DOI: 10.53477/2668-2001-21-37

ARTIFICIAL INTELLIGENCE IN HYBRID WARFARE: A LITERATURE REVIEW AND CLASSIFICATION

Elena Șușnea[1]
"Carol I" National Defence University
Ionuț-Cosmin Buță
"Carol I" National Defence University

Abstract

Artificial intelligence contributes greatly to enhance situational awareness, providing early warning and contributing to the decision making process in the hybrid warfare context. Artificial intelligence brings a paradigm shift to "new" wars and threats, powered by increasing availability of military data and rapid progress of artificial intelligence techniques. The purpose of this paper is to identify researchers' interest in the use of "artificial intelligence" in the "hybrid warfare" environment and to establish the topics they approach. In this respect, the aim of this paper is to produce a literature review by accessing a scientific database in order to perform an analysis on how connected topics, such as: machine learning, data mining, deep learning and artificial neural network are integrated in the military domain.

Keywords: artificial intelligence; hybrid warfare; hybrid threats; decision making; machine learning; cybersecurity.

INTRODUCTION

In the last decade the rise of hybrid warfare term by describing the new type of wars produced different concepts like: hybrid threats or hybrid conflict (Glenn, 2009, 1). In the same time, the quickening progress of new technologies like artificial intelligence, machine learning, data mining, deep learning, artificial neural network, cybersecurity, and other aspects related to defense technologies represent a must which produces effects in all security and defense domains. Moreover, in the hybrid warfare context, information superiority represents a key concept used to enhance situational awareness, providing early warning and contributing to the decision making process. Avoiding or reducing unwanted consequences and preparing for an effective response to hybrid threats is based on "providing timely information that allows decision makers to analyze the data in detail and establish intervention measures" (Susnea 2013. 427-431).

This paper analyzes two emerging military topics such as "artificial intelligence" and "hybrid warfare". Through this the purpose of this paper is to produce a literature review by accessing the ProQuest Database in order to identify the articles written in the two areas mentioned above and to perform an analysis on how related topics such as: machine learning, data mining, deep learning and artificial neural network are developed in the military field.

ARTIFICIAL INTELLIGENCE

Artificial intelligence aims to build artificial minds, and thus, cares most for how systems can emulate intelligent behavior. Techniques from artificial intelligence are attracting much interest in the military field because it leads to a massive expansion in means of human capability and propose better solutions than human might in hybrid warfare conditions.

Artificial intelligence in hybrid warfare has two main branches: computer software and robotic and autonomous systems (RAS). The computer software branch includes informatics approaches

[1] Corresponding author: esusnea@yahoo.com

from expert systems, speech recognition, natural language processing to machine learning, including digital records and metadata to military decision support systems. The robotic and autonomous systems branch is best represented by “powered machine capable of executing a set of actions through direct human control, computer control, or a combination of both” (Torossian et al., 2021. 5) and the cognitive (autonomous) aspects of these machine. These systems are based on technology that supports automatic target recognition, target acquisition, unmanned aerial vehicles (UAVs), loitering weapons and so on.

Artificial intelligence technologies present a real opportunity for military integration, particularly because of the level of artificial intelligence development in fields like intelligence, surveillance, and reconnaissance (ISR), logistics, cyberspace operations, information operations and deep fakes, command and control, semiautonomous and autonomous vehicles, lethal autonomous weapon systems (LAWS). Most of the applications listed above used supervised learning algorithms like logistic regression, k-nearest neighbor, decision trees, naïve Bayesian, support vector machine. Moreover, data mining plays an important role for decision support irrespective of type of military application. The increasing ability to track, collect and analyze large amounts of data in order to extract previously unknown patterns has lead to an interest in the development of data mining algorithms which can extract useful information from these large datasets or streams of data. If data mining techniques such as clustering, decision tree and association are applied to hybrid warfare, it would help improve early warning for increased situational awareness and contribute to the decision making process.

In recent years, deep learning has become the leader in the machine learning domain. Unlike conventional machine-learning and data mining techniques, “deep learning is able to generate a very high-level data representations from massive volumes of raw data. Therefore, it has provided a solution to many real-world applications” (Pouyanfar et al., 2018. 92).

HYBRID WARFARE

To better understand the nature of future conflicts first we should define the new threats. Nowadays potential enemies “blend various approaches in war to fit them within their strategic culture, historical legacies, geographic realities, and economic means” (Williamson and Mansoor, 2012. 2). Starting with this point, threats will no longer come from states that use conventional means, but from states or groups that have a whole range of threats, techniques, tactics and the technology needed to mix them in an innovative way to produce desired effects (Hoffman 2009, 35-37). Regarding hybrid threats “blend the lethality of state conflict with the fanatical and protracted fervor of irregular warfare” (Hoffman, 2009, 5) to achieve political and military objectives.

Nowadays the reality has shown that hybrid threats, including “cyberattacks in the context of armed conflicts” directed against critical infrastructures (Pătrașcu 2018. 140), have produced major changes in the genetics of the concept of war. A concept that cannot be seen under its dual nature of black and white, conventional or unconventional, lethal or non-lethal, regular or irregular (Mosquera and Bachmann, 2016. 64), but the actions were divided into the gray area of the terms, still unregulated from the International Humanitarian Law perspective.

METHODOLOGY

Our paper examines researches from ProQuest Database on peer review between 2005 and 2020 by looking at key words from two fields: hybrid warfare and artificial intelligence. Based on this analysis we identified that starting from 2012 substantial progress has been made in artificial intelligence and its application to hybrid warfare as written in table no. 1.

First, we looked up in the database for the concept of "hybrid warfare" and we identified a number of 7531 papers. Also, we looked up for the "artificial intelligence" concept and we found 1 179 272 papers. Then, we queried the ProQuest Database using both concepts "hybrid warfare" and "artificial intelligence" and results 519 papers.

Secondly, we extended the list of search terms mixed "hybrid warfare" and "machine learning”, "data mining", "deep learning", and "artificial neural networks" with the main purpose of

identifing researchers' interest in the use of artificial intelligence in the hybrid warfare and to establish the topics they approach.

During our research we encountered certain limitations in the case of non full text articles identified in the ProQuest database.

Quantitative Analysis of the Papers

Quantitative analysis perspective showed that research about artificial intelligence has been rapidly growing starting from 2012. Started from this moment, we queried 519 papers, but we found only 41 peer reviewed as shown in table no 1. Next, we extended the list of search terms by mixing and "machine learning" when the results showed us only 14 paper peer reviewed from a total of 155. Furthermore, we queried about "hybrid warfare" and "data mining" and the results showed that there are in the ProQuest Database only 13 peer reviewed paper from a total of 36. Last step was to search the database about "hybrid warfare" and "deep learning" where the results were less numerous than previous with 5 paper per reviewed from a total of 23. Finally, the last interrogation referred to "hybrid warfare" and "artificial neural networks" when the database returned only 1 peer reviewed paper from a total of 6.

Table 1. Total results in ProQuest database by year and peer review

Search terms	Oldest first result	Results	Peer reviewed results
"hybrid warfare" and "artificial intelligence"	2012	519	41
"hybrid warfare" and "data mining"	2016	36	13
"hybrid warfare" and "machine learning"	2017	155	14
"hybrid warfare" and "deep learning	2018	23	5
"hybrid warfare" and "artificial neural networks"	2019	6	1

After summing up, the total number of peer-reviewed articles was 74 as shown in figure no 1, but only 55 papers of these were identified without being duplicated.

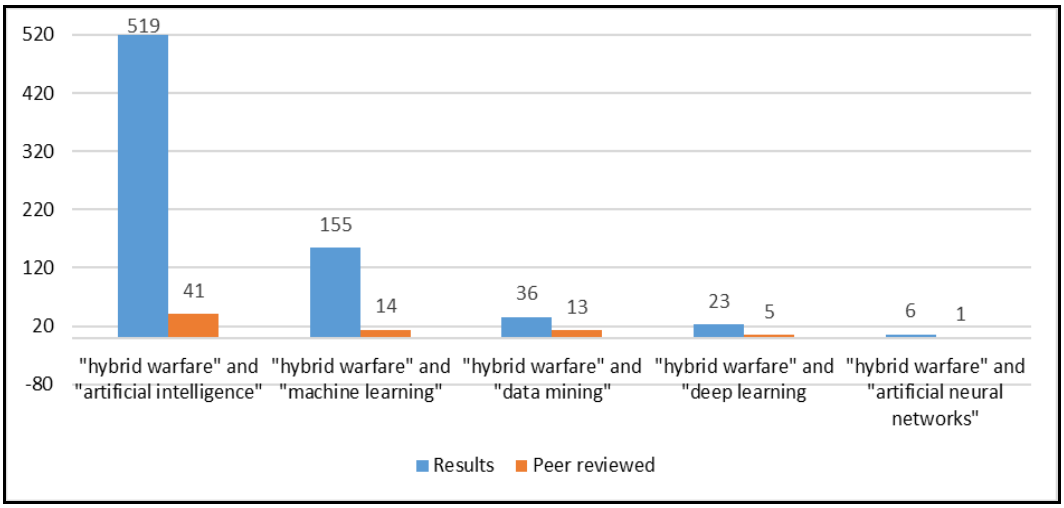

Figure 1. Total results on the searched topics in ProQuest database

The next step was to analyze the papers in terms of the year of publication. With this opportunity we found out that the oldest paper which contain the terms "artificial intelligence" and "hybrid warfare" is from 2012. This led us to the idea that, although the two terms are used frequently a few years before, only in 2012 is associated in the literature of technology of artificial intelligence with the new methods of waging war.

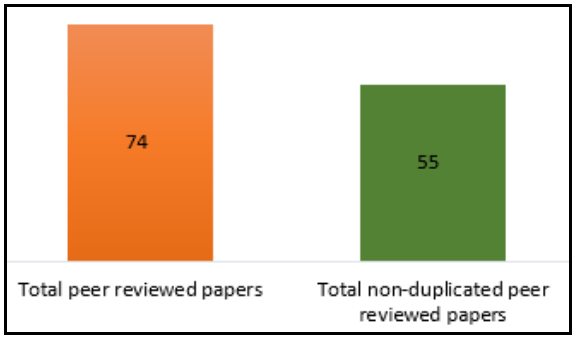

Figure 2. Total non-duplicated peer reviewed papers

Furthermore, this quantitative analysis will be extended with a qualitative analysis on the content of the 74 papers as shown in figure 2.

Qualitative Analysis of the Papers

Treating the literature review from a qualitative perspective may help writers to understand not only the numbers but also the semantic. What are the connected topics related to artificial intelligence which create effects in the hybrid warfare? How does artificial intelligence affect new methods of war? What countermeasures does the military have?

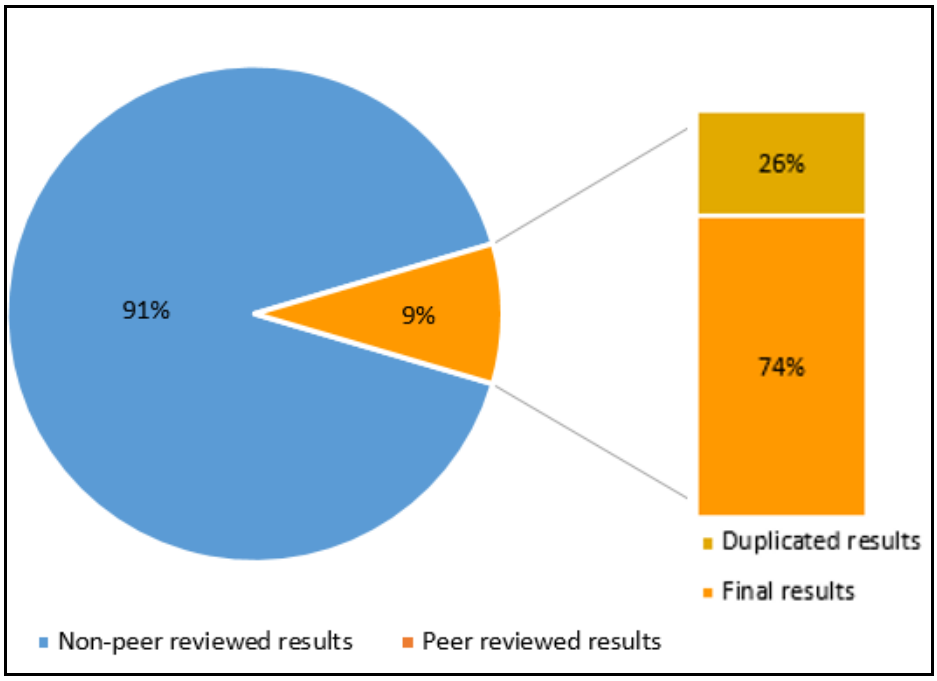

Figure 3. Percentage of peer reviewed articles

Following the qualitative analysis of the content of the 55 articles, a number of 6 military topics resulted, such as: information warfare, fake news/propaganda, threats in cyberspace /electronic warfare, drone warfare assets, decision making / C2.

Information warfare

From the information warfare (IW) perspective hybrid warfare was studied by analyzing dimensions like DIME/PMESII/ASCOPE (DIME – Diplomacy, Information, Military, and Economics; PMESII – Political, Military, Economic, Social, Information, and Infrastructure; ASCOPE – Areas, Structures, Capabilities, Organization, People, and Events) with the purpose of "building a framework for the problem space of influence/information/hybrid warfare and introduces the idea of the perception field, understood as a molecule (gestalt or shape) of a story or narrative that influences an

observer" (Kodalle, Ormrod, Sample, Scott 2020. 12). In this respect, one of the military leaders concerns is on how to integrate the "flow of information warfare (IW) data products and services into command and control (C2) systems to enable enhanced tactical and operational war-fighter and decision maker situational awareness". (Pirolo 2020, 1).

Fake news and propaganda

The term fake news is not new to mass media. A classic example of widespread fake news dates back to 1942, when the British set up the Aspidistra radio transmitter used in the air against Germany. The broadcasts tried to convince the German people that "the war was going badly for their country". (Crowdy 2008. 218) Recently, fake news has become a buzzword, especially since the 2016 US presidential election, because it is estimated that about "25% of tweets spread either fake or extremely biased news" (Bovet and Makse 2019, 1-14). In these times of hybrid warfare, the tremendous increase of online platforms and other Internet services has contributed to the growth in the abundance of fake news and deepfakes, which have become "the latest weapon in the war against truth" (Brown 2020 57-58)".

Our analysis of the ProQuest papers highlights the authors' interest in studying fake news and propaganda topics, like "what deep fakes are and who produces them, what the benefits and threats of deep fake technology are, what examples of deep fakes there are, and how to combat deep fakes" (Westerlund 2019, 39-52). Furthermore, some authors claim that although fake new were "recently recognized as a powerful weapon in the modern hybrid warfare" (Monakhov 2020. 1) yet the prospects of artificial intelligence and data analytics are very important, these "can be used to detect words or word patterns that might indicate deceitful stories" (Iasiello 2017, 51-63).

Threats in cyberspace and electronic warfare

Warfare tends to follow the same pattern of development as technology. Advances in information and communication technology and low-cost services have made transition from conventional warfare to hybrid warfare. Old threats specific to conventional warfare, such as nuclear threats, have been gradually replaced or supplemented in hybrid warfare with new types of threats. Cyber threats are new types of threats that "involve the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks" (Kremling et al., 2017. 18).

In the context of hybrid warfare uses of cyber assets as part of it is "one of the most important factors for understanding the future arc of conflict" (Simons et al., 2020. 337-342). This idea is reinforced by the multitude of papers published in the recent years and indexed in ProQuest database. In their academic studies, the authors manifest a major interest in cyber threats and electronic warfare, such as the examining "some intelligent computational methods for big data analysis which are applicable to issues of cyber security and military science" (Kamenov 2018. 255-262), "methodologies, and mechanisms to describe relevant data and knowledge" (Maathuis et al., 2018. 32), "linkages between electronic, cyber and hybrid warfare" (Shalamanov et al. 2020. 269-284), and "the malicious behavior of mobile terminals" (Bărbieru, Șușnea, and Șuteu 2019. 35-43).

Cyber threats create new opportunities and have the potential to change the playing field on modern battlefield. In this context, the existence of various types of electronic warfare (EW) systems that operate in cyberspace, and use of sophisticated methods for cyber defense are indispensable conditions affecting modern military operations. "These systems and their interactions are so complex that any modern military organization is unlikely to trace the full potential of any single cyber infiltration. The possibility exists for cyber attacks of every type, and the results can be catastrophic." (Alford 2000. 101)

Drone warfare assets

The development of new smart technologies contributes significantly not only to the replacement of old capabilities with new ones, but also to the adaptation of planning tools at hybrid warfare concept. Military strategy and policy "will likely opt to capitalize on its momentum in producing

more advanced, high-end technology systems …and developing more effective hybrid warfare CONOPS" (Kasapoğlu 2020, 124). Considering these aspects, it is crystal clear that new emerging technologies are decisive for both military planning and current operations and also may contribute to risk management in chemical, biological, radiological and nuclear (CBRN) conditions: "artificial intelligence that can recognize when people entering a hazardous zone are not wearing appropriate personal protective equipment" (Patel, Grace, Chellew, Prodanchuk, Romaniuk, Skrebets, Ryzhenko, Erickson 2020. 2)

Decision making and C2 systems

Some authors have analyzed the topic of emerging technologies from the military decision makers perspective, "how leaders are prepared to serve at the strategic level" (Cormier, 2020. 163) and how they "integrate the big data analytics with emerging technologies such as artificial intelligence (AI) into C4ISR capabilities …in times of conflict or crisis" (Poh and Ong 2019 115). Thus, the concept of decision making is analyzed not only from the perspective of decision makers but also from the integration of new technologies in the military decision-making process for increasing the situational awareness by "developing an understanding of the current situation, imagining future military actions …and establishing comprehensive approaches to achieve the desired end state" (Bălăceanu and Buță 2020, 18).

Critical infrastructure

Critical infrastructure has gained widespread public and private entities attention since September 11, 2001, attacks. These attacks "demonstrated our national level physical vulnerability to the threat posed by a formidable enemy-focused, mass destruction terrorism" (Department of Homeland Security 2003. vii). Protecting critical infrastructure against hybrid threats relies not only on national efforts, but on collective ones as well, engaging governments and the private sector, military and civilian stakeholder communities and international organizations.

In these unprecedented times, portrayed by complex and ambiguous hybrid threats and unprecedented evolution of artificial intelligence, there are authors claim that "critical infrastructures can be used as an instrument of hybrid warfare among weaker states" (Evans 2020. 35-42) and "coordinated information attacks have now become a violent tool for state and non-state actors, through the usage – coordinated information attacks against the strategic center of gravity of the enemy's critical infrastructure - of which, the set strategic objectives can be realized" (Csanád 2018 149-172). It is time "to put high stakes in the development of AI and escort the control of the critical infrastructure to AI." (Chaudhry et al. 2018, 4865-4866). These initiatives of the authors contribute significantly to the improvement of the security of critical facilities, systems, and functions as modern society become increasingly reliant on those that life-essential services, such as telecommunications, energy, water, transport and distribution, banking and finance, emergency services.

RESULTS

Based on the qualitative analysis of the articles indexed in the ProQuest database, we identified the topic in which each paper. Going further, we performed a quantitative analysis to determine the number of items that address a particular topic. These data are summarized in figure 4. Thus, we find that about 60% of the articles analyzed the topic "threats in cyberspace/electronic warfare" and "fake news/propaganda" and the difference of 40% covers the other 4 topics in the following order: "decision making/C2", "information warfare", "drone warfare assets", and "critical infrastructures".

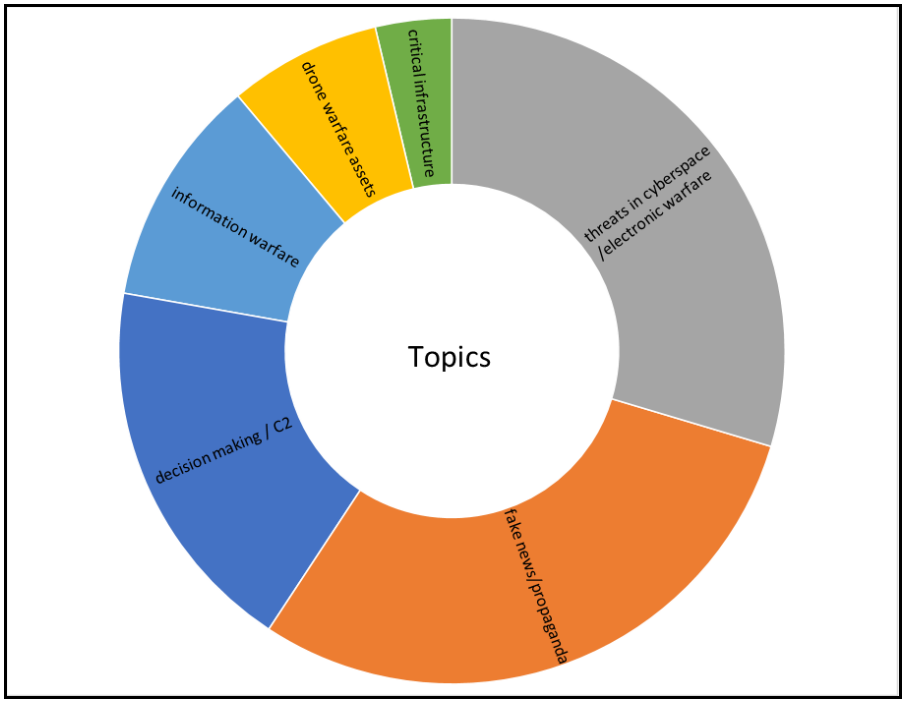

Figure 4. Peer reviewed articles topics

In the coming years, it is expected that artificial intelligence will develop a range of applications exceeding topics as shown above and being capable to develop complex tasks.

CONCLUSIONS

In recent years, the scientific community began focusing on how to use artificial intelligence in the hybrid warfare field. Starting from 2012, the authors have begun to correlate these two fields and moreover they have extended topics to others such as machine learning, data mining, deep learning and artificial neural networks.

From a quantitative perspective, our analysis showed that although there was a great interest in writing about artificial intelligence and hybrid warfare, there was still a reduced number of peer-reviewed papers. Out of a total of 519 papers, only 41 of them were peer reviewed and made the connection between artificial intelligence and hybrid warfare. Moreover, after associating 4 other terms with the concept of hybrid warfare such as machine learning, data mining, deep learning and artificial neural network, the number of peer review papers increased to 55 papers which represent a fairly reduced number considering that our research covered the period between 2012-2020.

To conclude, our paper studies the relationship between “artificial intelligence” and “hybrid warfare” in topics like INFOPS, decision making, ISR, Cyber, critical infrastructure. We discovered that none of the papers searched by the topics “artificial intelligence” and “hybrid warfare” in the ProQuest Database does not analyze hybrid warfare from the hybrid lawfare perspective. Moreover, only few of our 55 papers analyzed describe the countermeasures using artificial intelligence against hybrid threats in domain like: Strategic communication (STRATCOM), Cyber Operations, Political adviser (POLAD), Legal adviser (LEGAD), Psychological Operations (PSYOPS), Special Operation Forces (SOF), Civil-military (CIMIC), Civil Affairs (CA), and so on.

REFERENCES

Alford, Jr., Lionel D. 2000. “Cyber Warfare: Protecting Military Systems." Acquisition Review Quarterly, vol. 7, no. 2, p. 101.

Bălăceanu, Ion, Ionuț-Cosmin Buță, 2020. “Hybrid warfare’s influence in the military decisionmaking process”, Proceedings The 16th International Scientific Conference “Strategies XXI” Global Security and National Defence, National Defence Security “Carol I”, Bucharest, 15-20.

Bărbieru, Dragos, Elena Șușnea, and Dan Șuteu Ștefan-Antonio. 2019. "Integrated software platform for malware analysis of mobile terminals". *Bulletin of "Carol I" National Defense University* 8 (3).

Bovet, A., Makse, H.A. 2019. “Influence of fake news in Twitter during the 2016 US presidential election”. *Nature Communications* 10 (7): 1-14. https://doi.org/10.1038/s41467-018-07761-2.

Brown, Nina. 2020. “Deepfakes and the Weaponization of Disinformation”, 23 VA. J.L. & TECH. 1.

Chaudhry, J., Pathan, AS.K., Rehmani, M.H. et al. 2018. *Threats to critical infrastructure from AI and human intelligence.* J Supercomput 74, 4865-4866. https://doi.org/10.1007/s11227-018-2614-0

Cormier, Daniel J. 2020. “Will the united states learn from the Iraq war?” Naval War College Review 73 (1): 159-163.

Crowdy, Terry. 2008. *Deceiving Hitler: double cross and deception in World War II*. Oxford: Osprey. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=728283, 218.

Csanád, Fekete. 2018. “The strategic aspects of information warfare”. Hadtudomanyi Szemle = Military Science Review 11 (4): 149-172.

Department of Homeland Security, 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

Evans, Carol V. 2020. “Future warfare: weaponizing critical infrastructure”. Parameters 50 (2): 35-42.

Glenn, Russell W., 2009. “Thoughts on ‘Hybrid’ Conflict,” *Small Wars Journal*, [www.smallwarsjournal.com]

Hoffman, Frank G. 2009. “Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict”, *Strategic Forum*, no 240, 2009, 5.

Hoffman, Frank G. 2009. “Hybrid Warfare and Challenges”, JFQ / issue 52, 1st quarter 2009: 35-36.

https://hcss.nl/sites/default/files/files/reports/RAS_Military_Applicability_Final_.pdf

Iasiello, Emilio J. 2017. "Russia's improved information operations: from Georgia to Crimea." *Parameters 47* (2): 51-63.

Kamenov, Dimitar. 2018. “Intelligent methods for big data analytics and cyber security*”. Information & Security* 39 (1): 255-262.

Kasapoğlu, Can. 2020. “Turkey's burgeoning defense technological and industrial base and expeditionary military policy”. *Insight Turkey* 22 (3): 115-130.

Kodalle, Thorsten, Ormrod, Dave, Sample, Char, Knight, Scott. 2020. “A General Theory of Influence in a DIME/PMESII/ASCOP/IRC2 Model”, *Journal of Information Warfare*; Yorktown, Vol. 19, Iss. 2: 12-26,II-III.

Kremling, Janine, Sharp Parker, Amanda M. 2017. “Cyberspace, Cybersecurity, and Cybercrime”, *SAGE Publications*.

Maathuis, C., W. Pieters, and J. van den Berg. 2018. “Developing a cyber operations computational ontology”. *Journal of Information Warfare* 17 (3): 32.

Mansoor, Peter R., Murray, Williamson. 2012. “Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present”, Cambridge University Press, Cambridge: 2.

Monakhov, Sergei. 2020. "Early detection of internet trolls: introducing an algorithm based on word pairs / single words multiple repetition ratio." PLoS One 15 (8).

Munoz, Mosquera, Andres B., Bachmann, Sascha Dov. 2016. “Lawfare in Hybrid Wars: The 21st Century Warfare”, International Journal of Humanitarian Legal Studies, Vol. 7, no 1, 63-87.

Patel, Sonny S., Robert M. Grace, Patrick Chellew, Mykola Prodanchuk, Olha Romaniuk, Yuriy Skrebets, Sergii A. Ryzhenko, and Timothy B. Erickson. 2020. “Emerging technologies and medical countermeasures to Chemical, Biological, Radiological, and Nuclear (CBRN) agents in east Ukraine”. Conflict and Health 14: 1-4.

Pătrașcu, Petrișor. 2018. “Cyber security policies in the military domain”, International Scientific Conference "Strategies XXI", suppl. Strategic Changes in Security and International Relations; Bucharest, Vol. 3, (2018), 137-142.

Pirolo, Bradley M. 2020. “Information Warfare and Joint All-Domain Operations: A Primer for Integrating and Prioritizing Data Requirements”, USAF. Air & Space Power Journal ; Maxwell AFB Vol. 34, Iss. 4, 2020: 101-107.

Poh, Angela and Weichong Ong. 2019. "PLA reform, a new normative contest, and the challenge for ASEAN." Asia Policy 14 (4): 107-128.

Pouyanfar, S, Sadiq, S, Yan, Y, Tian, H, Tao, Y, Reyes, MP, Shyu, ML, Chen, SC & Iyengar, SS. 2018. 'A survey on deep learning: Algorithms, techniques, and applications', ACM Computing Surveys, vol. 51, no. 5, 92. https://doi.org/10.1145/3234150

Shalamanov, Velizar, Vladimir Monov, Ivaylo Blagoev, Silvia Matern, Gergana Vassileva, and Ivan Blagoev. 2020. "A model of ict competence development for digital transformation." Information & Security 46 (3): 269-284.

Simons, Greg, Danyk, Yuriy, Maliarchuk, Tamara. 2020. “Hybrid war and cyber-attacks: creating legal and operational dilemmas”, Global Change, Peace & Security, 32:3, 337-342, DOI: 10.1080/14781158.2020.1732899

Susnea, Elena. 2018. “A Real-Time Social Media Monitoring System as an Open Source Intelligence (Osint) Platform for Early Warning in Crisis Situations”. In: International conference KNOWLEDGE-BASED ORGANIZATION 24 (June 2018), 427–431. doi: 10.1515/kbo-2018-0127

Torossian, Bianca, Bekkers Frank, et al. 2020. “The Military Applicability of Robotic and Autonomous Systems”, https://hcss.nl/