



Research Division

NATO Defense College

NATO@70

NDC POLICY BRIEF

No. 4 – February 2019

Preparing for “NATO-mation”: the Atlantic Alliance toward the age of artificial intelligence

Andrea Gilli *

The unprecedented pace of technological change brought about by the fourth Industrial Revolution offers enormous opportunities but also entails some risks. This is evident when looking at discussions about artificial intelligence (AI), machine learning (ML) and big data (BD). Many analysts, scholars and policy-makers are in fact worried that, beside efficiency and new economic opportunities, these technologies may also promote international instability: for instance, by leading to a swift redistribution of wealth around the world; a rapid diffusion of military capabilities or by heightening the risks of military escalation and conflict.

Such concerns are understandable. Throughout history, technological change has at times exerted similar effects. Additionally, human beings seem to have an innate fear that autonomous machines might, at some point, revolt and threaten humanity – as illustrated in popular culture, from Hebrew tradition’s *Golem* to Mary Shelley’s *Frankenstein*, from Karel Čapek’s *Robot* to Isaac Asimov’s *I, Robot* and the movie *Terminator*.

This *NDC Policy Brief* contributes to the existing debate by assessing the logic behind some of these concerns and by looking at the historical record. While some worries are warranted, this brief provides a much more reassuring view. The implications

are straightforward: NATO, its member states and partners should not be afraid of ongoing technological change, but embrace the opportunities offered by new technologies and address the related challenges. In other words, the Atlantic Alliance should start a new transformation process directed toward the age of intelligent machines: it should start with what I call “NATO-mation”. The goal is not only preserving and enhancing NATO’s military superiority and thus better contribute to global security in the decades ahead but also ensuring that its values, ethical stances as well as moral commitments will remain central in a rapidly-changing security environment.

Strategic consequences of rapidly changing technology

Three main technological trends are currently underway. First, accelerating growth in the power of processors will add more computing power, over the next few years, than in all of human history combined.¹ Second, software is not only *eating the world*, it is also progressively re-designing it thanks to recent developments in computer science and, in particular, in the field of deep neural networks.² Finally, due to the growing availability of portable devices, electronic content has been doubling every 24 months in the recent past, to the extent that 90 percent of existing digital data was created in the past two years. Such growth rates are expected to accelerate in the near future.³

The results of these trends are, potentially, transformative, as increasingly sophisticated algorithms (machine learning) will exploit the growing availability of digital content (big data) to quickly gain

1 E. Brynjolfsson and A. McAfee, *The second machine age: work, progress, and prosperity in a time of brilliant technologies*, W. W. Norton & Company, New York, NY, 2014.

2 M. Andreessen, “Why software is eating the world”, *Wall Street Journal*, 20 August 2011.

3 D. Reinsel, J. Gantz and J. Rydning, “Data age 2025: the digitization of the world from edge to core”, *White Paper*, International Data Corporation, Washington, DC, November 2018.

* Senior Researcher in the Research Division, NDC.

The idea that countries can quickly exploit the technologies of the fourth Industrial Revolution for building military power is exaggerated

real-world experience and thus conduct human-like activities (artificial intelligence). Since machines are significantly better than human beings in some tasks, the speed, depth and breadth of interactions will likely grow exponentially. For instance, companies will increasingly exploit software and digital content for rapidly inventing, testing and developing new concepts, products and solutions.⁴ By the same token, as algorithms will improve in accuracy, online shopping might eventually transition to online shipping-only: software will autonomously ship to customers what they need, based on their digital records. Self-evidently, such changes will have enormous implications for business practices and organizational structures as well as for competition.⁵

Finally, improvements in software accuracy will lower the costs of adopting intelligent machines that, in turn, will progressively spread across borders and throughout industries, including in the defense and security domains. While economists, consultants and entrepreneurs have so far been relatively optimistic, security scholars have generally aligned with the concerns expressed in the public debate. Three deserve attention:

- *Geo-economic transition.* Many analysts worry that the transformation brought about by AI, ML and BD will rapidly alter the sources of wealth creation, thus favouring the rise of some countries and the demise of those lagging behind, ultimately affecting the structure of world politics.
- *Military transformation.* Others believe that this major wave of technological change, coupled with its dual-use nature, could influence the military balance at the tactical and operational levels, thus changing the dynamics of deterrence, destabilizing the international system and increasing the likelihood of war.
- *Crisis escalation and heightened risk of conflict.* Finally, there is concern in some quarters that algorithms will inadvertently escalate diplomatic crises into military confrontations or exacerbate the intensity of conflict as, lacking key human traits such as judgment and experience, autonomous machines may fundamentally, and systematically, misread the behavior of enemies and adversaries.

4 H. J. Wilson and P. Daugherty, *Human + machine: reimagining work in the age of AI*, Harvard Business School Press, Cambridge, MA, 2018.

5 A. Agrawal, J. Gans and A. Goldfarb, *Prediction machines: the simple economics of artificial intelligence*, Harvard Business School Press, Cambridge, MA, 2018.

Both historical evidence and deductive logic, however, warrant some caution.

Geo-economic transition and commercial technology

Automation is nothing new: it is part of a broader and longer-term industrial-era process of substitution of labor with capital. The main difference is that in the early 19th century, machines *primarily* replaced humans, animals or nature in the production of energy. Nowadays, machines *increasingly* substitute brainpower. The question is whether the technological revolution driven by AI, ML and BD can lead to a rapid shift in economic power around the world.

First of all, for rapid, worldwide shifts of economic power to occur, two conditions must be met: new technologies must rapidly change the sources of wealth creation (from wind to steam, from steam to oil, from oil to nuclear, and so forth) and only some countries must be in the position to transition quickly – thus leaving the others behind.

Historically, very rarely have technological transformations had immediate economic effects. With the first Industrial Revolution, for instance, it took about 100 years for the steam engine to unleash all its dramatic consequences. Similarly, modern computers did not significantly affect productivity statistics until the mid-1990s, albeit introduced in the early 1950s. This is because new technologies, sometimes, require improvement in other technologies, construction of infrastructure as well as cultural and social adaptation. This process takes time. Thus, if AI, ML and BD prove to be like the steam engine or the computer, they will exert enormous economic effects, but the risk of a rapid geo-economic transition is greatly exaggerated.⁶

Not all technological revolutions take so long, however: the fuel engine and electricity had much more immediate consequences. But for rapid geo-economic transitions to occur, the second condition must also be met: namely, only some countries must be able to adapt quickly; others, not. Concerns about economic competitiveness as well as the risk of lagging behind technologically are legitimate. However, if some technologies have massive and immediate economic effects, this also means they become available very quickly and thus there is a minimal risk of lagging behind. As a result, investing heavily in emerging and rapidly spreading technologies can, paradoxically, prove counterproductive as a country may end up indirectly subsidizing peers, competitors and even adversaries.

Some countries may decide to resist, for cultural reasons, some technologies or their armed forces may be unable, cognitively, to understand the

6 E. Brynjolfsson, D. Rock and C. Syverson, “Artificial intelligence and the modern productivity paradox: a clash of expectations and statistics”, *NBER Working Paper*, No. 24001, November 2017.

strategic implications of underlying technological transformations: but this has little to do with the properties of the technologies and more with the features of the adopters.⁷

Military transformation and emerging technologies

A second, and related, issue is the risk that, in the age of intelligent machines, AI, ML and BD may easily enable any actor to catch up, or even outpace, its adversaries in military terms. Here too, skepticism is warranted. First of all, these two concerns logically contradict each other. If we are witnessing a military transformation based on dual-use, general-purpose technologies such as AI, ML and BD that can be easily exploited in battle, then no actor can achieve a significantly enduring military advantage – at the tactical, operational or strategic level – as competitors can quickly catch up or deploy effective counter-systems.⁸

Next, military power is more than hardware. Tactical fluency and operational competence are in fact extremely important for victory on the battlefield – along with other variables. There is no reason to believe that this will change anytime soon, as warfare, war and by extension strategy are inherently adversarial: winners succeed because they defeat their adversaries – i.e., they neutralize enemy counter-measures, tactics, systems and innovations. Possessing capable hardware is thus, *per se*, not sufficient and, at times, not even necessary for winning. Commercial technologies offer great potential but are easily vulnerable to even basic counter-measures as they are not designed for combat.

By the same token, emerging technologies – whether developed for commercial or military applications – face performance trade-offs that constrain their immediate military utility. The French *Marine Nationale*'s mid-19th century bid to offset British naval superiority is telling: the steam engine granted independence from wind but suffered from limited endurance; iron hulls could not keep afloat when hit; and, explosive shells had shorter ranges than solid shots. When mature, these technologies ultimately transformed naval warfare, but it took almost a century for this to happen.⁹

There is no reason to believe that with AI, ML and BD things will be different. When it comes to software, in fact, even subtle and apparently minor details lead to catastrophic failure: because of simple mistakes in data gathering or processing such as automatic path control, military platforms may end up exceeding their maximum depth or altitude ceilings and thus expose

themselves to almost certain mission failure. Software already represents the primary source of procurement delays and cost overruns. As software becomes more central in weapon systems, the problems it creates can only exponentially increase. Additionally, through generative adversarial networks (GNAs), actors can increasingly feed compromised data into enemy systems to negatively affect tactical performance or operational success. Competent armed forces will thus deploy intelligent machines only in so far as the risks, problems and constraints they face are, slowly and progressively, addressed.

This brings us to a final consideration. In order to address these very risks, problems and constraints, investments in a broad range of fields are also needed so as to counterbalance investments by enemies and adversaries. Improving all the underlying technologies related to AI, ML and BD, learning about their potential, integrating them into existing military platforms and exploiting them for maximum strategic, operational or tactical effectiveness require time, human capital, institutional backing, technological competence and financial resources. In other words, the idea that countries can quickly exploit the technologies of the fourth Industrial Revolution for building military power seems exaggerated.¹⁰

Crisis escalation and heightened risk conflict due to technological change

This brings us to the final concern related to the current technological transition. According to the most pessimistic interpretations, algorithms are likely to escalate diplomatic crises into military confrontations and further increase the intensity of combat. In other words, conflict and the use of violence may soon become much more common because intelligent machines are allegedly lacking in political understanding and human experience. This is a crucial topic, worthy of the highest ethical considerations and political attention. But here again, history and logic reassure against the bleakest outlook.

First, automation is nothing new, as machines conducting calculations and computations have long existed: the late 19th century self-propelled torpedo relied on automatic devices for hydrostatic stability and course correction; early 20th century naval guns employed mechanical fire control systems for long-

By engaging with these issues, NATO can ensure that its values, ethical stances as well as moral commitments will inform this new age

7 D. Adamsky, *The culture of military innovation: the impact of cultural factors on the revolution in military affairs in Russia, the US, and Israel*, Stanford University Press, Palo Alto, CA, 2010.

8 S. D. Biddle, "The past as prologue: assessing theories of future warfare", *Security Studies*, Vol. 8, No. 1, 1998, pp. 1-74.

9 S. C. Tucker, *Handbook of 19th century naval warfare*, Naval Institute Press, Annapolis, MD, 2000.

10 A. Gilli and M. Gilli, "Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage", *International Security*, Vol. 43, No. 3, 2019, pp. 141-89.

range accuracy; similarly, electronics and computers have enabled the evolution of military aircraft through the 20th and 21st centuries as the speed, number and complexity of calculations have grown beyond the cognitive abilities of the pilot(s) in the cockpit.¹¹

Second, most observers look at the process of automation as a substitution between labor (personnel) and capital (hardware and software). In fact, any technological transition also entails a *complementation* process. By reducing the cost of some tasks and products, technological change inherently leads to an increase in the demand for goods or services that are jointly consumed (e.g., *complements*). For instance, by making real-time, long-distance video surveillance more readily accessible, drones have inherently called for a surge in bandwidth consumption and imagery analysts. Drones may be cheap and easy to build, but as their use increases, the availability of bandwidth and the supply of imagery analysts inevitably represent a growing constraint to operations. AI, ML and BD not only inherently raise similar challenges, but the more disruptive they prove, the more acute the related challenges will be – making it more difficult to exploit such new technology.

Some may object that algorithms can still misunderstand signals and thus pull countries into spirals of confrontation, escalation and conflict or, alternatively, lead to excessive violence in warfare. This is a reasonable worry that rests, however, on the assumption that countries have access to battle-proven autonomous systems, capable of neutralizing most counter-measures and also supported by all the necessary complements. If this assumption does not materialize, AI, ML and BD can deliver very little in battle. The above discussion shows that meeting those conditions is extremely challenging.

Implications for NATO

AI, ML and BD offer great opportunities, but also present risks and challenges. This analysis has tried to alleviate the most pressing worries: in so far as the public concerns are related to rapid geo-economic transitions, sudden redistributions of military power,

or the escalation of military crises, there are reasons to be relatively optimistic. This has many implications both for international security and for NATO, its constituent bodies, its member states and its partners.

First, many are worried about an AI arms race. Based on the analysis presented in this article, we should not be and, probably, we should even reinterpret our competitors' actions. Put simply, based on what is written so far, Russian President Vladimir Putin's famous *Lords of the Rings*-like speech about AI as a key instrument to control the world could have been intended to generate panic and thus slow down NATO and its member countries since Russia lacks the technological bases for competing in this field. However, if Russia's Ministry of Defense agrees with President Putin and then wants to reduce funding to nuclear weapons, ballistic missiles and nuclear submarines in order to invest in a set of so far unproven, unreliable and combat-ineffective technologies, we should definitely not oppose this move – and probably even encourage them to.

Second, NATO and its member states should not remain passive observers. On the contrary, they should start preparing to address the challenges that AI, ML and BD raise. In other words, the Alliance should start a process of "NATO-mation". This is important for three main reasons. By honing and improving existing technological and industrial capabilities, NATO can preserve and enhance its military superiority and thus guarantee its contribution for global security in the years ahead. Next, for this purpose, NATO should start thinking and addressing the complements challenges that will emerge: from infrastructural constraints to shortage of talent. Last but not least, by engaging with these issues, the Atlantic Alliance can ensure that its values, ethical stances as well as moral commitments will inform this new age.

*By honing
and improving
existing
technological
and industrial
capabilities,
NATO
can preserve
and enhance
its military
superiority*

11 S. A. Fino, *Tiger check automating the US air force fighter pilot in air-to-air combat, 1950–1980*, Baltimore, MD, Johns Hopkins University Press, 2017.



The views expressed in this *NDC Policy Brief* are the responsibility of the author(s) and do not necessarily reflect the opinions of the NATO Defense College, NATO, or any government or institution represented by the contributors.

Research Division

Thierry Tardy, PhD, Series Editor
NATO Defense College
Via Giorgio Pelosi 1, 00143 Rome – Italy
website: www.ndc.nato.int

Follow us on Twitter and Facebook
at https://twitter.com/NDC_Research
at https://facebook.com/NDC_Research
NDC Policy Brief
ISSN 2617-6009



The NATO Defense College applies the Creative Commons Licence "Attribution-NonCommercial-NoDerivs" (CC BY-NC-ND)