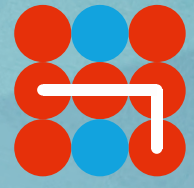
COI STRATEGY & DEFENCE

Hybrid CoE Working Paper 6

MARCH 2020

Artificial Intelligence – A key enabler of hybrid warfare

RALPH THIELE



Hybrid CoE

Hybrid CoE Working Paper 6

Artificial Intelligence – A key enabler of hybrid warfare

RALPH THIELE

Hybrid CoE Working Papers are medium-length papers covering work in progress. The aim of these publications is to share ideas and thoughts, as well as to present an analysis of events that are important from the point of view of hybrid threats. Some papers issue recommendations. They cover a wide range of important topics relating to our constantly evolving security environment. Working papers are not peer reviewed.

COI Strategy & Defence is focusing on hybrid warfare, related strategies and resulting implications for security policy, military and defence. It aims at discovering the essence and nature of hybrid warfare as well as the logic and pattern of hybrid strategies in order to develop an analytical framework for the assessment of current and future hybrid warfare situations and their practical implication. COI S&D follows an interdisciplinary academic based approach, hereby combining empirical evidence with the theory of war and strategy. Overarching objective is to contribute to the education of common and comprehensive judgment of Participants, EU and NATO as a precondition for joint and comprehensive action in defense and response.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-31-1
ISSN 2670-160X

March 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

Preface

> *"It is imperative to keep an eye on new technologies and their potential for future development and disruption, and to analyse these developments with regard to their relevance in a hybrid warfare context. Their relationships must be understood before their implications become manifest in the context of hybrid warfare. In this regard, the technological revolution requires orchestration. This should not be left primarily to potential hybrid challengers."* [1]

Hybrid warfare/conflict is nothing new in essence. However, technological trends suggest that the portfolio of hybrid hazards will rapidly expand.[2] With their disruptive potential, they open up new avenues for violence, as well as for the use of force in a hybrid warfare/conflict environment.[3] New technologies have a catalytic effect on hybrid methods and tools. They improve the starting conditions for hybrid action, expand the arsenal of hybrid players and thus help to increase the reach of their activities as well as their prospects of success. Today, new technologies provide a way to achieve political goals in the grey area of various interfaces, such as between war and peace. At the same time, however, new technological developments may offer options to better identify, understand, defend against and counter hybrid attacks. Therefore it is important for political, civilian and military leaders and decision-makers, as well as industry and academia, to develop a comprehensive understanding of the implications of new technologies in a hybrid warfare/conflict context.

With this in mind, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and its Community of Interest for Strategy and Defence (COI S&D) have initiated the **Hybrid Warfare: Future & Technologies (HYFUTEC)** project, aimed at assessing and enhancing understanding of the disruptive potential of new technologies in the context of hybrid warfare/conflict. Within its broad future & technology horizon scanning, the project has identified 19 technological trends with urgent and profound implications in the context of hybrid scenarios.[4]

HYFUTEC Technology Papers are designed to provide insights into selected technological trends and to improve understanding of their implications for hybrid warfare/conflict. In this vein, the papers intend to raise awareness, inform debate and contribute to the education of judgment within participating states, the EU and NATO in order to identify ways to deal with resulting threats and challenges effectively. This **HYFUTEC Technology Paper No. 1** concentrates on **artificial intelligence** as a catalyst and key enabler of **hybrid warfare**.

Johann Schmid
Director, Community of Interest for Strategy and Defence

Community of Interest Strategy & Defence (COI S&D)
HYFUTEC Hybrid Warfare: Future & Technologies

1 Johann Schmid and Ralph Thiele, "Hybrid Warfare – Orchestrating the Technology Revolution". In Robert Ondrejcsak & Tyler H. Lippert (Eds.), *STRATPOL. NATO at 70: Outline of the Alliance today and tomorrow*, Special Edition of Panorama of Global Security Environment 2019, Bratislava December 2019, 211–225, https://www.stratpol.sk/wp-content/uploads/2019/12/panorama_2019_ebook.pdf.
2 Ibid.
3 For a conceptual understanding of hybrid warfare, see Schmid, J. COI S&D Conception Paper: Hybrid Warfare – a very short introduction (Helsinki, May 2019), ISBN: 978-952-7282-20-5.
4 See Thiele, R. HYFUTEC Inspiration Paper No. 2 (updated): Hybrid Warfare – Future & Technologies Horizon Scan & Assessment (Sept 2019).

Data and algorithms

Artificial intelligence (AI) has emerged as **one of the most important technologies for any nation when it comes** to assisting human decision-making. Driven by data and algorithms, AI will affect almost every aspect of life, from developing more effective ways to educate people to changing the way they earn money, to defending against attacks in virtually any domain.[5] However, in the AI subfield of machine learning, AI results are mainly directed by training data. At present, trained algorithms act as black boxes. These **algorithms can, as such, be characterized by excellence or by errors, or be deliberately manipulated**. It will be crucial to ensure that the development and integration steps of AI are openly comprehensible and verifiable.

AI is one of the **key technologies of digitalization**.[6] Today, digitalization puts traditional economic sectors under pressure to transform. This pressure will intensify as new added value comes from utilizing data[7] in combination with AI systems. The technology for big data and AI is currently developing at a tremendous pace, which has major potential implications for business and industry, politics and society, **including a range of military applications.**

AI will increase the complexity of warfare. The effects of AI and machine learning in the military and the future of warfare can best be understood as a cluster of enabling technologies that will be applied to most aspects of the military sphere.[8] In hybrid warfare, it will significantly contribute to pushing the envelope in grey zones.

AI offers a myriad of possibilities for complementing individuals with superior capabilities in this field, thus providing a suite of technologies and applications that can help militaries resolve concrete challenges across a broad range of missions. These include higher cost-efficiency, reducing the human workload, and improved cyber capabilities in particular. AI-driven **autonomous tools will become 'useful teammates' for human beings** rather than tools used by them.

> **Artificial intelligence** is an umbrella term that covers methods that aim to automate decision-making processes that traditionally require the use of human intelligence, such as recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action. *Fuelled by sensors, data digitization, and ever-increasing connectedness, AI filters, associates, prioritizes, classifies, measures, and predicts outcomes, thereby enabling better-informed, data-driven decisions.*

In hybrid warfare, AI technology will drive an evolution whereby dominance in information and understanding can prove decisive by increasing the speed, precision, and efficacy with which information is wielded and made actionable. In hybrid conflicts, AI will enable group behaviours to be mimicked, influenced, and altered, thereby shaping the social and economic effects of hybrid conflict. Its potential for simplifying complex processes and making them more efficient makes AI a key priority for armed forces and intelligence services in dealing with hybrid warfare contingencies. For example, as facial recognition, biometrics, and signature recognition technologies become ubiquitous, it will become much harder to hide soldiers, proxies or their equipment. With a far more extensive AI-enabled intelligence-gathering, processing, and exploitation apparatus, a nation-state can do much to fight against hybrid insurgents.

Machine learning

Machine learning plays a particular role in AI. Even today, defence and security organizations apply machine learning and machine vision software

5 Eric Schmidt, Robert Work, "In Search of Ideas: The National Security Commission on Artificial Intelligence Wants You", War on the Rocks, July 18, 2019, https://warontherocks.com/2019/07/in-search-of-ideas-the-national-security-commission-on-artificial-intelligence-wants-you/.
6 Dietmar Harhoff, Stefan Heumann, Nicola Berlin Jentzsch and Philippe Lorenz, "Outline for a German Strategy for Artificial Intelligence", July 2018, 6, https://www.ip.mpg.de/fileadmin/ipmpg/content/aktuelles/Outline_for_a_German_Artificial_Intelligence_Strategy.pdf.
7 Dr. Raphael Paschke, HYFUTEC study input.
8 Niklas Masuhr, "AI in Military Enabling Applications", CSS Analyses in Security Policy No. 251, October 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf.

Zapp2Photo / Shutterstock.com

to permanently update *knowledge* about the operational environment. New capabilities have emerged with the introduction of deep learning combined with the free availability of large amounts of data and increasing processing ability in order to enhance force protection, sustainment, and logistics, thereby reducing the political costs of protracted military engagements.

The US military, for example, already uses AI in the context of intelligence, surveillance and reconnaissance platforms and sensors. This enables it to make professional use of unstructured data sources, including full-motion video or comparable approaches to the automated exploitation of audio and text. In this way, reaction times can be dramatically reduced without compromising precision. At the same time, the AI-driven integration of real-time data provides for a better understanding of behavioural patterns, structures and processes to include technological relationships.[9]

AI-based image processing can identify and categorize enormous quantities of surveillance video/images captured by unmanned aerial vehicles (UAVs), for example. The algorithm behind the software is not only able to identify relevant objects and anomalies in the video/image material for which it has been trained, but it also alerts analysts to a human operator and points them to the marked objects.[10]

AI technologies can be:

- Employed to find the best assignment of scarce resources to targets. Optimization algorithms can help identify key points in time or space that are worth monitoring. If real-time target tracking is possible, new options for target reassignment can be proposed immediately.
- Used to determine in advance which measures promise the best possible success in the context of repairing damage caused by enemy actions. Algorithms can simultaneously and

9 Daniel Egel, Eric Robinson, Charles T. Cleveland, Christopher Oates, "AI and Irregular Warfare: An Evolution, Not a Revolution", War on the Rocks, October 31, 2019, https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/.
10 Marcus Roth, "Artificial Intelligence in the Military – an Overview of Capabilities", February 22, 2019, https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/.

quasi automatically show several options for action. Virtual analysts support human analysts in capturing complex facts.

- Designed to help human analysts select and determine targets. Pattern recognition algorithms allow the processing of large amounts of information. Reasoning algorithms combine available information into a well-structured, coherent proposal.[11]

Machine learning facilitates greater precision and can complement human assessments and predictions. In principle, it can vastly accelerate decision-making processes by enabling decision-makers to understand and analyze situations much more swiftly than before. Up to now, finding ways to ensure the absence of biases or analytical errors in machine learning has been a matter of intensive research. It is difficult to judge from an external viewpoint how precise or trustworthy an AI-generated assessment will really be in a different environment or situation. Consequently, it must not acquire too much authority in decisions at the political-strategic level. Who exactly has access to AI, and is thus in a position to contextualize it and interpret its results will, therefore, be of critical importance.[12]

Predictive

Predictive analytics is an important feature of AI that renders information actionable.[13] For example, the US Air Force has introduced "predictive logistics" for several fleets of aircraft types. It engages artificial intelligence to identify the need for repair and maintenance tasks. This makes it possible to allocate the necessary work to individual aircraft in a much more targeted manner.[14]

AI can pool vast amounts of data, such as message data, state identity data, charts, spreadsheets, telephone records, and documents within a state database, including filed police reports, network data, sensor data, and full motion video. This pooling of data helps to detect unseen patterns, and aids in criminal, terrorist or hybrid warfare investigations. Pooling vast quantities of data enables algorithms to generate predictions independently in relation to as yet unknown data and, ideally, to autonomously improve their own performance over time. This will prove particularly valuable in hybrid contingencies when uncovering the opponent's shifting/altering centres of gravity is required.

Even today, some of these software algorithms are capable of surpassing human talent in their respective areas. For example, by correlating information, predictive analysis models may provide support in the search for signs of planned criminal or terrorist attacks, such as the purchase of a weapon or bomb-making material. In this way, they would contribute significantly to preventing the execution of criminal or terroristic plans from the outset.[15] Predictive analytics software can also make a prediction about possible suspects of a hybrid offence based on various environmental factors and past record data.

Multiple applications

In border security, artificial intelligence enables large areas to be monitored and, if necessary, relevant objects to be detected and marked using compact, lightweight radar systems installed, for example, in drones. This significantly improves the situation overview along unclear borders. AI-supported software supports the assessment of travellers using standard Advance Passenger Information and Passenger Name Record. This helps to match data at security and border checkpoints. It may also improve the speed at which governmental agencies can generate predictive models of risk for incoming travellers.[16]

11 Philip Kerbusch, Bas Keijser, Selmar Smit, "Roles of AI and Simulation for Military Decision Making", TNO 2018, https://pdfs.semanticscholar.org/885b/182170db541d48ca7f0380bc0447ce56c9ae.pdf.
12 Fabien Merz, "AI in Military Enabling Applications", CSS Analyses in Security Policy, No. 251, October 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf.
13 Millicent Abadicio, "AI at the US Department of Homeland Security – Current Projects", April 16, 2019, https://emerj.com/ai-sector-overviews/artificial-intelligence-homeland-security/.
14 Niklas Masuhr, "AI in Military Enabling Applications".
15 Marcus Roth, "Artificial Intelligence in the Military".
16 Millicent Abadicio, "AI at the US Department of Homeland Security – Current Projects".

In personnel development, training and organization, likely AI benefits include:

- personalized training, fair assessments and promotions;
- more realistic exercises, manoeuvres and simulations, particularly in combination with VR techniques;
- credible simulations of future technologies and their applications.

AI can be used here to create and continuously update personalized curricula. Depending on the student's learning style, he or she can decide to learn via mathematical formulas, visualizations or sports analogies. AI could also help to make staffing and promotions more objective, as it helps to assess candidates holistically.[17]

With AI, real and virtual exercises can be made much more realistic and demanding. In this way, management personnel can be better prepared for complex operations. This is particularly important when it comes to hybrid warfare scenarios, where decision-makers can learn to act flexibly and dynamically against opponents through AI-supported modelling and simulation. Particularly when combined with rapid developments in augmented reality, artificial intelligence will significantly improve realism in tactical training, forming the basis for operational concepts to be further developed. In addition, through highly complex simulations, AI can help to determine the best ways of using new technologies and make suggestions on how best to integrate them into existing systems.[18]

Operational benefits

NATO and the EU – as well as hybrid aggressors – can expect **vast and diverse operational benefits from AI**.[19] These include:

- more efficient processing of data from different sources, duly promoting superior decision-making;
- a reduction in administrative and staff work through predictive logistics;
- improved ISR capabilities and risk reduction through autonomous systems.

Developments point in particular to further improvements in the performance of unmanned systems and to optimizing the data and information-processing capability within military C4I systems. As the number of platforms, and thus the number of sensors on the battlefield, has increased – and the sensors themselves have become increasingly sophisticated technologically, capturing all spectra – the demands for their evaluation have also increased.[20] Information overload has become a real problem. AI-driven intelligent and automated evaluation provides for evaluating and processing all relevant data and applying these in a timely and effective manner.

Generally, it can be expected that AI will help the armed forces to collect, categorize, analyze and evaluate data much more quickly and efficiently than is currently possible. **Its potential to simplify and streamline processes has made the introduction and use of AI a key priority for armed forces.** AI-enabled systems are multi-tasking capable and can collect, categorize and transmit data and signals, images and video collected by drones according to the requirements of multiple users.[21]

AI will benefit military applications from the strategic to the tactical level, particularly by analyzing big data, optimizing processes, and supporting strategic and operational planning, vastly accelerating **decision-making** processes and achieving **multidomain situational awareness** using any available data source in a structured way.

At the political-strategic level, AI-enabled systems could support complex simulations relating to ongoing crises in real time in particular, with a view to scrutinizing hybrid opponents that are thinking and acting in complex and dynamic ways.

At the operational level, the possibility to feed less structured but greater volume into C4I systems can enable faster and better decisions, as AI can ensure that decision-makers are only supplied

17 Niklas Masuhr, "AI in Military Enabling Applications".
18 Ibid.
19 Andy J. Fawkes, Martin Menzel, "The Future Role of Artificial Intelligence – Military Opportunities and Challenges", *JAPCC Journal 27*, 2018, https://www.japcc.org/the-future-role-of-artificial-intelligence/.
20 PWC, "Nations will spar over AI", 2018 AI predictions, https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions/ai-arms-race.html.
21 Niklas Masuhr, "AI in Military Enabling Applications".

with relevant information without being distracted by complex computer interfaces.

At the tactical level, AI may provide improved and faster situational awareness for the crews of combat vehicles. It can automate threat detection by recognizing persons or object types, but also by recognizing potentially dangerous behaviours. Conversely, the system can use AI to record information in the form of natural speech, digitize it, and make it available to the system in a pre-processed form, thereby significantly increasing efficiency.[22] AI-enabled technologies will likely ease logistical burdens, ensure military-technological superiority and enhance combat reaction times.[23]

Competitive

Current AI strategies focus on the development of a global competitive AI ecosystem characterized by strong networks between science and economic actors – encompassing the full spectrum from start-ups to big companies – as well as society at large. Innovations arise in particular from close exchanges and collaboration between researchers, developers, universities, companies, investors and start-ups.

Clearly, **defence technology is driven by civil technology** in this field today. Private markets drive developments. The dual-use character of AI, namely the simultaneous suitability of technologies for civil and military purposes, makes it imperative for governments to seek a close exchange with industry and research. The armed forces must try to adapt the disruptive, rapidly changing civil technology as quickly and as efficiently as possible in order not to lag behind. This requires careful calibration as to the extent to which internal processes, organizational structures and doctrines that have evolved over a long period of time could and should be replaced. Alongside the technological and organizational components, the legal, ethical and, most importantly, the political context must also be taken into account.

As NATO and the European Union advance their strategies and concepts, both civilian and military decision-makers need to explicitly address the role of AI in hybrid warfare. This should include an assessment of where existing training, tactics, techniques, and procedures allow for the effective use of AI-enabled systems and capabilities. Most importantly, defence officials need a comprehensive view of AI-related initiatives across departments, agencies and international organizations. This is required in order to better anticipate the effects of fielding different AI-enabled systems and capabilities with a view to tactical, operational, and strategic objectives.[24]

Vulnerable

Since AI-capable weapons are relatively easy and inexpensive to obtain, they will also be accessible to non-state actors and proxies. Some states could even deliberately provide these capabilities, as they have done with conventional weapons to date.[25]

Furthermore, due to the open availability of most developments of AI and the ease of implementation, technologies and the capability to adapt them in the military context will be available to any opponent, sooner or later. These AI capabilities will constitute significant threats to those parts of Western economies, infrastructure, and populations that are most vulnerable to disruption, subversion and further hybrid threats. As opponents will likely use all available tools in a well-orchestrated, synchronized manner, the response must also be comprehensive and well-orchestrated.[26]

With the rise of the "Internet of Things" (IoT) and our increasingly algorithmic and big- data-driven processes, advanced societies are becoming perilously dependent on networks of information, and data-gathering and exchange for communication, analysis and decision-making purposes. As a recent Rand study highlighted: *"Aggressors will increasingly have the opportunity not merely to spread disinformation or favorable narratives or to damage*

22 Marcus Roth, "Artificial Intelligence in the Military".
23 Michael C. Horowitz, "The Promise and Peril of Military Applications of Artificial Intelligence", *Bulletin of the Atomic Scientists*, April 23, 2018, https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/.
24 Egel et al., "AI and Irregular Warfare".
25 Ibid.
26 Aaron Mehta, "AI makes Mattis question 'fundamental' beliefs about war", C4ISRNET, February 17, 2018, https://www.c4isrnet.com/intel-geoint/2018/02/17/ai-makes-mattis-question-fundamental-beliefs-about-war/.

physical infrastructure, but to skew and damage the functioning of the massive databases, algorithms and networks of computerized or computer-dependent things on which modern societies will utterly depend."[27] Actually, a shift from front-end manipulation (messages, narratives, stories etc.) towards back-end manipulation (data, algorithms, networks etc.) may occur.[28]

AI in its present shape is still a fairly vulnerable technology – susceptible to training data poisoning and manipulation by adversarial actors. It may well fail when confronted with tasks or environments different from those it was trained for; it may behave unpredictably due to its opaque algorithms.[29]

As Margarita Konaev has pointed out: "*Another risk is that of the speed of engagement between autonomous systems fighting each other. AI may subsequently push humans out of the loop in life-and-death decisions."*[30] The implications of both gradual and disruptive technological innovations may well change civil-military relations, political power, and the way wars are waged. Consequently, while technology is evolving, ethical considerations must be addressed from the very outset in order to be integrated into further developments accordingly. At present, there is an investment asymmetry between mission performance and oversight in AI.[31]

AI takeaways

- *One of the key enabling technologies of digitalization.*
- *A priority for armed forces as well as intelligence.*
- *Machine learning and algorithms have a particular role.*
- *Predictive analytics is an important particular feature.*
- *Upcoming challenges and opportunities cross-cut existing technologies across all military & intelligence branches.*
- *Likely beneficial to C4I, cyber operations, decision-making, electronic warfare, autonomous systems & swarms, extended reality as well as to logistics, operational tempo & targeting, predictions & risk management, simulation and training, and situational awareness.*
- *Defence technology is driven by civil technology.*
- *Governments lean on commercial sector.*
- *Technological leadership of opponents may lead to unforeseen risks.*

27 Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke J. Matthews, "The emerging risk of virtual societal warfare", RAND 2019, https://pile.sdbs.cz/docs/RAND_RR2714.pdf.
28 Comment by Rick Meessen, TNO. In a recent RAND study this phenomenon has been described as *Virtual Societal Warfare: Michael Mazarr*, Ryan Bauer, Abigail Casey, Sarah Heintz, Luke Matthews, "The Emerging Risk of Virtual Societal Warfare", RAND 2019, https://www.rand.org/pubs/research_reports/RR2714.html.
29 Margarita Konaev, "With AI, We'll See Faster Fights, but Longer Wars", War on the Rocks, October 29, 2019, https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/.
30 Ibid.
31 Nathan Strout, "AI oversight", C4ISRNET, June 10, 2019, https://www.c4isrnet.com/artificial-intelligence/2019/06/10/where-is-the-investment-in-ai-oversight-asks-inspector-general/.

Recommendations

- Employ the game-changing attributes of AI as an enabler.
- Ensure that AI systems assist people and do not take autonomous decisions (Human-in-the-loop).
- Develop a coherent strategy. Institutionalize AI as a part of doctrine, strategy, and tactics.
- Carry out regular portfolio reviews of integrated and joint investments in AI.
- Establish certification processes.
- Shape AI's impact to NATO´s and the EU´s advantage.
- Prioritize AI-related research and development projects.
- Protect AI-related industrial know-how.
- Enhance collaboration and teaming across the armed forces, security and defence agencies, the private sector, and academia to develop the data culture and architecture necessary for success.
- Establish effective norms.
- Recruit, develop, retain, and enable personnel capable of leveraging AI capabilities.
- Recognize data as critical resources, continue instituting practices for their collection and curation, and increase sharing while resolving issues in protecting the data after sharing and during analysis and use.
- Make a selection of security- and defence-related data sets available to the AI community; build appropriate databases to train the tools.
- Draw on the blended skill set of data scientists, operators, and intelligence professionals.
- Develop AI employment technologically, organizationally and politically.
- Invest in oversight.
- Identify:
  - The most relevant areas for European cooperation;
  - What kind of AI military capabilities the EU member states should be ready to develop together;
  - Possible EU-NATO capability cooperation areas in AI.

Author

Colonel (R) Ralph D. Thiele is Managing Director of StratByrd Consulting, Chairman Political-Military Society, Berlin, and President EuroDefense – Germany. StratByrd Consulting, founded in 2013 in Germany, advises and implements solutions to strategy and digital transformation issues of networked security at the interface between industry and government against the backdrop of hybrid challenges. StratByrd is a freelance consulting company with a large network of science and politics, business and society, which configures itself flexibly and task oriented.


Hybrid CoE