for AI model training, leading to complex questions regarding data governance and the coordination of national policies and practices in that area, including but not limited to linkages with the EU's General Data Protection Regulation (GDPR). Fourth, contrary to what is the case for armaments technologies, the technological cutting-edge in AI is largely in the hands of civilian-oriented commercial and research entities, raising the question of how to engage more deeply with such entities.

The rest of this chapter is structured as follows. The first section contains a short review of recent analyses and commentary on the likely impacts of AI in the NATO context, followed by the main arguments for the chapter's focus on adoption challenges. The subsequent four sections address each of the four challenge areas identified above, namely iterative development, access to human capital, access to data, and engagement with civilian-oriented technology organizations.

How AI Might Challenge NATO

Any significant change that affects Allies in an asymmetrical manner, whether related to the international security environment or to domestic conditions, raises the question of the Alliance's continued ability to act collectively for its common defense. Interoperability is at the heart of such considerations. As noted by Dufour, interoperability includes "technical features permitting systems to physically connect to one another and exchange information and the alignment of procedures and processes to allow military personnel to function within the same space and achieve common goals" (2018). The rise of AI is a clear case of an asymmetrical technological shift as far as Allied armed forces are concerned – with the United States strongly in the lead and with significant differences among European Allies as well. Several authors have expressed concerns regarding risks to interoperability from these developments (see e.g. Dufour, 2018; Lin-Greenberg, 2020).

In parallel, the very nature of AI will challenge decision-making in matters of deterrence and defense. This includes issues such as compressed tactical decision-making and other potential new risks in terms of escalation dynamics (see e.g. Schaus & Johnson, 2018; Wong et al., 2020). For example, one could imagine sets of autonomous weapon systems from opposite sides confronting one another and taking tactical decisions at speeds that humans could barely comprehend. Such reflections are theoretical at this time, given the actual level of technological attainment. However, if carefully carried out, they can point to valid questions for defense and security policy.

In fact, one may argue that reflections of this nature are already guiding the security policy positions of certain states. From first principles, one may deduce that this is the case in the following manner. Let us assume that states predict a future level of technological attainment, such that most tactical military activities could rely on AI without human involvement. This assumption may lead major powers into an arms race dynamic, with each major power fearing that the others will soon achieve considerably faster tactical decision-making cycles. As AI matures and becomes more widely adopted, one could also expect a partial

crowding out of human constraints within each power's armed forces, lest potential adversaries gain a potential military advantage through the pursuit of a maximalist adoption strategy. As a result, a race to the top might unfold, towards extensive adoption and integration of autonomous functions and systems. Similarly, Altmann and Sauer argue that "current expectations regarding future armed conflict (and the need for speed)" provide an incentive for the adoption by competing powers of autonomous weapon systems (2017). Anticipating such developments, states with a relatively lower potential to develop these capabilities would be expected to call for international agreements to restrict their use, while leading powers may be expected to adopt less restrictive positions. Given that such a distribution of national positions has emerged in the context of the consultations of the United Nations Group of Governmental Experts on Lethal Autonomous Weapons Systems (see e.g. CRS, 2020), one may conclude that something akin to the aforementioned assumption has been internalized by the relevant state parties.

While high-level conceptual policy work on the regulation of future autonomous systems is important and by no means trivial, one may argue that it is conceptually more straightforward than the actual, mid-term road ahead that Allies are beginning to engage upon, as they transition from currently available military capabilities towards greater adoption of AI. Indeed, the reasoning above did not address how AI will need to be developed, and then integrated with human operators, their equipment, and their chains of command. While narrowly-defined tactical use cases would seem evidently attractive for fully autonomous capabilities, actual combat missions will likely retain a degree of complexity and surprise that will warrant continued human supervision and control, even at the tactical level. As military practitioners often note, effective human-machine teaming will likely remain the main priority, and the greatest challenge, as armed forces adopt AI. This would not be primarily because of national and international norms that would call for retaining human control, though this would also be a factor, but rather because unmanned systems with autonomous functions might not be able to cope, unsupervised, with the full range of conceivable real-life conditions. As a result, military operators and commanders would not be willing to entrust these systems with certain tasks.

A second set of issues relates to machine-machine teaming – or collaborative robotics – as more versatile systems will need to exchange information and data with each other and pursue effective team behaviors. A related third set of issues concerns the architectures needed to cope with a mix of multiple and heterogenous human and machine agents. To generate these future capabilities, considerable work will be needed in the area of capability development, including Testing, Experimentation, Validation, and Verification (TEVV) and standardization. In order for Allies and NATO to successfully tackle these sets of issues, they will in any case have to address the essential enabling factors that allow for AI to be adopted to begin with, corresponding to the adoption challenges that were identified in the introduction.

Challenge 1: Iterative Development

Major defense acquisitions are often associated with long development cycles, long lead times, and frequent delays and cost overruns. As timelines are long, successive technological advances tend to be batched together into successive generations of types of platforms in the various operational domains. This can have certain advantages, as capability development communities have ample time to conduct thorough TEVV against stable requirements, standards, and technologies, and as armed forces have ample time to conduct exercises and process 'lessons learned' from exercises and deployments back into the decision-making cycle.

This slow-moving pattern of generational shifts is challenged by the far more rapid pace of innovation that occurs with software development and use. AI will prove more challenging still.

From a project management perspective, traditional development generally follows a 'Waterfall model', whereas the dominant contemporary trend in software development is typically referred to as an 'Agile model'. Waterfall development is a linear process, where each step is completed before moving on to the next step. It is typically a slow-moving process that puts a premium on stability and long-term predictability. An Agile approach, by contrast, allows for development steps to be revisited and adjusted multiple times. Timelines are considerably shorter, and development is much more iterative, based on rapid and repeated testing and revisions. General problem statements are used, rather than rigid statements of requirements at the beginning of the process. Products are placed in the hands of users before they are mature: updates and upgrades are sent along later, as new needs emerge, indeed repeatedly so over time. Also, Agile development thrives on having much closer and more dynamic interactions between end users and developers. In the software industry, the recent trend is to combine Agile development with operations, which is referred to as 'Development Operations' (DevOps) (see e.g. Kim, Humble, Debois & Willis, 2016). The practice of building in relevant security aspects throughout the development and operations process is encapsulated in an additional expression: 'Development Security Operations' (DevSecOps) (see e.g. Morales et al., 2020, for a guide to DevSecOps for highly regulated environments such as defense).

In addition to the demands of Agile software development, AI also requires integrating the training datasets according to efficient, automated approaches that ensure quality control. In industry, that latter set of activities may be referred to as 'Data Operations' (DataOps) (see e.g. Valentine & Merchan, 2018; Atwal, 2020). In sum, contemporary thinking about best practice in AI and Machine Learning (ML) development and use can be portrayed as a search for the best insights from DevOps, DevSecOps, DataOps, as well as older concepts from Design Thinking (see e.g. Hechler, Oberhofer & Schaeck, 2020). These reflections have led to the emergence of the terms 'Artificial Intelligence for IT Operations' (AIOps) and 'Machine Learning Operations' (MLOps). While organizations of all kinds continue to learn from experience and refine their approaches, the general ingredients that are repeatedly raised revolve around non-linear, rapid, highly iterative development and deployment processes, often with multiple feedback instances from end users, and supported by automated data processes.

To rise to the challenge, organizations need to be able to source and manage all key resources in a flexible manner. This encompasses people, data, computing and storage capacities, and testing and experimentation facilities. With respect to people, ML model builders need to have seamless access to data professionals as well as to end users. Unless a defense organization has all the necessary staff in-house, that will mean a need for contractors with security clearances and easy access to the relevant premises, systems, data, and people. Managerial practices and attitudes within organizations need to allow for these activities. In terms of formal arrangements, regulations, and governance, a range of tensions may arise between traditional institutional set-ups and those required for an era of Agile development.

Allied defense establishments face a structural challenge, as their software-intensive activities already seek to integrate the practices described above, while other activities largely do not. Within the NATO Enterprise, staff from the NATO Communications and Information Agency (NCIA) and from the Innovation Hub at the Allied Command Transformation (ACT) already pursue Agile approaches. In many other parts of the Enterprise, these concepts are unfamiliar or unknown.

From an organizational perspective, this leads to two broad questions. One is how and to what extent Agile models should be brought into the development of physical systems, including major military platforms. The second is how and to what extent Agile approaches need to apply to overarching organizational functions, such as planning, budgeting, financing, procurement, and human resources management. There are no definitive answers to these questions. Allies and NATO need to move forward, experiment, learn, and revise their approaches and procedures over time, based on experience, as the development and use of AI generates new lessons and insights. However, senior-level awareness and support are essential to ensure that the most cutting-edge thinking and experience from specialist communities are allowed to develop, grow, and disseminate to a broader audience.

Challenge 2: Human Talent and Skills

AI development requires relatively large teams of experts with complementary sets of skills, first and foremost across relevant sub-fields of computer science, mathematics, neuroscience, and robotics. A further, even broader set of skills is required to support development, adoption, integration, use, and feedback processes back into development, as a wide range of real-life phenomena and areas of human cognition are to be modelled through AI. Also, the implications of AI for senior-level decision-making need to be understood.

One may conceive of three lines of effort to address these challenges. First, there is a need to develop, hire, and retain large numbers of cutting-edge technical experts. Second, there is a need to convert a number of professionals with other specialist backgrounds into competent supporters, facilitators, users, and trouble-shooters of AI. This second category covers a broad range, e.g. project and program managers, intelligence analysts, logistics managers, legal advisors. Third, there is a need to educate and sensitize senior decision-makers with the implications that AI may bring to their decision-making responsibilities. This includes both new governance responsibilities directly related to AI and data, as well as broader impacts on traditional areas of operational, strategic, and political decision-making.

A first, low-cost step that can support the second and third lines of effort is the production and use of educational materials for non-technical audiences in Allied defense institutions. National examples include the Defence Science and Technology Laboratory (DSTL) in 2019 and the Joint Artificial Intelligence Center (JAIC) in 2020, respectively in the UK and the US. At NATO, a broader educational effort addressing eight emerging and disruptive technologies – including Big Data Analytics (BDA), AI, and Autonomy – was published in April 2020 (Reding & Eaton, 2020).

More systematic and comprehensive educational programs or strategies can also be pursued. In the United States, pursuant to Section 256 of the Defense Authorization Act for Fiscal Year 2020 (US Congress, 2019), the Secretary of Defense is tasked with the development of “a strategy for educating service members in relevant occupational fields on matters relating to artificial intelligence”.

The first line of effort – developing, hiring, and retaining technical staff – requires ambition, ample funding, and reforms to human resources regulations currently in force in typical defense institutions. Administrative barriers lead to slow and inflexible hiring and contractual practices, including on tenure, salary and mobility within hiring organizations (i.e. across administrative units and bodies), and between hiring organizations and entities of interest in the broader AI ecosystem, such as universities, research laboratories, private

industry, other relevant national state institutions, and the national defense institutions of fellow Allies and partner nations.

Challenge 3: Data as a Strategic Resource

Defense establishments are subject to the phenomenon of Big Data, as opportunities for data collection multiply with rising connectivity and the integration of more sensors, and of qualitatively better sensors, into equipment of all kinds. Big Data's defining features – volume, variety, velocity – rapidly overwhelm any organization that has not put in place best-practice data pipelines that allow for the automated processing of these vast data flows. Under current conditions, valuable opportunities for analysis are missed, as there is a mismatch between the supply of data, and the ability of defense establishments to process it (see e.g. Zelaya & Keeley, 2020).

US and UK data strategy documents (US DoD, 2020; UK MoD, 2020), lay out similar visions and intents in favor of becoming "data-centric" (US) or "data-driven" (UK) and of viewing data as a "strategic asset" (both). In the US case, a set of goals are outlined, namely that DoD data should be visible, accessible, understandable, linked, trustworthy, interoperable, and secure. In the UK case, strategic objectives refer to availability, accessibility, good governance, quality, consistent and coherent use, integrity and security, having a relevant skills base, and exploitable for new data-driven technologies. For illustration, the US visibility goal includes, among others, objectives relating to data being (internally) advertised, catalogued, and discoverable through common (internal) platforms and search tools. The UK objective regarding availability and accessibility also refers to a greater use of common internal systems, based on a "manage once, use many times" principle.

In the NATO context, subject to Allied confirmation, a NATO Data Exploitation Framework Policy will be developed in the course of 2021 (NSCAI, 2020). In that context, the question of data sharing, among Allies and between Allies and the NATO Enterprise, is an important policy challenge that warrants further attention. The National Security Commission on Artificial Intelligence (NSCAI) calls for the development of coordinated data sharing practices, to be supported by new privacy-preserving AI and ML technologies (2020). In this context, it is important to note that defense and security are outside of the scope of application of the European Union's General Data Protection Regulation (GDPR). However, some Allies that are also member states of the European Union (EU) have adopted national legislation that extends the scope of parts or all of the GDPR to defense. In sum, European Allies present a complex patchwork of legislation and practices concerning data protection and data privacy in the field of defense. Several approaches may be considered to facilitate data sharing in spite of differences in national legislation and practices. One possibility could be to encourage Allied governments to make a common political commitment towards certain well-defined data sharing facilitation goals. Each Ally would then be responsible for adjusting its national provisions to ensure that the facilitation goals are met. A second approach is to pursue the NSCAI's recommendation to seek technological solutions that could, in some way, enable the sharing of data without compromising data privacy and protection obligations. A further insight is that national institutions and NATO bodies could pursue the exchange of successive versions of data-trained algorithms, rather than exchanging the data itself.[1] As it is not possible to deduct the contents of a training data-set that contains multiple observations from a comparison of the pre-training and post-training algorithms, data could in principle be exploited for model development purposes without needing to be shared at all. In practice, a process of this nature would

[1] The author is indebted to Mark Shiffer, Director of Engineering at Redhorse Corporation, for this insight.

require very tightly managed procedures, and it remains the case that full access to all datasets will more easily support consistency in important processes such as data cleaning and documentation. Nevertheless, the notion of 'model sharing' should be included in future discussions on multinational data sharing challenges.

Challenge 4: Engagement with Non-Defense Technology Actors

A fundamental set of questions arises with respect to the adoption of capabilities in BDA, AI, Autonomy and Robotics, and related fields. These areas of activity are not merely dual-use: they are civilian-dominated, in terms of R&D expenditures, and in terms of revenue shares. As a result, there is a strong case for Allies and NATO to expand, deepen, and streamline their channels of commercial engagement with non-defense technology companies, big and small, as they may hold much needed cutting-edge technologies. This is not limited to mere procurement of specific products and services. There is also a case for crosscutting government policies to foster innovation in these technology areas, as part of a broader, whole-of-government drive to remain competitive and maintain the technological edge of the West, both economically and militarily. In that same context, Allies are concerned about the rising challenge from certain non-Western powers, which includes heightened intellectual property acquisition, through both licit means (such as corporate mergers and acquisitions and academic mobility programs) and illicit means (such as espionage). A sound public policy response to these challenges may follow two tracks: defensive mechanisms, and proactive mechanisms.

Defensive mechanisms include national legislation, regulation, and institutional efforts to place calibrated restrictions on exports of technologies, on Foreign Direct Investment (FDI), and on access to certain areas of industrial and academic activity. Such efforts will, due to their nature, be pursued overwhelmingly at the national level, though some coordination and exchange of good practices may be useful in relevant bilateral and multilateral formats. For example, Allies that are members of the EU are subject to Regulation (EU) 2019/452 that establishes a framework for the screening of FDIs. In the United States, the US Treasury Department's Committee on Foreign Investment in the United States (CFIUS) has seen its role strengthened by the entry into force of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which "expands the scope of transactions reviewable by CFIUS to address more effectively current national security concerns" (US Treasury, 2018).

Proactive mechanisms include programs to channel state investments as well as greater private investment, from trusted sources, into Allied innovation ecosystems. A range of mechanisms may be deployed in support of these goals. Existing mechanisms cover interrelated ranges in terms of financial scale, time horizons, and depth of guidance offered to potential private sector recipients.

The most basic mechanism, with the smallest financial pay-outs to individual recipients, is innovation challenges organized by general-purpose defense and security agencies. A national defense body or a NATO body, whose mission is not limited to promoting innovation, issues a public call, inviting private companies and entrepreneurs, usually with certain nationality restrictions, to propose a solution to a particular technological challenge. The winning bid or bids are rewarded with greater visibility and recognition on the part of the relevant official body, formal and informal contacts with defense officials, and other small rewards, which may or may not include an actual financial pay-out. For Allied institutions, a step forward is made in addressing a particular need at a very low financial cost, partly thanks to the expected future value of becoming a supplier for the institution, and partly thanks to the intangible brand value of NATO, or of the

relevant national entity. In the case of the NATO Enterprise, innovation challenges are held by the ACT (NATO Innovation Challenge) and the NCIA (NCI Agency Defence Innovation Challenge).

A more developed and systematic approach is defense innovation accelerators, for example the United Kingdom's Defence and Security Accelerator (DASA) which aims to "find and fund exploitable innovation to support UK defence and security quickly and effectively, and support UK prosperity" (DASA, 2019). Defense innovation accelerators are distinct agencies that specialize in the use of support measures for potentially promising innovators, notably but not exclusively through the use of competitive award mechanisms, including innovation challenges. The clearer role and mandate of accelerators enables the constitution of a wide portfolio of funding projects, leading to much more detailed insights about available innovation potential, and to gains from experience in running multiple competitive calls. Nevertheless, individual financial pay-outs remain modest by the standards of defense equipment procurement. In the case of DASA, for financial year 2018/2019, a total of GBP 36.8 million was allocated to 226 winning proposals (DASA, 2019). This implies an average pay-out of approximately GBP 163,000 (about EUR 180,000) per winning proposal.

On a larger financial scale, state-sponsored venture capital mechanisms are also being deployed to foster innovation, with a notable focus on start-up companies. A long-standing example is In-Q-Tel, which was originally set up by the Central Intelligence Agency (CIA). As noted by Mahoney, this development grew out of "a recognition within the American defence community that the United States government was no longer a central actor in technological R&D" (2020). Contrary to ordinary venture capital, which is profit-oriented, In-Q-Tel aims to incentivize an inflection in a recipient company's R&D and product development trajectory, such that it becomes a potential future supplier of products and services for defense and security agencies (though, very importantly, not necessarily exclusively so). With the In-Q-Tel model, relationships with recipients have comparatively long-time horizons.

An emerging attempt to combine proactive support mechanisms with defensive policy goals is the US Department of Defense (DoD)'s Trusted Capital Marketplace initiative. Ellen Lord, US Undersecretary of Defense for Acquisition and Sustainment, described the initiative as a mechanism to "strengthen the defense supply chain and deny adversarial access [by fostering investment deals] between companies building technologies critical to the defense sector and trusted capital providers" (2020). The reasoning here is to generate a boundary between trusted and non-trusted investors, based on US government screening of prospective investors for potential national security risks. Once investors are deemed secure, they enter the scheme and are able to offer venture capital to innovators. By implication, potentially interested investors that do not pose a potential security risk but that are interested in such investments will self-select into applying for the scheme, pass the screening procedures, and the set of trusted investors will grow. Investors with undesirable entanglements with rival powers will be kept out unless they divest from such entanglements. Ideally, this would lead to three incentivizing effects: one, provided the defense and security innovation market is large enough, the profit motive will drive many investors to make the desired switch; two, investors will be drawn in by the US government's appeal to their sense of patriotism; and three, peer pressure will build on undecided investors if a critical mass of US investors make the desired switch.

While the US DoD continues to develop this system, one may also consider the case for a similar and compatible trusted capital marketplace model that could be applied across several Allied nations, and potentially also certain partner nations of NATO. Under favorable conditions, such a model could create a new reality, as it would spread outward from an initial core, acting as a desirable certification that both innovating companies and potential investors would seek to obtain.

How a trusted capital marketplace certification would complement national and EU-level investment screening provisions would remain to be determined. In any case, one could imagine investors from certain non-Allied nations retaining access to non-sensitive sectors, while not being granted the certification for sensitive technology markets. Such a differentiation may be important in terms of engagement and signaling. It would be clear to relevant non-Western powers that the policy goal is not to rule out broader forms of mutually beneficial economic exchange, but to protect sensitive sectors from inappropriate attention. Conversely, a trusted capital marketplace which would welcome like-minded investors from like-minded nations could provide a boost to Western cohesion.

Conclusion

AI is a disruptive technology because it transforms organizations and their activities not only once it is in place, but also and already during its adoption. This chapter has highlighted a range of managerial, organizational, and governance challenges that already manifest themselves in national defense institutions, as well as at NATO, concerning processes, people, data, and financing. These challenges are substantial and will require significant attention, willingness to reform, and adequate resources if Allies wish to maximize the benefits that AI may bring in a timeframe that accounts for international risks and rivalries. That said, some of the measures Allies should consider have the potential to strengthen Alliance cohesion, and to raise the efficiency of common Allied and NATO activities in a broader sense. The challenge of AI is fundamentally an opportunity to revisit old practices and to modernize how Allies and other like-minded nations collaborate and exchange in the pursuit of talented personnel, data, organizational insights, and well-designed legal and regulatory frameworks.

References

Altmann, Jurgen & Frank Sauer (2017). “Autonomous Weapon Systems and Strategic Stability”. In Survival, Vol. 59, No. 5, pp. 117-142.

Atwal, Harvinder (2020) (ed.). Practical DataOps: Delivering Agile Data Science at Scale. New York City: Apress Media.

CRS (Congressional Research Service) (2020). International Discussions Concerning Lethal Autonomous Weapon Systems. In Focus series, IF11294, Version 2 (updated).

DASA (United Kingdom Defence and Security Accelerator) (2019). Defence and Security Accelerator (DASA) Annual Review 2018-2019.

DSTL (Defence Science and Technology Laboratory) (2019)- The Dstl Biscuit Book, 1st Revised edition.

Dufour, Martin (2018). “Will artificial intelligence challenge NATO interoperability?”. In NATO Defence College, NDC Policy Brief No. 6.

Hechler, Eberhard, Martin Oberhofer and Thomas Schaeck (2020) (eds.). Deploying AI in the Enterprise: IT Approaches for Design, DevOps, Governance, Change Management, Blockchain, and Quantum Computing. New York City: Apress Media.

JAIC (Joint Artificial Intelligence Center) (2020). Understanding AI Technology. In United States Department of Defense.

Kim, Gene, Jez Humble, Patrick Debois, and John Willis (2016) (eds.). The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations. Portland: IT Revolution Press.

Lin-Greenberg, Erik (2020). “Allies and Artificial Intelligence: Obstacles to Operations and Decision Making”. InTexas National Security Review, Vol. 3, No. 2, pp. 56-76.

Lord, Ellen (2020). “Trusted Capital Marketplace Protects DoD Supply Chain”. In National Defense Magazine.

Mahoney, Charles W. (2020). “United States defence contractors and the future of military operations”. In Defense & Security Analysis, Vol. 36, No. 2, pp. 180-200.

Messina, Angelo & Franco Fiore (2016). “The Italian army C2 evolution: from the current SIACCON2 land command & control system to the LC2EVO using “Agile” software development methodology”. In 2016 International Conference on Military Communications and Information Systems (ICMCIS), IEEE, pp. 1-8.

Morales, Jose, Richard Turner, Suzanne Miller, Peter Capell, Patrick Place, and David James Shepard (2019), “Guide to Implementing DevSecOps for a System of Systems in Highly Regulated Environments”. In Carnegie Mellon University, Technical Report.

NSCAI (National Security Commission on Artificial Intelligence) (2020). Interim Report and Third Quarter Recommendations.

Reding, Dale F. & Jacqueline Eaton (2020) (eds.). Science & Technology Trends 2020-2040 - Exploring the S&T Edge. Brussels: NATO Science & Technology Organization.

Schaus, John & Kaitlyn Johnson (2018). “Unmanned Aerial Systems' Influences on Conflict Escalation Dynamics”. In Center for Strategic and International Studies, CSIS Briefs.

Svenmarck, Peter, Linus Luotsinen, Mattias Nilsson and Johan Schubert (2018). “Possibilities and challenges for artificial intelligence in military applications”. In: Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists’ Meeting, NATO Science & Technology Organization.

UK MoD (United Kingdom Ministry of Defence) (2020), Data Management Strategy.

US Congress (2019). National Defense Authorization Act for Fiscal Year 2020. Public Law 116-92, 116th Congress.

US DoD (United States Department of Defense) (2020). DoD Data Strategy.

US Treasury (2018). FIRRMA FAQs, undated online document.

Valentine, Crystal & William Merchan (2018). “DataOps: An Agile Methodology for Data-Driven Organizations. In Oracle Corporation.

Wong, Yuna H. et al. (2020) (eds.). “Deterrence in the Age of Thinking Machines”. Santa Monica: RAND Corporation.

WORKING GROUP REPORT

NATO, BIG DATA AND AUTOMATION: DECISIONS AND CONSENSUS

Andrea Gilli - NATO Defence College

Working Group (WG) 3 had a comprehensive, deep and sophisticated discussion. Some issues were touched upon at the very beginning but were then further elaborated in later comments. In other cases, some big topics were broken into smaller pieces throughout the entire activity of the WG. For these reasons, this report summarizes the discussion analytically (by theme) rather than chronologically (by time).

Change

A first question concerns the type and pace of the change we are observing and the response for which it calls. Is Artificial Intelligence (AI) a technological revolution, or is this an instance of technological evolution? Participants did not have a single view: different pieces of evidence can support both interpretations. For instance, the first conference on AI was held in 1956, but progress in deep neural networks is less than a decade old. From an academic perspective, there is some degree of consensus that AI is a major technological revolution because of its general-purpose nature, its potential pervasiveness. However, as such, it will take time – and investments – to unleash all its potential. Within the transatlantic Alliance, the US has been at the forefront of both technological and military innovation during and after the Cold War. Thus, its role will be crucial in making AI evolutionary or revolutionary for defense, with cascade effects on the Alliance, the militaries and the defense industries of NATO's European members. Competition with China may be the driver of such leap for the US, but Europe presents different views in this regard, as well as on the type of change to be brought by AI in the defense domain.

Participants thus discussed how to approach such change. Some were calling for extensive and profound reforms. Others made the point that technology is part of our societies, economies and polities: hence, harsh changes and quick adaptation reforms for the pursuit of superior efficiency or effectiveness may have unforeseeable or even counterintuitive effects. More specifically, according to some, it will be hard for NATO Allies, from a political perspective, to adapt swiftly to a rapid technological revolution. And in any case, NATO's approach, because of the consensus characterizing its procedures, will have to be more evolutionary, granular and nuanced. From a military perspective, caution is in any case warranted, as the most recent similar debate – on the revolution in military affairs – led in several instances to questionable strategic narratives or policy choices.

It was also noted that, in the NATO context, we are unlikely to see AI making decisions for the North Atlantic Council (NAC) or the Nuclear Planning Group (NPG) any time soon. There are psychological, cultural, organizational and political reasons – including that human beings are hesitant to cede control. But there are also, more simply, technical factors. Machine Learning (ML) algorithms are extremely good at prediction and pattern recognition, but they require plenty of data. Political decisions are often taken in different contexts and, rather than being informed by data analytics-based prediction, they are often shaped by political

judgement, which is something machines cannot (yet) master, not the least because it cannot be easily turned into data and parameters.

Input

The conversation then moved, repeatedly, to the key inputs AI requires. Ben Buchanan of Georgetown University speaks of a triad: processors, algorithms and data. In different ways, participants highlighted the importance of both the performance and the globalized nature of high-tech sectors, including the supply chains, their security and the dependencies they brought. Whether China will catch up or not and what NATO Allies can do in this respect is open to debate.

When it comes to AI, preserving a leading transatlantic industrial base in the realm of semiconductors is however key for the future. Progress in algorithms is a second important element. Software are difficult to develop, not the least because of recruitment and organizational challenges. Universities are no longer able to keep the pace with the progress in softwares – in fact, many academic curricula are obsolete. Similarly, organizations – whether civilian or military – struggle to attract the talent needed to exploit AI. Finally, ML algorithms are fed by data. Within NATO, however, there are different views, sensitivities and policies about data (including privacy, sharing and sovereignty). Such differences impact the availability of data at the national level but also at the Alliance level, with profound impact on interoperability. Data, additionally, is like oil, in the sense that it needs to be processed before it can be used. As whole, the issue of AI could be included also in the current NATO reflection on the resilience of Allies' technological and industrial bases, as well as of Western societies at large.

Enablers

The discussion on inputs led, repeatedly, to a useful conversation on the enablers. Most participants agree in fact, to quote one of the interventions, that the journey to AI will be troublesome. That is because it will call for reforms, strategies, actions and investments. For instance, military organizations will have to revise recruitment and retainment policies – we will need individuals with different skills who, as such, may appeal to different or non-traditional incentives. Organizations will have to change to attract, promote and exploit innovation. Many participants discussed the case of agile software development: while enabling the development of superior software, this approach also calls for different procedures, organizational structures and processes. Just like other related organizational challenges, this is difficult, not the least because it touches upon organization's identities, missions and culture.

At the NATO level, one participant highlighted the constraining role of military culture, as well as the difference between "doers", tasked to conduct current operations, and "developers", charged to look at future operations and drive military transformation accordingly. Within the Alliance, this dualism is embodied by the division of labor between two commands: Allied Command Operations (ACO) and Allied Command Transformation (ACT). The former experiences greater political priority in the Allies' agenda, in light of both ongoing crisis management operations and increasing deterrence and defense activities. This situation could prevent the full exploitation of AI and of innovation more in general in the years ahead. Moreover, with AI, the border between research and product blurs – which suggests that with the introduction of AI in the military realm, the border between training, education and capabilities development, on the one hand, and operations on the other, may also blur. Logically, this could represent a challenge in the future.

Another issue which attracted significant attention concerns private-public partnership and the alleged or potential disadvantages NATO Allies face vis-à-vis China. In this respect, the experts' consensus seems to be that all actors trying to enter the AI race will face the same challenges, and the trade-off between control and innovation is not going to disappear, also for Beijing. In other words, China may have an advantage in directing its domestic economy, but this may end up stifling some innovations; conversely, NATO Allies' softer industrial policies may not provide sufficient incentives to invest in specific fields, but this may still leave room for creative individuals to develop effective solutions. In any case, it was repeatedly stressed that the relations between NATO and major civilian companies working on AI and Big Data are relatively weak and have to be strengthened. One interesting option for NATO could be launching a forum, like the NATO Industry Forum, on AI, aimed at enabling the AI ecosystem to better connect and network with the Alliance's structures and capabilities.

Output

A recurrent theme of the entire Conference concerned AI's meaning within the defense domain. WG3 delved into this issue as well. Some raised questions about arms control, others about capabilities, while decision-making was dealt with extreme cautiousness. One participant highlighted that AI can be divided in three tiers: Enterprise AI, Operational AI and Mission Support AI. Enterprise AI concerns applications generally deployed in controlled environments, from personnel to every-day logistics or finance. In such environments, failure is both easier to predict and less catastrophic if it happens. Operational AI, conversely, is about supporting missions and operations. A good example is an AI-centered system for target detection or for cybersecurity. In these cases, uncertainty is higher due to the more heterogeneous environment, and implications for failure are more relevant. Finally, Mission Support AI refers to applications, such as logistics and maintenance, where the degree of control over the environment varies, but it is not the highest. Clarifying these issues is relevant for policy-makers to appreciate different degrees of risk.

In this respect, one of the most important questions Allies should ask themselves is what they want AI to do. This is not just a military or defense question: this is a political and probably ethical issue since there is a wide spectrum of views, sensitivities and perceptions involved. Important debates about arms control or data governance are ultimately connected to these broader issues. Some Allies may want to use AI just to optimize logistics and increase efficiency in the management of various NATO activities. Others may see it widely used at a tactical level, particularly with intelligence, surveillance and reconnaissance functions. Others may be looking at integrating AI into their force structure with a more ambitious visions, somehow recalling the revolution in military affairs approach.

Against this backdrop, a debate about AI-related ethics in the defense domain is paramount, not only to reach a consensus among Allies but also to strengthen the political bonds of the Alliance. From this starting point, NATO can play an important role in other domains. In some cases, like standardizations, NATO has historically been an important player, and should make further steps also to prevent interoperability problems due to a fragmented adoption of AI. In other instances, some creativity may be needed: for instance, should NATO provide cloud computing services, namely enablers, the same way it provides air-space management – through Airborne Warning and Control System (AWACS) aircrafts – or ground surveillance – through the Alliance Ground Surveillance (AGS) program? Could NATO envision an integration of nationally-owned AI assets as it does with the integrated air and missile defense? These are important

questions which, however, highlight the fact that defense is a sovereign issue and most decisions are taken by national governments, not by NATO as such.

NATO's Role and the Interaction with the EU

What is, then, NATO's role? Although the issue was mostly discussed in the last session of the WG, participants exchanged views on the potential role of NATO throughout the entire debate. The conversation sedimented around a few central themes. In many ways, from membership to mandate, from resources to capabilities, NATO and the European Union (EU) differ remarkably. In particular concerning AI-related policy and regulatory measures, the Alliance has a smaller staff and a smaller budget than the Union, and does not have the same power – differently from the EU, NATO is not a legislative body whose directives are automatically implemented by member states, and it lacks financial instruments.

Bearing in mind that caveat, the WG discussed a recent report by the NATO Defense College (NDC), which illustrated some areas where the Alliance can pragmatically play an important role. For instance, besides the aforementioned important issue of ethics, NATO could establish an AI champion to help Allies understand, adopt and integrate AI. Such champion could start with small projects aiming at validating the effectiveness of the solution, then it could help Allies in training. Related to this topic is indeed the issue of education. A recent report from the US National Security Commission on Artificial Intelligence noted that the NDC could promote strategic level education on AI to understand the implications of the transformation we are observing. Similarly, the role of wargames, simulations and experimentations is going to grow, and NATO has a role to play here, as the unique avenue to convene allied military and political bodies. Noticeably, in its recent exercises, data analytics were gathered and processed. The Alliance could also mimic what was done with the Prague Capabilities Commitment and then with the Cyber Defence Pledge, i.e. help Allies identify capability goals and priorities, and develop a roadmap for their adoption of AI. WG participants noted that the NATO Defence Planning Process (NPPP) has an important, yet difficult role to play in this regard, because AI adoption is inherently different and somehow less tangible than the procurement of military platforms.

At the same time, in some areas NATO could benefit from working closely with the European Union (EU) or with the Organization for Economic Co-operation and Development (OECD), as they have more capabilities and expertise. For instance, some participants noted that without a more integrated European defense market and industry, it will be hard to have an effective conversation on these issues, and the EU has an important role to play in this regard. On a more general note, another participant pointed out that, in Europe, NATO faces a scarcity of high-tech companies, and this may create tensions as well as capability gaps with the US in the future. Current debates about the applicability of the General Data Protection Regulation (GDPR) or about a digital tax, somehow point in this direction. The recent history of high-tech, however, suggests that a single market is not always sufficient to develop Big Tech giants: Samsung is from South Korea and Nokia is from Sweden – both medium-sized countries. Regardless of how the conversation about Big Tech and AI will evolve politically and ideationally in the forthcoming years, the key issue for NATO is how to deal with AI in the defense domain, how to promote cooperation with the EU and, broadly speaking, between the US and Europe.

Acronym list

ACO	Allied Command Operations
ACT	Allied Command Transformation
AGS	Alliance Ground Surveillance
AI	Artificial Intelligence
AIOps	Artificial Intelligence Operations
AWACS	Airborne Warning and Control System
BDA	Big Data Analytics
BFT	Below-Blue Force Tracker
C2	Command and Control
CCD	Cooperative Cyber Defence
CENTCOM	United States Central Command
CFIUS	Committee on Foreign Investment in the United States
CIA	Central Intelligence Agency
CoE	Centre of Excellence
CRS	Congressional Research Service
DataOps	Data Operations
DARPA	Defense Advanced Research Projects Agency
DASA	Defence and Security Accelerator
DDoS	Distributed Denial of Service
DevOps	Development Operations
DevSecOps	Development Security Operations
DFRLab	Atlantic Council Digital Forensic Lab
DIU	Defense Innovation Unit
DIUx	Defense Innovation Unit Experimental
DNC	Democratic National Committee
DoD	Department of Defense

DSTL	Defence Science and Technology Laboratory
EDTs	Emerging Disruptive Technologies
ENISA	European Union Network and Information Security Agency
EU	European Union
FDIs	Foreign Direct Investments
FIRRMA	Foreign Investment Risk Review Modernization Act
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
HES	Hamlet Evaluation System
HFC	Hybrid Fusion Cell
HROs	High Reliability Organizations
HPIT	Hyper-Personalized Influence Targeting
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
IAI	Istituto Affari Internazionali
ICTs	Information Communication Technologies
IR	International Relations
IRA	Russian Internet Research Agency
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JAIC	Joint Artificial Intelligence Center
JALLC	Joint Analysis and Lessons Learned Centre
JISD	Joint Intelligence and Security Division
LAWS	Lethal Autonomous Weapons Systems
MCDS	Multinational Capability Development Campaign
ML	Machine Learning
MLOps	Machine Learning Operations
MoD	Ministry of Defence
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization

NCIA	NATO Communications and Information Agency
NDC	NATO Defence College
NPG	Nuclear Planning Group
NPPP	NATO Defence Planning Process
NSA	National Security Agency
NSCAI	National Security Commission on Artificial Intelligence
OODA	Observe, Orient, Decide, Act
OECD	Organization for Economic Co-operation and Development
OTA	Other Transaction Authorities
PLA	People's Liberation Army
PwC	PricewaterhouseCoopers
R&D	Research & Development
SACEUR	Supreme Allied Commander for Europe
SEES	Situation awareness, Explanation, Estimate and Strategic notice
SMEs	Small and Medium Enterprises
StratCom	Strategic Communications
TEVV	Testing, Experimentation, Validation, and Verification
TFEU	Treaty on the Functioning of the European Union
UAS	Unmanned Aircraft System
UGS	Unmanned Ground Systems
UK	United Kingdom
US	United States
US Navy SEALs	US States Navy Sea, Air, and Land Teams
WG	Working Group