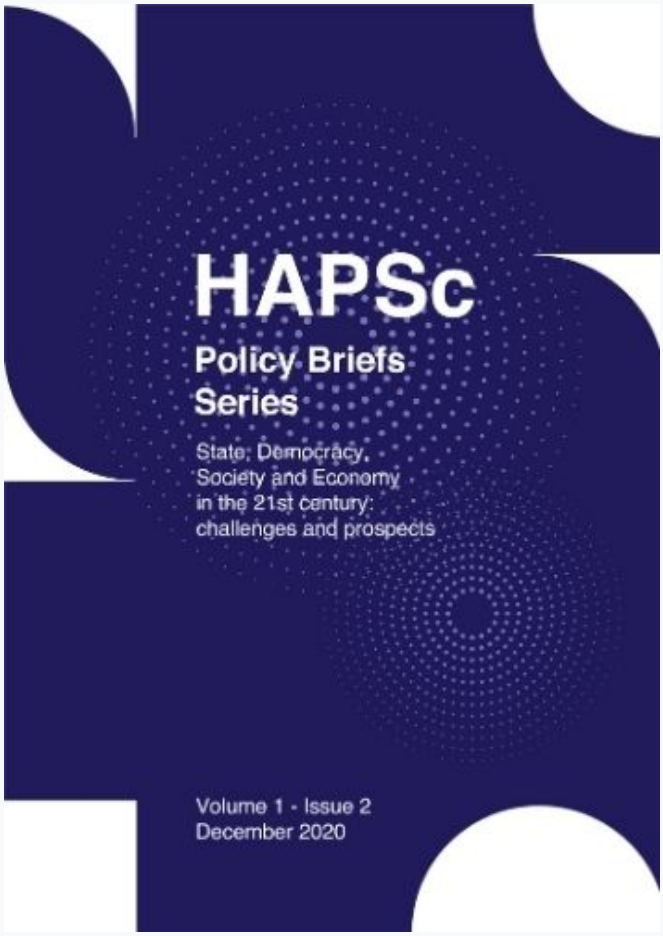
HAPSc Policy Briefs Series

Vol 1, No 2 (2020)

HAPSc Policy Briefs Series



The Evolution of War Conflicts. The Fourth Military Revolution (RMA) & Operational Applications

Nicholas Paounis

doi: 10.12681/hapscpbs.26523

To cite this article:

Paounis, N. (2020). The Evolution of War Conflicts. The Fourth Military Revolution (RMA) & Operational Applications. *HAPSc Policy Briefs Series*, *1*(2), 279–285. https://doi.org/10.12681/hapscpbs.26523

The Evolution of War Conflicts. The Fourth Military Revolution (RMA) & Operational Applications[1]

Nicholas Paounis[2]

Abstract

The phenomenon of War, historically could be characterized as multidimensional. War, that is, the confluence of military forces, over the course of the Centuries, has differed in terms of Strategic Concept, in terms of Doctrine of Operations, and in terms of technological capabilities. At the heart of the new form taken by the phenomenon of war is the possibility of mass collection and utilization of information, in combination with the technological development of weapons systems. New technologies have also attracted the doctrines of military operations. Traditional military forces, but also emerging ones, are at the forefront of new developments in the field of war.

Keywords: War; Fourth Military Revolution; Operational applications.

Introduction

If we wanted to define the concept of war, we could describe it, as organized conflict between states or between social groups, using armed force to achieve ideological domination, the seizure of wealth or the seizure of territories. The evolution of technology in combination with the evolution of globalized society and the "emergence" of new forms of threats, tends to change drastically, even the “ontology” of war. But the intentions of a conflict remain unchanged.

In the present paper we won’t attempt to give a new form of typology of each type of conflict, but will describe the role of information in the new field of conflict, the change of battle doctrines, the partial shift of the center of gravity of operations from human to robotic applications, and from the platform (jets, ships etc) to the missile.

All the aforementioned changes mark the so-called "fourth military revolution" or "revolution in military affairs", to which the modern military forces must adapt, otherwise they will be marginalized, and will be defeated by a potential opponent. However, factors such as "friction", "uncertainty" and "liquidity" remain unchanged as inherent properties of war.

[1] To cite this paper in APA style: Paounis, N. (2020). The Evolution of War Conflicts. The Fourth Military Revolution (RMA) & Operational Applications. *HAPSc Policy Briefs Series*, 1(2): 279-285. DOI: 10.12681/hapscpbs.26523

[2] Nicholas Paounis is Teaching Staff at the University of Athens and Researcher of the Institute of International Relations of Panteion University.

1) Info-Based Warfare and Cyber Warfare.

We are undoubtedly living in the age of post-industrial society, or the age of information ("information age", commonly known as the digital age, or season of the "digital revolution"), the period where technology applications (eg mobile phones, computers , tablets, etc.), IT (device software eg Windows, android, etc.), improved the quality of life of citizens, as the collection, processing and exchange of information created a new framework in the areas of services, research, transactions etc.

Sociologists talk about the post-industrial age, the "key" of which is considered the concept of information. Of course, the aforementioned cosmogenic changes in the level of access to information have a key impact on the areas of internal security and national defense. Telecommunications and information are vital parameters for the successful conduct of military operations. The goal of any military action is to prevail against the opponent, with the lowest possible losses in a short period of time.

The early form of the Internet, known as ARPA-NET (Advanced Research Project Agency), was a military application developed by the Pentagon in the 1960s to help researchers securely circulate information related to the developing world military programs. In the early 1980's, the adoption of a single information transmission protocol (TCP / IP Transmission Control Protocol / Internet Protocol), as well as the separation of military activities through MILNET (Military Network, now SIPRNET), contributed to the rapid development of the "peaceful" uses and applications "of the Internet. After the end of the Cold War, the widespread use of the Internet, led to the gradual networking between private companies, households, public services, which is crucial for increasing the influence of the Internet in all human activities and consequently in security (Palermo & Cox, 2014).

Nowadays, on the one hand, the interdependence between society and infrastructure on the Internet is constantly increasing, on the other hand, there is a lack of security when using the Internet, so the question arises as to whether it is possible to shield economic, industrial and public infrastructure against malware. And here is the core of the philosophy for the development of a new kind of "military" operations.

In the field of "cyber warfare", the battlefield is Cyber space (cyber space), ie a battlefield in the internet spectrum without physical space (longitude, latitude). Cyberspace means the general networking of people, companies, services (and so on), via PCs and telecommunications, regardless

of geographical location. Cyberspace is not a single field, since each individual network creates its own independent cyberspace (McCallion, 2020).

In conclusion, cyberspace is numerous, while the stratification of a cyberspace is divided into three categories i) hardware (H / Y) ii) semantic (information content) iii) syntax (software, operating systems, applications, etc.).

Due to the new data that emerged, a new strategic concept for the so-called "Information Based Warfare" was developed. Information-Centered (or Information-Based) Warfare - like Network-based - has at its core the activities around the concept of "information", and can be part of a "Non-Linear Warfare" (in the broadest sense), in order to actors (State, International Organization, paramilitary organization, militia, terrorist group, etc.), to impose on the enemy in a sudden, bloodless and effective way (Paounis, 2019).

Info based Warfare, however, focuses on the collection, evaluation, and dissemination of information, without including further extensions of Net-Centric Warfare (e.g., data traffic from operations centers to platforms). The problem of over-accumulation of information and the consequent inability to fully evaluate them, led the US to the so-called "decentralized" models of governance.

A "subcategory" of Info based Warfare can be considered Cyber Warfare. The objectives during a "Cyber War" are summarized as follows: Cyber defense: i) protection of deadly information systems and information from a hostile cyber attack, ii) silencing of hostile information (De Vries, 1997).

In the context of a cyber attack, the objectives are: i) access and exploitation of enemy information, ii) attacking enemy information systems, iii) spreading false news aimed at the morale of enemy, civilians and soldiers, etc. These attacks can through the use of malware (viruses, Trojan Horse etc), or through the deliberate introduction of large amounts of information into a system (inability to process and crash or malfunction of the system). The aforementioned are considered the weapons of a cyber attack.

Through a cyber attack, it is common to seek alternative i) attack on infrastructure (eg electricity distribution network), ii) blocking users from accessing a system (eg banning the use of services), iii) cyber espionage and iv) the alteration of data circulating in a system (eg destruction or alteration of web page content). These targets may include hostile telecommunications, water supply, financial institutions, transport, insurance and postal services, and military installations.

The advantage of Cyber Warfare lies in the fact that the attack is carried out almost inexpensively, without the involvement of conventional means of strike (aircraft, missiles, etc.), and can cause damage to critical facilities, and lead to the collapse of the enemy state. It can also pave the way for

a second attack with conventional weapons. The "non-linearity" of the attack can cause chaos, disorganization of state services and low morale among the people. Unlawful acts can be carried out by individual hackers, or small criminal groups and of course by properly organized services of a state actor (Johns Hopkins Applied Physics Laboratory, 1995). So far, the most recent example is the collapse of all of Estonia's infrastructure following a cyber-attack in 2007 (Ottis, 2008).

2) Net Centric Warfare and Anti Access/Area Denial

Network-centric warfare (NCW) is the entire military operation to gather information and transmit it to attack platforms. The process is implemented through the networking of weapons, sensors, satellites and decision-making centers, in order to have a unified perception of the existing tactical situation, speed of decision-making, synchronization and increased viability of friendly forces, and finally effective use of weapons systems. Commonly, the integrated interconnection of all sensors, weapons systems and command centers offers an excellent picture of the tactical situation, the possibility of timely and correct decision-making, perfect coordination (or at least to the best degree) and maximization of the result on the battlefield (Kopp, 2008).

The benefits at management level are manifold. Due to the very good knowledge of the tactical situation, faster decisions are allowed, a fact which implies the firing of an immediate overwhelming fire in order to eliminate the possibility of the opponent escaping, the realization of the appropriate maneuver, etc. However, the challenge comes from the fact that an unprecedented amount of information is over-concentrated with a high rate of renewal, which carries the risk of inability to manage all the information, ie irrational judgment and decision making.

From a technical point of view, a SoSA (System of Systems Analysis) is required, ie a wider network of high-processing, data management and data analysis computers that will be interconnected and provide an "integrated picture" to support command, control, communications & Intelligence, the continuous flow of data to weapons systems, etc (Anand, Raja, Rajan, 2011).

The first attempt to interconnect several weapons systems, decision-making centers and even multinational forces, took place during the first Gulf War in 1991. The challenge in this case was in addition to coordinating the actions of a multinational force, and cooperation due to ethno-religious peculiarities. The Alliance's Joint Communication and Unification Coordination Center was set up and operated at the Defense and Aviation Building (MODA) in Riyadh, Saudi Arabia (Paounis, 2018).

China - especially after 2005 - carefully studied the new possibilities stemming from the widespread use of satellite systems (Yaogan-30), unmanned aerial vehicles (UAV's/Drones), ground-based

observation networks, electronic warfare aircrafts, and networked with each other to create an unprecedented observation grid, collection and utilization of information. The "end" of all these multi-grid systems are the YJ-18 missiles (Dong Feng DF-21, and, very soon the DF-100). The famous anti-access/area denial (A2/AD) was achieved in the same way (Tsai, 1996). The Turkish Armed Forces also waged a network-centric war during the occupation of Afrin, during the Olive Branch operation (Paounis, 2018).

3) Artificial Intelligence Weapons and the generation of Hypersonic Missiles.

The end of the INF Treaty on August 2, 2019, due to the reluctance of the US to extend its further implementation, coincides with the development of new missile systems, known as post-nuclear super-weapons. The Treaty, in its implementation, prohibited the development of medium-range surface-to-surface cruise missiles and missiles, ie from 500 to 5,500 km/IRBM's (Grivas, 2013).

The main reason for the negative attitude of the USA was the development by China and Russia networks of anti-access areas (A2/AD) and air defense "domes" respectively, with the aim of preventing the approach of specific geographical areas by the U.S. Navy and the U.S. Air Force. As a proper solution to "pierce" the aforementioned "domes", the development of a new generation of missile systems was chosen, among other things (Grivas, 2019).

Central to the new generation - of any kind - missiles, is artificial intelligence (hence the high degree of independent navigation, in the phase of approaching the target), and high accuracy. In recent years, maneuvering missiles (supersonic & hypersonic missiles) have appeared to avoid anti-ballistic missiles, and to strike a decisive blow against the target.

Russia presented the anti-ship missiles P-800 Oniks, 3M22 Zircon etc (Kimball & Kingston, 2019). China has DF-17s and recently introduced the DF-26 long-range missile, capable of maneuvering and striking "medium" targets, such as Destroyers. In October 2020, the US tested the C-HGB system, which developed a speed greater than 5 mach (hypersonic missile). As a result, the great military forces of the planet are entering a new era where the existing anti-ballistic missile systems (Patriot PAC3, S-400/SA-21, SAMP/T etc.) are becoming obsolete and the development of new ones is immediately required.

Another notable element of the new missile formats is the case of the CHAMP missile, which has an EMP-type warhead, through which it emits electromagnetic pulses and can disrupt the enemy's electronic infrastructure (soft kill).

Significant changes are also observed in the Artillery. New rockets with increased range, with thermobaric heads, and shells with propulsion mechanism are introduced. In general, Artillery tends to become a “game changer” factor.

4) UAV’s and Loitering Munitions

Over the past decade, there has been a rapid development of "Unmanned Air Vehicles" technology around the world. Indicatively, the countries with the systems in use are as follows: USA (MQ-9 Reaper, MQ-1 Predator), United Kingdom (WatchKeeper 450), Israel (Hermes, Heron), Turkey (Bayraktar TB2, ANKA, Karayel, Akinci), Russia (Sukhoi Okhotnik), Spain (Skeldar V-200), Iran (Shahed, Mohajer) and Azerbaijan (Orbiter). There are at least 30 countries using Unmanned Aerial Vehicles.

In fact, Azerbaijan, with the assistance of Turkish Bayraktar (in combination with the high mobility of the Infantry), crushed the Armenian military forces during the recent conflict in Artsakh (autumn 2020), while making widespread use of Loitering Munitions. The specific munitions, after being launched, searches for the target either autonomously or under the guidance of a soldier, and then charges and destroys it. Their small size and large autonomy make them difficult to deal with and extremely effective in attacking ground and sea targets. Loitering munitions are being developed by countries such as Israel (IAI Harop / Harpy), Turkey (Alpagu / Kargu), and Iran (Qasef-1).

The distinction between loitering munitions and UCAV’s is blurred (e.g. Harpy), but it can certainly be argued that robotic applications are flooding the military technology sector, and are becoming increasingly crucial to the successful outcome of operations (Gettinger & Michel, 2017).

The US Navy is developing the LOCUST system, which launches a "Squadron of Drones" over a hostile area, which is literally scanned. During tests, 31 drones were launched in 40 seconds, which can interfere with enemy telecommunications and generally operate in the E/M range. Finally, the role of UAVs in network-centric operations is considered crucial in the sense that they "collect" and directly transfer the image of targets to impact platforms.

Conclusion

It becomes clear that the changes on the battlefield are at the “crossroads” for the way future operations are conducted. In a broader analysis, we would see a change in the Doctrine of War (e.g. Multi Domain Battle), but also the use of Social Media (twitter, youtube) during a conflict. Countries

facing military threats need to redefine the training, doctrine and military equipment framework in order to successfully meet the new operational requirements.

References

Anand, D., Raja, Ch. and Rajan, Dr. E. G. (2011). Network Centric Warfare, Concepts & Challenges. CiiT International Journal of Networking and Communication Engineering, 3 (14): 898-902.

De Vries, A. (1997). Information Warfare and its Impact on National Security. Newport, Rhode Island: Naval War College. Available at: https://www.hsdl.org/?view&did=459698 (Accessed: 30/11/2020).

Gettinger, D. and Michel, H. A. (2017). Loitering Munitions in Focus. Bard College: Center for the study of the Drone.

Grivas, K. (2013). *The Military Rise of China and the Geopolitics of War in the Middle East*. Athens: Livanis Publications [in Greek].

Grivas, K. (2019). *The New Military Revolution and the Greek Defense Strategy*. Athens Livanis Publications [in Greek].

Johns Hopkins Applied Physics Laboratory (1995). The Cooperative Engagement Capability. *Johns Hopkins APLS Techical Digest*, 16(4)377-395.

Kimball, D. and Kingston R. (2019). The Intermediate Range Nuclear Forces (INF) Treaty at a Glance. Arms Control Association. Available at: https://www.armscontrol.org/factsheets/INFtreaty (Available: 30/11/2020).

Kopp, C. (2008). Understanding Network Centric Warfare. *Australian Aviation*, 101(19): 168-171.

McCallion, J. (2021). What is Cyber Warfare? IT pro. Available at: https://www.itpro.co.uk/security/28170/what-is-cyber-warfare (Accessed: 30/11/2020).

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited, pp. 163-168.

Palermo, E. and Cox, L. (2014). Who Invented the Internet. Live Science. Available at: https://www.livescience.com/42604-who-invented-the-internet.html (Accessed: 30/11/2020).

Paounis, N. (2018). The Net Centric Warfare (NCW), Platforms and International Experience. *ELIAMEP*, 95: 3-9 [in Greek].

Paounis N. (2019). Info Based Warfare & Cyber Security. *ELIAMEP*, 99: 1-9 [in Greek].

Tsai, S. X. (1996). Introduction to the Scene Matching Missile Guidance Technologies. National Air Intelligence Center. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a315439.pdf (Accessed: 30/11/2020).