THE GLOBAL RACE FOR TECHNOLOGICAL SUPERIORITY

Discover the Security Implications

edited by **Fabio Rugge**
introduction by **John R. Allen** and **Giampiero Massolo**

ISPI
BROOKINGS

THE GLOBAL RACE FOR TECHNOLOGICAL SUPERIORITY

edited by Fabio Rugge

ISPI BROOKINGS

Via Alamanni, 11 – 20141 Milano – Italy
www.ledizioni.it
info@ledizioni.it

The Global Race for Technological Superiority
Edited by Fabio Rugge
First edition: November 2019

This report is published with the support of the Italian Ministry of Foreign Affairs and International Cooperation (in accordance with Article 23- bis of the Decree of the President of the Italian Republic 18/1967), within the framework of the activities of the Centre on Cybersecurity jointly promoted by ISPI and Leonardo. The opinions expressed are those of the authors.

Print ISBN 9788855261432
ePub ISBN 9788855261449
Pdf ISBN 9788855261456
DOI 10.14672/55261432

ISPI. Via Clerici, 5
20121, Milan
www.ispionline.it

Catalogue and reprints information: www.ledizioni.it
Cover image: Fulvio ranieri mariani, turbine aereo, 1938

BROOKINGS

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public.

Table of Contents

4. AI in the Aether: Military Information Conflict

Tom Stefanick

Since the advent of modern deep learning earlier this decade, there has been significant discussion of artificial intelligence and information warfare. In his paper, titled *"Mind Hacking": Information Warfare in the Cyber Age*, Fabio Rugge[1] discusses the growing strategic importance of the "information space" as a regime of conflict in military operations. "Operations in this domain are central to Russia's security strategic thinking, featuring prominently in its 'New Generation War' military doctrine"[2]. In early 2019, ISPI highlighted a different element of warfare with the publication of "Artificial Intelligence: A New Era of Warfare" by John R. Allen, President of the Brookings Institution. In his piece, Allen warns that the synergy of artificial intelligence (AI), analytic methods applied to huge data sets, and super-computing "represents the core ability to remain competitive in an era of great power conflict"[3]. I will extend those discussions to electronic warfare and it's central role in NATO's ability to deter Russian intimidation and aggression.

---

* This chapter is part of a forthcoming book on artificial intelligence and how it may impact military capabilities. The book will be published by Brookings Press in late 2020.

[1] F. Rugge, *"Mind Hacking": Information Warfare in the Cyber Age*, ISPI Analysis no. 319, ISPI, January 2018.

[2] Ibid., p. 1.

[3] J.R. Allen, "Artificial Intelligence: A New Era of Warfare," *The World in 2019*, ISPI Dossier, January 2018.

Electronic warfare (EW) systems directly impact the information space of military conflict. With the increasing automation of EW systems, modern AI algorithms are being investigated to determine their value as a component of new EW systems. I discuss the ways in which modern AI algorithms may or may not be incorporated into EW systems, and prospects for the sudden emergence of a Russian AI-driven EW capability. I will also highlight the serious dilemma created by effective EW, as it can inhibit human control over unmanned weapons, while at the same time bolstering NATO's deterrence of Russia. To begin this analysis, I walk through some explanations of AI and EW before returning to their importance for NATO.

What is Artificial Intelligence?

The term "artificial intelligence" has had no fixed meaning since it first entered the computer science lexicon in the late 1950s. The definition used here is narrower than that typically used in the current policy and futurist literature, and is proposed as a baseline to focus discussion. However, the definition is sufficiently broad to encompass current research and implementations that are likely to have practical national security implications within the next 20 years. "Machine learning" is a term that encompasses a very wide set of algorithms – including modern AI algorithms – which perform a range of tasks as described below. Machine learning, as the much broader concept, includes algorithm designs based on a much wider range of mathematical principles than the principles underlying modern AI algorithms.

The surge of excitement, apprehension, and imaginative speculation about the impacts of artificial intelligence (AI) since around 2014 appears to follow upon a rapid sequence of newsworthy technical accomplishments. These accomplishments include highly accurate image, video, and face recognition; improved prediction of machinery degradation; language translation and sentiment/topic detection in text; recommendations

for the next video to watch; reliable voice recognition and automatic dialog generation; synthetic image, video and voice generation of individuals ("deep fakes"); control of complex physical systems; and high-level game play against opponents in board games and computerized warfare games. Many of these algorithms are widely available as open-source software.

Recent AI algorithm advances are the product of a convergence of three elements that have been a long time in development: advances in algorithms based on extremely large neural networks with millions of adjustable parameters, adaptation of inexpensive parallel-processing computer chips including graphical processing units (GPUs) and other designs, and the ever-expanding availability of online data generated by humans and sensing devices through all forms of social media and other online services.

Modern AI as defined here comprises two main classes of algorithms: deep neural networks and deep reinforcement learning algorithms. The foundational modern AI algorithm is the deep neural network (DNN), which may be configured in a large number of ways depending on its function and the data it is using. Deep neural networks are built up from a very large number of simple computational sub-functions, which in the aggregate have millions to hundreds of millions or more adjustable parameters. These DNNs can approximate virtually any complex relationship between inputs and outputs by using large data samples to adjust these parameters depending on the intended use. New DNN architectures and approximation methods are invented regularly, and no attempt is made to reference them all explicitly.

The second group of algorithms driving modern AI – deep reinforcement learning (deep RL) – is designed to interact with complex environments such as game systems or control variables for physical systems. As the name suggests, deep RL algorithms incorporate deep neural networks to store the information they extract from their environments. As deep RL algorithms explore these environments by moving through possible

system states, they receive data on how actions result in changes to the environment, and they also reap a reward signal that guides their behavior. Over many – often millions – of interactions with the same environment and reward rules, these deep RL algorithms compute approximate solutions for operating in that environment and store these solutions in the embedded DNNs.

As a final note regarding definitions, it is recommended that discussion of autonomous systems – physical or computational – be clearly distinguished from AI as defined above. Any number of algorithms, including but not exclusively AI algorithms may enable highly effective autonomous systems. Moreover, physical autonomous systems are constrained by physical limitations (e.g. energy) that must be considered when assessing their capabilities. The electronic warfare systems of all modern militaries are heavily reliant on autonomous algorithms which have been refined over decades.

It is noteworthy that to the extent that EW systems are capable of disrupting communications systems of the adversary's remotely piloted vehicles – the very communications that allow human control over the weapons on those unmanned vehicles – that the assurance of human control over those weapons diminishes. DARPA's Collaborative Operations in Denied Environment (CODE) is an example of a technological response to the challenges of modern EW[4]. As unmanned vehicles continue to enter the arsenals of modern states in parallel with effective EW systems, military planners will face a choice: allow fleets of remotely-piloted unmanned vehicles to become ineffective, or push some of the decision-making processes into the unmanned vehicles themselves, moving them toward lethal autonomous weapon systems[5]. Electronic warfare R&D may

[4] S. Wierzbanowski, "Collaborative Operations in Denied Environment (CODE)", DARPA.

[5] This point of view is also articulated by K.D. Atherton: "To understand autonomous weapons, think about electronic warfare", C4ISR NET, 15 November 2018.

point to a way out of this dilemma, through the development of jam-proof communications and navigation algorithms for unmanned vehicles. However, this sets up a spiral of technological racing in the EW domain that will take on increasing importance.

What is Electronic Warfare?

Military operations are enabled by data transmitted through several media, but none of these media are more important than the electromagnetic (EM) spectrum. In particular, EW refers to data propagating through the atmosphere and space between transmitting and receiving antennae and electronics. The EM spectrum includes gamma and X-rays, to visible light, and on to infrared and radio waves used for communications and radar. Most military communications systems rely on EM transmissions and most sensors that are used to detect and track targets use EM signals – the undersea environment being a major exception[6]. Remote sensors that detect objects at a distance using EM signals are central to modern military and intelligence capabilities. These may be autonomous sensors, such as space-based sensors on satellites, sensors on aircraft (manned or unmanned), sensors on ships, submarines, or ground sensors.

Military means for manipulating or using the EM signals of an adversary – electronic warfare – have developed in tandem with detection and communication measures, giving rise to technological struggle between opponents within the electromagnetic spectrum. For the US military, the definitive explanation of EW is found within the Joint Chiefs of Staff (JCS) Joint Publication 3-13 series on Information Operations[7] – of which

[6] Most practical EM waves do not propagate in the ocean, so acoustic sensors and communications are used in that environment.

[7] Joint Publication 3-13 Information Operations, 27 November 2012, Incorporating Change 1, 20 November 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

EW (Joint Publication 3-13.1) is a part[8]. The various functions of EW are placed in three categories: electronic attack, electronic protection, and electronic warfare support. Examples of EW functions include: directed energy to attack and disable personnel, facilities or equipment; actions taken to protect one's own forces from directed energy; jamming radar and communications; injecting deceptive data into radars and communications; and finding the location of and adversary's communication and radar emitters. Thus, the term "electronic warfare" encompasses powerful offensive weapons for destroying electronics and jamming GPS signals that every person relies on for safety, as well as defensive systems to protect one's own communications. Data links exist between almost any combination of dismounted soldiers, ground vehicles, satellite, aircraft, ships, land sites, submarines with near-surface antenna, etc. These links enable coordination and command and control of forces across echelons and across geographic regions.

There is concern within NATO leadership that electronic warfare capabilities have not received the attention that they need to, largely due to the fact that recent conflicts have not included EW threats. The primary use of EW in Iraq and Afghanistan was to jam the remote detonators for improvised explosive devices, and NATO's adversaries in those conflicts had little EW attack capability. An excellent summary of the NATO EW situation was recently provided by Commander Malte von Spreckelsen, Chief Policy Section, NATO Joint Electronic Warfare Core Staff:

> In the face of such limited opposition, coalition and Alliance forces could use the electromagnetic spectrum with few limitations. This enabled the uninterrupted use of the Global Positioning System (GPS) for navigation and heavy reliance on systems like the Blue Force Tracker. Friendly forces enjoyed virtually unhindered communications means for command and

[8] Joint Publication 3-13.1 Electronic Warfare, 8 February 2012, https://fas.org/irp/doddir/dod/jp3-13-1.pdf

> control. Old, valuable concepts such as radio discipline, electromagnetic signature control, and frequency hopping were less important in these environments. Therefore, over the years, the focus and devotion towards EW faded within NATO. Policies, plans, and doctrine slowly, but steadily, became outdated. EW training in forces throughout NATO lost focus and EW skills atrophied. Additionally, new, more publicly accessible capabilities like "Cyberwarfare" emerged and dragged a lot of effort, resources, and attention away from traditional EW, which was to some degree viewed as the purview of high-end militaries and a threat that had faded with the demise of the Soviet Union[9].

Indeed, cyberwarfare has become a critical element of military communications, and has the additional characteristic that every individual in modern societies are connected to the internet and is influenced by the cognitive impact of social media interfaces. However, military EW and EW countermeasures are an essential component in the management of conflict, as the data the flows on networks directly impact understanding of the moment-by-moment military picture.

The importance of EW has steadily grown as modern military command and control has emphasized connectivity through all echelons. The United States led the way in emphasizing Network-Centric Warfare since the 1990s[10]. After the end of the Cold War, and through the period of relative US dominance in controlling worldwide communications in air, space, and then the Internet, it was natural for future-looking US military technologists to envision a world in which all levels of military operations had full access to all data all the time. However, as the vulnerabilities of the Internet-linked data flows became more apparent, the risks of corrupted data, deceptive data, or not data at all became clear.

---

[9] Commander M. von Spreckelsen, NATO Joint Electronic Warfare Core Staff, "Electronic Warfare – The Forgotten Discipline", Joint Air Power Competence Center.

[10] A.K. Cebrowski and J.J. Garstka, "Network Centric Warfare: Its Origin and Future", Proceedings of the Naval Institute, vol. 124, no. 1, January, 1998, pp. 28-35.

How Does Electronic Warfare Relat to Information Warfare?

To discuss information warfare, it is helpful to distinguish the information environment in military operations from the physical. The physical domains of warfare are ground, maritime, air, and space. Platforms (tanks, ships, aircraft, satellites) as well as the warriors, sensors, and weapons they carry operate within this physical environment, and are necessarily constrained by laws of physics. The bridge between the physical domains and the information domain is data. Data is generated by sensors, people, and computer hardware. For the purposes of this analysis, the physical elements of data flow are computing systems, cables, transmitters, receivers, and other objects that enable the flow of data[11]. Data is stored on physical devices and transmitted through the physical world: as electrical signals, light signals in fiber optic cables, and electromagnetic waves through air and space. Data transmission and reception are themselves constrained by physics.

Information, on the other hand, is related to cognitive processes such as inference and decision-making. Information is carried by data, but is not data itself: information has to be extracted from data, interpreted, and used in the context of making an inference about the state of the world, and making a decision based on inference[12]. The US Joint Chiefs of Staff have

[11] From JP 3-13, the description is "The physical dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries".

[12] Quoting from a standard graduate textbook on information theory, "The concept of information is too broad to be captured by a single definition". T. Cover

established some useful definitions and conceptual distinctions in Joint Publication 3-13 Information Operations:

> The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive[13].

The cognitive dimension is clearly called out by JCS Doctrine as the most important of the three dimensions.

> The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Defining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects. As such, this dimension constitutes the most important component of the information environment[14].

EW seeks to disrupt the physical means of data flow in order to impact the cognitive abilities of the adversary[15]. Electronic warfare is the physical part of a battle to degrade the adversary's command and control of their forces by disrupting data.

---

and J. Thomas, *Elements of Information Theory*, p. 13.

[13] Joint Publication 3-13, p. I-1…, cit.

[14] Ibid., p. I-3.

[15] The JP 3-13 also defines an "information dimension" of the "information environment", but that distinction will not be used here. It is described as follows: "The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information".

Algorithms are, by definition, automated means of manipulating data, and sophisticated signal processing algorithms are already at the heart of EW systems. Is there something special about the new modern AI algorithms that might significantly change this military function?

How Might Modern AI Algorithms Be Applied to EW?

Radars, navigation systems, and radio communications systems have been carefully designed over the decades to provide the maximum information and range. Even in the absence of EW, electromagnetic waves propagating through the atmosphere and space are disturbed by many effects. This has led designers to craft specialized signal patterns for communications, navigation, and radar signals that are well known, and tend to preserve the information content of the signal. Experts in signal processing can therefore develop highly effective algorithms using expert knowledge of how electronic communications systems are designed. In attempting to apply modern AI algorithms to the field of signal processing, the deep neural network learning-based algorithms must therefore compete against a mature field. An expert in the fields of signal processing as well as deep learning methods put it this way:

> Communications is a field of rich expert knowledge about how to model channels of different types, compensate for various hardware imperfections, and design optimal signaling and detection schemes that ensure a reliable transfer of data. As such, it is a complex and mature engineering field with many distinct areas of investigation which have all seen diminishing returns with regards to performance improvements, in particular on the physical layer. Because of this, there is a high bar of performance over which any machine learning (ML) or deep learning (DL) based approach must pass in order to provide tangible new benefits. In domains such as computer vision and natural language processing, DL shines because it is difficult to characterize real

> world images or language with rigid mathematical models. For example, while it is an almost impossible task to write a robust algorithm for detection of handwritten digits or objects in images, it is almost trivial today to implement DL algorithms that learn to accomplish this task beyond human levels of accuracy. In communications, on the other hand, we can design transmit signals that enable straightforward algorithms for symbol detection for a variety of channel and system models (e.g., detection of a constellation symbol in additive white Gaussian noise (AWGN)). Thus, as long as such models sufficiently capture real effects, we do not expect DL to yield significant improvements on the physical layer[16].

The above quote captures a very important idea in assessing how modern AI algorithms might affect military and intelligence systems in general. Current algorithms at the core of most modern military systems usually derive from well-founded theory based in mathematics and its sub-fields of probability, statistics, optimization, as well as decades of work in computer science. There is an enormous literature and experience base of applications of this theory – combined with clever heuristic thinking – that current military systems are based on. In each particular application where we think about the impact of modern AI algorithms, there will almost always be a range of alternative algorithms that have been crafted for the particular problem, integrated within tightly-designed systems, and operated successfully.

In order to forecast the extent to which modern AI algorithms might be incorporated into intelligence or military systems, including EW, it is critical to assess the data associated with these systems when they are in use. Modern AI algorithms used for classification of signals, such as deep neural networks, would require very large amounts of well-labeled signal data for parameter optimization prior to implementation. While this is

[16] T. O'Shea, *An Introduction to Deep Learning for the Physical Layer*, arXiv:1702.00832v2 [cs.IT], 11 Jul 2017. The author goes on to describe how applying modern AI algorithms to signal data can provide useful insights.

certainly possible, the modern EW environment is characterized by very agile systems, that can adapt and change. To the extent that a deep neural network is trained on less than the full range of possible data it might encounter, its performance will be uncertain.

Deep reinforcement learning (deep RL) algorithms might appear to be more readily adaptable to the EW problem, but in this case, the parameter optimization data is built up over very large numbers of interactions with the "adversary" system, with the introduction of appropriate reward signals. Unlike training a deep RL algorithm to play the game Go, or StarCraft II, in which the adversary plays by consistent rules millions of time, military EW does not allow for long, repeated engagements with fixed rules. There are cases of adversaries adapting rapidly to sophisticated EW by shifting tactics to different parts of the EM spectrum[17].

Nonetheless, it is very possible that there will be particular applications for military systems in which the attributes of modern AI algorithms will demonstrate improvements in the future. It is worthwhile, then to survey some of the recent international technical journals to assess some research directions pertinent to AI and EW.

Modern radar, communications, and EW signal processing developments have developed a common theme based on the concept of adaptation of the system to information gained from the environment. One of the prominent themes in this feedback-based view is espoused by Simon Haykin[18]. This research

---

[17] "As one example to illustrate the conundrum faced by the U.S., [the Joint-Improvised Threat Defeat Organization] spent $2.3 billion to develop an electronic signal jamming device to stop IED triggers that use two-way radios or garage door openers. In response, the insurgents switched to laser trigger devices, thereby negating the investment", R. Mordfin, *Insurgents are Learning to be More Effective on the Battlefield*, The University of Chicago, Harris Public Policy, 7 February 2018.

[18] S. Haykin, "Cognitive Radar: A Way of the Future", *IEEE Signal Processing Magazine*, January 2006, pp. 30-40. S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications", *IEEE Journal on Selected Areas in Communications*, vol.

represents only one of many active themes in modern research that is not related to deep neural network-based algorithms[19]. However, researchers have recently been applying deep neural networks to selected sub-problems within these EW domains. Some examples include: application of convolutional neural networks for improving direction-of-arrival estimates for EW systems[20], using deep neural networks to classify radar pulses based on images created by time-frequency images of the radar signals[21], competitive deep reinforcement learning-based methods for adapting ones' own communications to an EW environment where the opponent is using adaptive jamming[22], and other approaches based on applications of a wide array of algorithms to the automated confrontation between electronic systems.

A review of the technical literature from the US and China indicate that researchers are experimenting with application of modern AI algorithms to particular functions within the overall EW signal processing chain. There is a growing body of technical literature that is showing incremental improvements in the overall capabilities of EW processing chains. This is of course exactly what we would expect from any new technology as it is applied within complex systems with many stages and components. To date, however, there is no evidence of a major improvement in EW system capability driven by the introduction of deep neural networks or deep reinforcement learning. The

---

23, no. 2, February 2005, pp. 201-220.

[19] K. Bell, et. al. "Cognitive Radar Framework for Target Detection and Tracking", *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 8, December 2015.

[20] A. Elbir et al., "Cognitive Radar Antenna Selection via Deep Learning", *IET Research Journals*, pp. 1-10. Accessed via arXiv:1802.09736v3 [eess.SP], 4 February 2019.

[21] QU Zhiyu et. al., "Radar Signal Intra-pulse Modulation Recognition Based on Convolutional Denoising Autoencoder and Deep Convolutional Neural Network", *IEEE Access*, vol. 7, 2019, pp. 112339-112347.

[22] LI Yangyang et. al., "On the Performance of Deep Reinforcement Learning-Based Anti-jamming Method Confronting Intelligent Jammer", *MDPI Applied Sciences* (China), 2019, vol. 9, p. 1361.

fact that research in China is now applying modern AI algorithms to EW may be driven in part the incentives and funding available associated with the Chinese government's artificial intelligence goals[23].

Russia's Focus on Electronic Warfare

Russian military thinkers have long understood and theorized about the importance of information in all aspects of military decisions and operations[24]. Domains of military competition that have in the past been considered separately, such as space, electronic warfare, networked operations, and cyber operations are increasingly viewed as a seamless operational domain. The term "hybrid warfare – the use of proxies, disinformation, and other measures short of war"[25] has been associated with articles and speeches of General Valery Gerasimov, and termed the "Gerasimov Doctrine". Eugene Rumer of the Carnegie Institution places Gerasimov's statements into a longer historical context, articulated first by former foreign and prime ministry Yevgeny Primakov[26].

> Russia's military posture vis-à-vis NATO appears to be a calculated mix of hard power and hybrid warfare designed to deny NATO its advantages – the numerical superiority of allied militaries, technological superiority, an edge in air power, economic potential, and a long record of political cohesion and commitment to shared principles. Russia's posture suggests a country

[23] For a coherent explanation of how these incentives to work on AI-related matters operate within China, see M. Sheehan, "How China's Massive AI Plan Actually Works", Macro Polo, Chicago, IL, Paulsen Institute, 12 February 2018.

[24] V.V. Druzhinin and D.S. Kontorov, *Concept, Algorithm, Decision (A Soviet View)*, Chapter 3, Moscow, US Air Force, 1972.

[25] N. Ng and E. Rumer, *The West Fears Russia's Hybrid Warfare. They're missing the Bigger Picture*, Commentary, Washington DC, Carnegie Endowment for International Peace, 3 July 2019.

[26] E. Rumer, *The Primakov (Not Gerasimov) Doctrine in Action*, Washington DC, Carnegie Endowment for International Peace, 5 June 2019.

> that is realistic about its limited prospects to achieving superiority and is instead focused on denying its opponent's advantages – consistent with Primakov's vision[27].

For Russia, EW is a low-cost, low-risk means to inject uncertainty into NATO, as well as a means of assuring its own command and control in the face of NATO's technical superiority. Russia has been updating their EW systems, and has a recent history of using them in eastern Ukraine and Syria. Indeed, these uses of EW have provided NATO with insights on Russian tactics and capabilities[28]. Russia's response to superior NATO capabilities[29] has been significant, but the offensive capabilities of Russian EW have also been exaggerated. A great deal of Russia's investment and deployment of EW capabilities has been to defend and protect their own communications links. The most recent Russian uses in Syria were most likely focused on force and base protection[30]. On the offensive side, EW remains a very cost-effective counter to NATO capabilities that rely on communications, sensor networks, and targeting data connected from sensors to weapon systems[31].

How does the steady buildup of EW capabilities by Russia impact on NATO's ability to deter adventurism on a small scale? This can be addressed in the context of the most likely scenario in which Russia might attempt some incursion in NATO. In the book, *The Senkaku Paradox*, Michael O'Hanlon establishes some key scenarios that help define the most likely type of scenarios between great powers for armed conflict. Briefly,

---

[27] Ibid., p. 15.

[28] J. Kjellén, *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defense Research Agency, FOI-R – 4625 – SE, September 2018.

[29] J. Kjellén, *A More Nuanced View of Russian Electronic Warfare*, Swedish Defense Research Agency, 6 March 2019.

[30] R. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging Russia in the Electromagnetic Spectrum*, International Centre for Defence and Security, Republic of Estonia Ministry of Defence, September 2017, p. 21.

[31] Ibid.

O'Hanlon's argument is that major military engagements between Russia and the US would be unlikely. The more likely scenario would be an incursion by the Russians in a small part of one of the Baltic states[32]. According to Roger McDermott, author of a detailed report on Russian EW capabilities: "If conflict with Russia ever erupts on NATO's Eastern Flank, the first sign of activity will be in the EMS – and in this spectrum the initiative and advantage will be determined"[33].

Electronic warfare is[34] a critical part of conflict throughout its stages, just as military command, control, communications and intelligence are. Prior to troop movements, artillery, missile and other physical attacks, EW is a precursor to hostilities. EW attacks have been performed by Russia in Crimea, Donbass, and Syria prior to and during physical hostilities. The recent Russian demonstration of GPS signal jamming during NATO's Trident Juncture exercises in northern Norway[35]. The EW attacks against GPS, which is a core technology associated with precision guided munitions (PGMs), may be an attempt to signal Russian willingness to try to neutralize one of NATO's key technological strengths. Or it may be simply a low-risk means to try to undermine NATO confidence in its capabilities. To ensure that NATO's command and control, precision-guided munitions, radar, and communications are demonstrably solid, there is no alternative than to engage in a concerted effort to maintain control of the electromagnetic environment.

It does not appear that Russia could make sudden strides in EW by applying modern AI algorithms. In the first place, modern AI algorithms are not easily substituted into the integrated, mature architectures of modern EW systems, as I have already argued. In the second place, Russia has not demonstrated the

---

[32] M.E. O'Hanlon, *The Senkaku Paradox: Risking Great Power War over Small Stakes*, Washington DC, Brookings Institution Press, Chapter 2, 2019.

[33] R. McDermott (2017), p. 28.

[34] Commander M. von Spreckelsen…, cit.

[35] B. Tigner, *Norway says Russia jammed GPS during major NATO exercise*, New Atlanticist/Atlantic Council, 15 November 2018.

investments in modern AI algorithms that the US and China have, and those two countries have not fielded AI-based EW systems. In the field of modern AI algorithm R&D, Russia has established a few innovation centers[36], and certainly starts from an historic tradition of strong advanced education and research in mathematics and related disciplines. However, Russia appears to have difficulty maintaining top talent[37], and there is has not been a long-term push from the very top for taking a leading role in modern AI algorithm development, in particular as compared with China's repeated emphasis over the past few years. Taking all this into account, there is unlikely to be a sudden, significant improvement in AI-enabled EW from Russia that would provide an overwhelming advantage to Russia in the electromagnetic spectrum[38]. More likely, Russia will continue to make progress in improving the responsiveness and speed of their EW systems.

[36] A. Bateman, "Russia's Quest to Lead the World in AI is Doomed", *Defense One*, 19 June 2019.

[37] Ibid.

[38] Although it is beyond the scope of this paper, I would argue for similar reasons that we are unlikely to see a sudden significant improvement in Russian command and control through the application of modern AI algorithms, as I define them here. The functions required in military command and control include: fusing data, estimating the locations, status, movements, etc. of hostile forces as well as own forces; forecasting this "tactical picture"; allocating resources optimally to counter threats; planning routes subject to tactical, environmental and physical constraints; and continually updating this process as new data arrives. Algorithmic solutions to this wide variety of tasks are similarly varied, and no single type of algorithm appears the best choice to integrate all these functions. Russian announcements of integrated command and control systems, (R. McDermott, "Moscow Showcases Breakthrough in Automated Command and Control", *Eurasia Daily Monitor*, vol. 16, no. 164, 20 November 2019) should be taken very seriously as advances in algorithms and integration, but not as evidence of AI breakthroughs per se.

Conclusion

We have seen that Russia has an interest in EW to protect its own forces and to disrupt its adversaries in military crises as well as full scale military operations, and has been investing and training its capabilities. It is not an EW superpower, and many of the Russian capabilities are defensive in nature. We have also seen that EW technology is inherently automated due to the rapid speed of signal generation, propagation, and processing. Advances in digital technology have made it possible for modern militaries to develop highly flexible and adaptable electronic systems with feedback that enable rapid adaptation to the electromagnetic environment. While modern AI algorithms are being applied to EW through research and development, there is no indication of any kind of breakthrough in the foreseeable future.

Russia will be capable of continuing developments in EW, and may introduce some elements of deep neural networks for signal recognition. However, Russia is unlikely to develop any kind of decisive lead in this area as long as the US and its NATO allies continue to invest in the EW countermeasures to the measures that are developed.

The temptation to disrupt communications over the internet as well as in the electromagnetic environment will remain a strong for Russia if it attempts further incursions. According to the National Defense Strategy Commission report:

> Electronic warfare capabilities will be critical in any future conflict, especially those against major-power rivals. U.S. competitors have invested heavily in electronic warfare as a way of neutralizing U.S. advantages and weakening America's ability to project power. Recommendation: DOD must enhance its electronic warfare capacity and capability to overcome adversary electronic warfare investments, and to degrade and defeat anti-access/area denial capabilities and adversary command, control, and communications architectures[39].

[39] National Defense Strategy Commission, *Providing for the Common Defense. The*

Finally, there is paradox of effective US/NATO electronic warfare capability that goes to the core of an extensive debate about modern AI algorithms and autonomous weapons. The ability of robust EW to control, deny, and even manipulate radio and other EM transmissions and sensors will interfere with human control over remote weapons. In a highly contested EW environment, human control over unmanned platforms, sensors, and in particular weapons becomes unreliable. This uncertainty will create a technological imperative for unmanned systems to become autonomous. Balancing the need for robust EW for warfighting, and avoiding a rapid drive toward lethal autonomy will be a complex debate.

Assessment and Recommendations of the National Defense Strategy Commission, 2018, p. 68.