JYX JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Lehto, Martti; Henselmann, Gerhard

Title: Non-Kinetic Warfare : The New Game Changer in the Battle Space

Year: 2020

Version: Published version

Copyright: © 2020 ACPIL

Rights: In Copyright

Rights url: http://rightsstatements.org/page/InC/1.0/?language=en

Please cite the original version:

Lehto, M., & Henselmann, G. (2020). Non-Kinetic Warfare : The New Game Changer in the Battle Space. In B. K. Payne, & H. Wu (Eds.), ICCWS 2020 : Proceedings of the 15th International Conference on Cyber Warfare and Security (pp. 316-325). Academic Conferences International. The proceedings of the ... international conference on cyber warfare and security. https://doi.org/10.34190/ICCWS.20.033

Non-Kinetic Warfare: The New Game Changer in the Battle Space

Martti Lehto and Gerhard Henselmann
University of Jyväskylä, Finland
martti.j.lehto@jyu.fi
office@ghenselmann.de
DOI: 10.34190/ICCWS.20.033

Abstract: Cyber warfare, information warfare, electronic warfare, command and control warfare, spectrum warfare. Those are only some of the names by which researchers and military experts describe their offensive and defensive non-kinetic actions. The reason for the diversity of the non-kinetic environment is the evolution of the military Electromagnetic Spectrum (EMS) and digital environment over 100 years. With the arrival of radio in the early 20th century, the militarization of the electronic operating environment began. The latest expansion is the formation of the cyber space. Also, the definitions vary significantly. There are differences between USA, Russia, China and NATO. Western countries talk about cyber space, while Russia and China talk about the information environment/space. A recent development in superpowers defense networks has been the integration of Electronic Warfare (EW), Information Warfare (IW) and Cyber Warfare (CW) systems designed to generate non-kinetic effects on intruders in partnership with the traditional use of kinetic weapons. The new capacities of armed forces create new possibilities, both the kinetic and non-kinetic use of force in battlespace. This paper addresses the non-kinetic battlespace elements Electronic Warfare, Information Warfare and Cyber Warfare and the operations in those environments, and which constitute a complete non-kinetic warfare environment (NKW). These advanced and new capabilities form a whole new non-kinetic environment in which they become a game changer in battle space. This paper argues that, although there is an overlap between Cyber Warfare, Information Warfare and Electronic Warfare, these three concepts are not totally analogous. In this paper we focus on EW, IW, CW definitions in the new man made non-kinetic environment and create a Non-Kinetic Warfare environment description and describe EW, IW, CW in the levels of warfare.

Keywords: Electronic Warfare, Information Warfare, Cyber Warfare, Non-Kinetic Warfare

1. Introduction

In the traditional warfare model, nation-states fight each other for reasons as varied as the full array of their national interests. Military operations in traditional warfare normally focus on an adversary's armed forces to ultimately influence the adversary's government. Irregular Warfare. This form of warfare is characterized as a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation's established government. (JP-1, 2017)

Defining a non-kinetic environment is not easy to do because the components included therein have had different emphases at different times. The domain definitions have fluctuated at different times depending on what is being emphasized the most.

Control of information has always been part of military operations. The origins of the term information warfare can be traced back to the late 1980s when the expression was specific to the military domain (Hutchinson, 2006). It was discovered in the early 1990s that information infrastructures are vulnerable to attack. At that time specifically the information infrastructure was the focal point (consisting of information, information systems, telecommunications, networks, and technology) and it depends, in turn, upon other infrastructures such as electrical power and other forms of energy.

In July 5, 1990, President Bush issued National Security Directive 42, recognizing the vulnerabilities of telecommunications and information processing systems. According to Directive 42 "telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat." (NDS-42, 1990)

In March 1993 was published the Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30 (MOP 30). In MOP 30 the starting point was Command and Control Warfare (C2W). C2W was the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade

or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. So C2W is the military strategy that implements Information Warfare on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of combat forces. (MOP 30, 1993) In other words C2W included IW or brought a new addition to IW.

Arquilla and Ronfeldt published in 1993 article *Cyberwar is Coming!*, where they described Netwar and Cyberwar. They described that Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population “knows” or thinks it knows about itself and the world around it. Respectively Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. In their definition, Netwar can be considered Information Warfare.

Martin Libicki (1995) used this document when he published a National Defence University essay in August 1995 "What is information Warfare?". His taxonomy included seven forms of IW. In his taxonomy, IW is a top notion that includes among others EW and CW.

The Presidential Decision Directive/NSC-63 May 22, 1998 focused on Critical Infrastructure Protection. PDD/63 mentioned that critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. So cyber was focused on critical infrastructure. For each infrastructure sector that could be a target for significant cyber or physical attack. (PDD/63, 1998)

The term cyberspace was not officially designated by the Department of Defense (DoD) as a warfighting domain until 2006; prior to 2006, the term cyberspace was perhaps understood as a commercial realm in which the military sent and received data packets but had no real need to do more than worry about the DoD's own networks. (Mirenda, 2011)

In 2008 USAF defined that “cyberspace encompasses the electromagnetic spectrum with its distinctive physical properties and those of the manmade electronic systems created to operate across the domain” (USAF, 2008). So cyber space comprises also the electromagnetic spectrum.

The research will find out the evolution, nature and character of the non-kinetic warfare. The research has made by using USA sources, because the USA has been a forerunner in the development of non-kinetic capability. Other Western countries have adapted those results. The study has used content analysis as a research method making analysis from written communication. The data collected through it are summarized so that the meanings, consequences and connections of the phenomena and issues under study can be examined.

2. The spaces of non-kinetic warfare

2.1 Electromagnetic spectrum

The electromagnetic spectrum (EMS) is a broad area of activity characterized by physically observable activities such as visible light and lasers and unobservable phenomena such as microwaves and electromagnetic energy. EW uses electronic means to paralyze enemy EMS based systems like communication, radar, navigation while ensuring the integrity of their own systems.

The EMS is a physics-based maneuver space essential to control the operational environment during all military operations. Information and data exchange between platforms and capabilities will at some point rely on the EMS for transport. This maneuver space is constrained by both military and civil uses as well as adversary attempts to deny the use of the EMS, creating a congested and contested environment. (JP 6-01, 2012)

Use of EMS and EMS-enabled capabilities to achieve effects may reduce risk by limiting exposure of combatants, lower costs by offering significant life-cycle savings over conventional munitions, and present commanders with an array of non-kinetic options that can achieve effects unattainable through kinetic fires. (TRADOC, 2018)

2.2 Information space

In the mid-2000s, according to the United States, information is a resource created from two things: phenomena (data) that are observed, plus the instructions (systems) required to analyze and interpret the data to give it meaning. The value of information is enhanced by technology. (Wilson, 2007)

The information environment comprises and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The information environment also includes technical systems and their use of data. The information dimension represents the content of the information used by the decision maker. Once someone applies meaning to any data element, the data element is transduced into information. This distinction is subtle; but the impact is profound. (JP 3-0, 2018)

Adversaries conduct sophisticated influence operations and leverage cyberspace as a force multiplier in the information environment. They use propaganda and disinformation through social media to affect public perception, sway public opinion, and catalyze protests and violence in ways that popular movements once took months or years to build. (TRADOC, 2018)

JP 3-13 (2016) uses the term information environment instead information space. The information environment is defined as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." The information environment is comprised of the physical, informational, and cognitive dimensions. Information operations primarily focuses on affecting the cognitive dimension, where human decision making occurs, through the physical and information dimensions. (JP 3-13, 2016)

2.3 Cyberspace

The Internet forms the basic structure of cyberspace. Still, there is no widely accepted definition of cyberspace. Cyberspace is a man-made environment and is therefore unlike the natural domains of air, land, maritime, and space, so cyberspace is a military medium subject to the tenets of warfare that exist in the other physical media (Libicki 2012). Cyberspace is its own medium with its own rules (Libicki, 2009). Cyber space exhibits unique physics, it is not spatially distinct from the other domains; rather it pervades all the other domains.

Some definitions divide it into constituent parts or different levels. Some focus more on information flows or processes from a holistic point of view. Yet, others concentrate more on the administrational, governmental and legal side of this new, artificial and continually changing space. (Kukkola et.al, 2017)

IN US military context cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 1-02, 2016; JP 3-12R, 2018).

Cyberspace is a domain. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace. (JP 3-12R, 2018)

Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks (Klimburg, 2012). The ITU uses the term to describe the "systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks (ITU, 2012).

2.4 Non-kinetic environment

USAF describes the non-kinetic environment: "Kinetic actions are those taken through physical, material means like bombs, bullets, rockets, and other munitions. Non-kinetic actions are logical, electromagnetic, or behavioral, such as a computer network attack on an enemy system or a psychological operation aimed at enemy troops. While non-kinetic actions have a physical component, the effects they impose are mainly indirect- functional, systemic, psychological, or behavioral". (AFDD 2, 2007)

For example, the number of continuously internet-connected devices that communicate with one another is doubling every five years, a process building the phenomenon of the 'internet of things. Even if the future of warfare is one of radical change, can we assume that technology will play a decisive role in driving that change? (Tuck, 2019)

In our taxonomy the operations of Electronic Warfare, Information Warfare, and Cyber Warfare constitute a complete set of non-kinetic network-based operations. So network, broadly understood, and EMS are the environment of those operations.

3. Non-kinetic warfare

3.1 Electronic Warfare (War in EMS)

Generally, formal military technology defines electronic warfare as a military action whose objective is the control of the electromagnetic spectrum. This objective is achieved through offensive electronic attack (EA), defensive electronic protection (EP), intelligence gathering and threat recognition electronic warfare support (ES) actions. (De Martino, 2018) EW capabilities include directed energy, decoys, and radiofrequency (RF) jamming to deny, disrupt, or deceive an adversary's electromagnetic capability. (Arnold, 2009)

Indeed, there is every indication that electronic warfare will continue to generate more consequential effects on the battlefield than cyber warfare because electronic warfare is not an artifact of the other side's poor decisions. It is an unavoidable aspect of long-distance RF communications. And, as noted, there is no classic strategic treatment of electronic warfare; nor is there indication that such effort is missed. (Libicki, 2014)

EW systems can be described as "front end" analog systems that sense and receive information and "back end" digital data processing systems with functionality driven by software. A front-end system with broad capabilities can be paired with modern electronics—as employed in radars, communications, precision-navigation-targeting (PNT) and of particular concern here, jammers and decoys. (TRADOC, 2018; JP 6-01, 2012; JD 3-16, 2016)

EW represents the ability to use the electromagnetic spectrum—signals such as radio, infrared or radar—to sense, protect, and communicate. At the same time, it can be used to deny adversaries the ability to either disrupt or use these signals. Electronic warfare is therefore any strategic use of the electromagnetic spectrum, or of tactics related to the use of the electromagnetic spectrum, against an enemy in a military conflict. (TRADOC, 2018; JP 6-01, 2012; JD 3-16, 2016)

Joint Electromagnetic Spectrum Operations (JEMSO) consisting of EW and joint EMS management operations, enable EMS-dependent systems to function in their intended operational environment. EW is the mission area ultimately responsible for securing and maintaining freedom of action in the EMS for friendly forces while exploiting or denying it to adversaries. JEMSO therefore supports Information operations by enabling successful mission area operations. (JP 13-3)

Advanced materiel properties and switching architectures have increased the speed and capacity of EMS operations enabling low power, near-simultaneous transmission, and jamming in the same frequency band. These developments, together with software-defined algorithms, wideband frequency hopping, and cognitive radios, have already outpaced current practices for modeling, allocating, and managing EMS activity.

Technologies such as application-specific integrated circuits, programmable logic devices, digital radio frequency memory, and shared aperture electronic attack, increase the number of ways users can attack through the EMS. Lower power demand, smaller size and weight, higher sensitivity, and wider frequency ranges for sensing and transmitting revolutionize a commander's operational capabilities. These technological advances expand access to the EMS resulting in congestion from commercial users, local and national host nation governments, adversaries, partners, and Army EMS-enabled systems that saturate available bandwidth and constrain maneuver within the EMS. (TRADOC, 2018)

3.2 Information Warfare: War on Minds

Information warfare (IW) is a concept involving the battlespace use and management of information and communication technology (ICT) in pursuit of a competitive advantage over an opponent. Information warfare

is the manipulation of information trusted by a target without the target's awareness so that the target will make decisions against their interest but in the interest of the one conducting information warfare. IW is about gathering, providing, and denying information in order to improve one's own decision-making while damaging the enemy's. Information operations have been accomplished through various means of communication, psychological operations, media manipulation and disinformation campaigns. Unifying those capabilities has always been a challenge, however, especially the technical and informational elements. (JP 3-13, 2014; RAND, 2019; Crane, 2019)

Information operations are the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own information, information-based processes and information systems. Information operations are also known as influence operations and include the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent. The objective in information space is to achieve information superiority. (JP 3-13, 2014; RAND, 2019)

Power of information and media is overriding all other policies and instruments of power in today's world. Perception development, shaping and management have become the prime means for fostering attitudes, behaviors and decisions by the target audiences. The sole aim of information operations is to flood massive volumes of information into the mind of the target audience. This flooding leaves the audience unable to filter the right from wrong. Whether information is believed, ignored or distrusted will depend upon the intellectual standing of the receiver and reputation and credibility of the sender. (IWP, 2019)

Information operations are not a fundamentally new type of warfare, but the failure to understand its potential as an offensive tool and the vulnerabilities inherent in such conflict presents potentially grave strategic threats to countries with a high dependency on information- and network-based economies.

Over the past two decades, there has been debate about the relationship between information warfare and cyber warfare. General Kevin Chilton, Commander USSTRATCOM said in 2010, that it is justified to separate cyber from information operations on the recognition that cyberspace is now an independent line of operation. He continued that "Cyberspace operations play such a significant role they deserve their own identity, no longer subordinated under a generalized category of IO." (Reimer, 2010)

3.3 Cyber Warfare (War in bits and bytes)

Cyber Warfare (CW) is the newest non-kinetic warfare concept which has a connection to EW and IW. Cyber warfare involves non-kinetic attacks on information data and its collection process aimed at damaging, disrupting or destroying decision making processes. It is both offensive and defensive, ranging from methods that prohibit the enemy from exploiting information to corresponding measures to guarantee the availability, reliability, and interoperability of friendly information assets. Thus, CW encompasses the use of all digital systems "tools" available to paralyze or even destroy enemy's ICT-technology based systems while keeping our own systems operational. Cyber warfare is an outcome of information age paraphernalia like satellites, electronic mailing system, internet, computers and micro-chip. (Wooding, 2019; Wardrop, 2018)

Levels of cyber warfare need to be distinguished from one another. Cyber warfare, like warfare itself, is about the conduct of war, carried out inevitably to further the performance of combat in the physical domain (operational level). Cyber warfare is undertaken to affect the will of the adversary directly (strategic level). (Libicki, 2014)

What is the line between cyber warfare and traditional warfare? Definitions matter when implementing policy, and in developing a CW a variety of factors must be considered. In essence, this question focuses on the role of information technology as an enabler of warfare and, therefore, as a viable target from both attack and defense viewpoints. Cyber warfare will have kinetic effects, meaning it will cause real direct and indirect damage to physical infrastructure. (Colarik and Lech, 2012)

General (ret.) John Allen and Amir Hussain described in their article a possible cyber warfare scenario as a part of Hyper war: "The guided-missile destroyer had not "seen" the incoming swarm because it had not recognized that its systems were under cyber-attack before things turned kinetic. The undetected cyber

activity not only compromised the destroyer's sensors, but also "locked-out" its defensive systems, leaving the ship almost helpless. The kinetic strikes came in waves as a complex swarm. The attack appeared to be conducted by a cloud of autonomous systems that seemed to move together with a purpose, reacting to each other and to the ship." (Allen & Hussain, 2018)

To argue that cyber warfare can have a revolutionary effect on the battlefield requires establishing that digital networking is itself revolutionary (Libicki, 2014). The working hypothesis is that a cyber-attack used in lieu of kinetic methods creates more ambiguity in terms of effects, sources, and motives. Thus, if cyber-attacks work – and this is a tremendous if – they change the risk profile of certain actions, and usually in ways that make them more attractive options. (Libicki, 2011)

Cyber warfare differs fundamentally from traditional armed conflict. Unlike the conduct of past warfare, opponents can wage cyber warfare from far reaches of the globe rapidly, cheaply, anonymously, and devastatingly. (Smart, 2011)

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. Cyber warfare refers to the use of digital attacks - like computer viruses and hacking - by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction. (RAND 2019b)

US Air Force (USAF) has made organizational changes to integrate traditional ISR (intelligence, surveillance, recognition) sensors and platforms in each domain with electronic warfare and cyberspace tools. This advance is expected to lead to "increased war-fighting capabilities by leveraging the intersection of ISR, cyber and the electromagnetic spectrum." In 2018 the cyber and intelligence missions (the 24th and 25th Air Forces) were re-assigned back to Air Combat Command (ACC) and were integrating cyber mission with electronic warfare and other traditional Air Force combat tasks. The objective is to integrate missions of cyber closer to war fighting and not support. (Healey, 2019)

USAF announced in September 18 a new information warfare focused organization called 16th Air Force that combines cyber, intelligence, surveillance and reconnaissance, electronic warfare and information operations (Pomerleau, 2019). The USAF will use the assets focusing on space, air, surface, subsurface, and cyber, and all that data needs to be put into a network that can be shared, stored, accessed and secured (Everstine, 2019).

3.4 Non-Kinetic Warfare

Non-Kinetic Warfare (NKW) does not have a uniform or widely accepted definition. It can be defined broadly as "use of informational, psychological, diplomatic, economic, social and technological tools of the statecraft to achieve national interests and objectives by either acquiescing or impairing national will of the adversary." Non-kinetic engagements can create unique uncertainties prior to and/or outside of traditional warfare, precisely because they have qualitatively and quantitatively "fuzzy boundaries" as blatant acts of war. Non-kinetic engagements often utilize non-military means to expand the effect-space beyond the conventional battlefield. (Farooq, 2014)

NKW occurs in a realm located simultaneously at different layers of non-kinetic environment (physical, syntactic, semantic, service and cognitive) that intersects activities in, through, and concerning the electromagnetic spectrum, information space and cyber space which seamlessly crosses other domains. The extent to which NKW differs from kinetic warfare represents a paradigm shift in modern military affairs. However, differences exist between the actors and the means/ways of armed conflict in the physical world and their counterparts associated with conflicts in the non-kinetic environment. (Smart, 2011; Lehto 2015)

The rapid growth in non-kinetic activity challenges traditional notions of hostile action and accountability within international law. Cyber operations synchronized with electronic warfare in the context of a full spectrum approach may overmatch conventional forces that are not prepared for conflicts in the electromagnetic environment and cyberspace simultaneously. The situation now exists whereby technological advantage is being eroded by non-conventional warfare using electromagnetic and cyber activities. (Ministry of Defence, 2018)

In the Non-kinetic Warfare Spectrum it is possible to join the Electromagnetic Spectrum Operations, the Information Space Operations and the Cyber Space Operations so that they address many of the capabilities required to protect the Force's ability to acquire, process, distribute and act on the digital environment to enhance combat power.

The expansion and diffusion of advanced technology has lowered the cost of entry into the Non-kinetic Warfare Spectrum such that non-state actors can now acquire electronic-information-cyber related capabilities that once were available only to developed countries.

Here figure 1 illustrates the IW-EW-CW in Non-kinetic Warfare Spectrum with different missions.

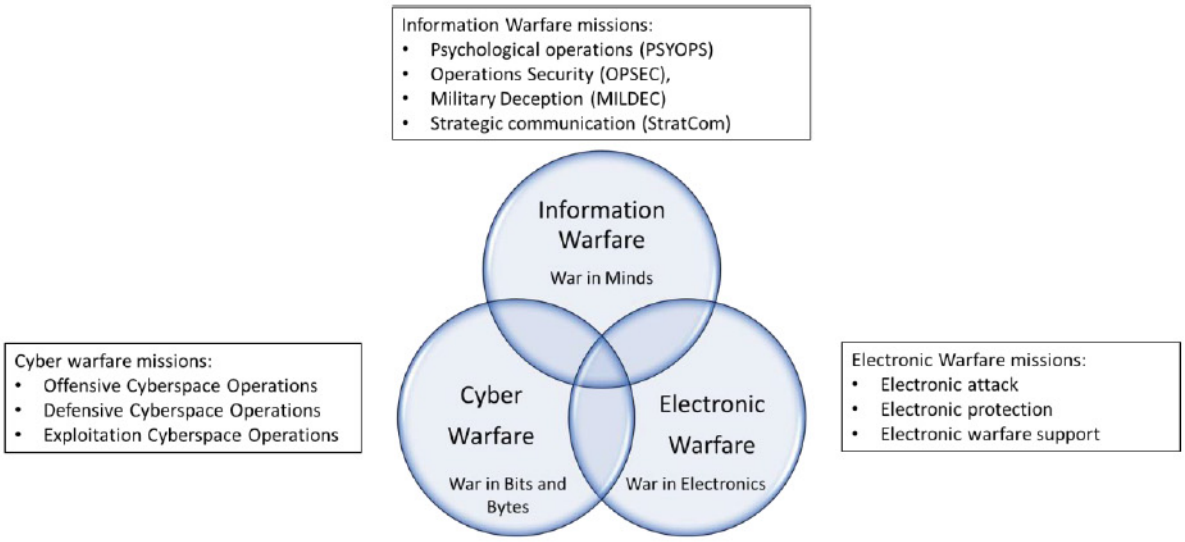

Figure 1: Non-kinetic Warfare Spectrum

By our definition Non-kinetic Warfare (NKW) is a comprehensive operational concept that is applied in interlaced, overlapping and integrated Electromagnetic Spectrum, Information Space and Cyber Space to enable the achievement of non-kinetic environment superiority. NKW enhances battle strength through the large-scale use of networked sensors, decentralized command and control systems, and large scale use of manned and unmanned weapon systems. The aim is to create shared awareness, speed up the process of decision-making and action, to increase military mission effectiveness, to improve the probability of survival among friendly forces, and to raise the level of self-synchronization in the execution of action and commands.

4. Non-Kinetic Warfare elements in warfare hierarchy

Within the military, there is a hierarchy of terms that define and delineate specific activities related to different levels of national security policy and military operations. They begin with "tactics" at the lowest level and move upward and outward to "grand strategy" at the highest level (Biddle, 2015).

In general, tactical level translates potential combat power into success in battles and engagements through decisions and actions that create advantages when in contact with or in proximity to the enemy. Operational level is concerned with employing military forces in a theater of war or theater of operations. Strategy (or theater strategy) concerns the direction of the largest military units in a battle space. So military strategy prescribes how military instruments per se are to achieve the goals set for them by grand strategy within a given theater of war. Grand strategy identifies and articulates a given political actor's security objectives at a point in time and describes how they will be achieved using a combination of instruments of power (military, diplomatic, and economic). (CADRE, 1997; Biddle, 2015)

In this study we have placed IW, EW and CW concepts on different levels of warfare. In addition, table 1 defines the notion of superiority in IW, EW and CW area. This definition is a combination from different sources (JP 3-13, 2016; DoD 2016; USAF, 2008; CADRE, 1997; Biddle, 2015; TRADOC, 2018).

Table 1: IW, EW and CW concepts on different levels of warfare

Level	IW	EW	CW
Grand Strategy	Nation is able, using Strategic Communications, to focus efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of national interests, policies, and objectives.	Nation can prevent electromagnetic spectrum attacks against critical information infrastructures in all situations.	Nation can prevent cyber space attacks against critical infrastructures and vital functions in all situations and strengthen national cyber resilience.
Strategy	Ensuring the Armed Forces can achieve strategic outcomes (ends) in its missions in a contested information space.	Ensuring the Armed Forces can achieve strategic outcomes (ends) in its missions in a contested electromagnetic spectrum.	Ensuring the Armed Forces can achieve strategic outcomes (ends) in its missions in a contested cyber space.
Operational	The operational level focus is on employing military forces in a theater of war of information space to obtain an advantage over the enemy and thereby attain strategic goals through the ways, means and ends, design, and conduct of campaigns and major information operations.	The operational level focus is on employing military forces in a theater of war of electromagnetic spectrum to obtain an advantage over the enemy and thereby attain strategic goals through the ways, means and ends design, and conduct of campaigns and major EW operations.	The operational level focus is on employing military forces in a theater of war of cyber space to obtain an advantage over the enemy and thereby attain strategic goals through the ways, means and ends design, and conduct of campaigns and major cyber operations.
Tactical	At a tactical level the military forces will be employed in a series of information operations to accomplish a common objective in a given time and space. Tactical level information operations translate potential capability into success in battles and engagements through decisions and actions that create advantages in information space.	At a tactical level the military forces will be employed in a series of electromagnetic spectrum operations to accomplish a common objective in a given time and space. Tactical level electromagnetic spectrum operations translate potential capability into success in battles and engagements through decisions and actions that create advantages in electromagnetic spectrum.	At a tactical level the military forces will be employed in a series of cyber operations to accomplish a common objective in a given time and space. Tactical level cyber operations translate potential capability into success in battles and engagements through decisions and actions that create advantages in cyber space.
Superiority	The degree of superiority is a dynamically changing state that arises from the adaptive behaviors of people and their use of information systems over time. The degree and nature of information superiority is always in flux, there is no final goal and no end-state.	The degree of superiority in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting an adversary's ability to do the same.	The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by military forces at a given time and place without prohibitive interference by an adversary.

NKW combines IW, EW, CW at different levels of warfare. From the point of view of the management and execution of warfare, the NKW Joint Operation Concept must be established so that all non-kinetic capabilities can be used effectively throughout the non-kinetic environment. The objective of NKW Joint Operation Concept is to guide the transformation of the future joint force. The concept should produce non-kinetic capabilities that render previous ways of warfighting obsolete and may significantly change the measures of success in military operations overall. (DoD, 2005)

5. Summary

For historical reasons EW, IW and CW are often used interchangeably, nested and differently subordinate to each other. This paper argues that, there is a large overlap between EW, IW and CW, and they form a new Non-Kinetic Warfare environment.

Moreover, the paper posits that CW goes beyond the boundaries of traditional IW, where in CW the battle is in bits and bytes, while in IW the battle is in human's mind. EW covers all communication, data transmission and utilization in EMS.

The integrated employment of the core capabilities of EW, IW and CW in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, usurp, paralyze or even destroy adversarial human and automated decision-making while protecting our own and finally the adversary's ability to wage war.

The structural reorganization is now underway. For example the mission statement of U.S. Army Cyber Command now reads that it "integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries." (Crane, 2019)

This means that the integration of all operations in the electromagnetic spectrum and digital environment, i.e. the realm of digital and electronic communications systems and the information conveyed through them, becomes increasingly necessary.

References

AFDD 2 (2017). The Air Force Doctrine Document 2, April 3, 2017
Allen J. & Hussain A. (2018) On Hyper War, Fortunas Corner, 2 January 2018
Arnold J. (2009) Where Cyber and Electronic Warfare Operations Coexist, A Research Report, Air War College, Air University, Montgomery, Alabama, 17 February 2009
Arquilla J. and Ronfeldt D. (1993) Cyberwar is Coming! Comparative Strategy, Vol 12, No. 2, Spring 1993, pp. 141–165. Taylor & Francis
Biddle T. D. (2015) Strategy and Grand Strategy: What Students and Practitioners Need to Know, The United States Army War College, December 2015
CADRE. (1997) Three Levels of War, Air and Space Power Mentoring Guide, Vol. 1, USAF Air University, Air University Press
Colarik A. M., Janczewski L. (2012) Establishing Cyber Warfare Doctrine, Journal of Strategic Security, 5 (1), pp. 31-48
Crane C. (2019) The United States Needs an Information Warfare Command: A Historical Examination, June 14, 2019
De Martino A. (2018) Introduction to Modern EW Systems, Second Edition, Artech House
DHS. (2018) Cybersecurity Strategy, May 15, 2018
DoD. (2016) DoD Strategy for Operations in the Information Environment, June 2016
DOD. (2005) Capstone Concept for Joint Operations Version 2.0, August 2005
Everstine B. (2019) USAF Developing "Cyber Flight Plan" to Determine Intel's Future, Air Force Magazine, September 4, 2019
Farooq U. (2014) My Perspective on Non-Kinetic Warfare, September 12, 2014 https://www.linkedin.com/pulse/20140912094416-299391920-my-perspective-on-non-kinetic-warfare-selections-from-my-talk/
Government of Canada. (2010) Canada's Cyber Security Strategy
Healey J. (2019) Why the new Air Force's cyber and information strategy is a return to the past, FifhtDomain, February 11, 2019
Hutchinson W. (2006) Information Warfare and Deception, Informing Science Volume 9, pp. 213-223
IWP. (2019) Information Operations and Information Warfare, the Institute of World Politics (IWP), https://www.iwp.edu/courses/information-operations-and-information-warfare/
ITU. (2012) National Cybersecurity Strategy Guide, Geneva, 2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
JD 3-16. (2016) Joint Doctrine Note 3-16, Joint Electromagnetic Spectrum Operations, 20 October 2016
JP-1. (2017) Joint Publication 1, Doctrine for the Armed Forces of the United States, 25 March 2013, incorporating Change 1, 12 July 2017
JP 1-02. (2016) Department of Defense Dictionary of Military and Associated Terms, 8 November 2010, as amended through, 15 February 2016
JP 3-0. (2018) Joint Publication 3-0, Joint Operations, 17 January 2017, incorporating change 1, 22 October 2018
JP 3-12R. (2018) Joint Publication 3-12R, Cyberspace Operations, 8 June 2018
JP 3-13. (2016) Joint Publication 3-13, Information Operations, 28 April 2016

JP 6-01. (2012) Joint Publication 6-01, Joint Electromagnetic Spectrum Management Operations, 20 March 2012
Klimburg A. (Edit.). (2012) National Cyber Security Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence
Kukkola J., Nikkarila J-P. Ristolainen M. (2017) Asymmetric frontlines of cyber battlefields in Game Changer Structural transformation of cyberspace, Finnish Defence Research Agency Publications 10, 2017, pages 69-122
Lehto M. (2015) Phenomena in the Cyber World, in M. Lehto, P. Neittaanmäki (Edit.) Cyber Security: Analytics, Technology and Automation, Springer, Berlin, pages 3-29, 2015
Libicki M. C. (1995) What is information Warfare? National Defence University, August 1995
Libicki M. C. (2009) Cyberdeterrence and Cyberwar, RAND, 2009
Libicki M. C. (2011) The strategic Uses of Ambiguity in Cyberspace, Military and Strategic Affairs Volume 3, No. 3, December 2011, pages 3-10
Libicki M. C. (2012) Cyberspace Is not a Warfighting Domain, Journal of Law and Policy for the Information Society, Vol 8:2, 2012, pp. 321-336
Libicki M. C. (2014) Why Cyber War Will Not and Should Not Have Its Grand Strategist, Strategic Studies Quarterly, Spring 2014, pages 23-39
Ministry of Defence. (2018) Cyber and Electromagnetic Activities, Joint Doctrine Note 1/18, February 2018
Mirenda, R. J. (2011) Offensive Cyber Warfare, Marine Corps Gazette September 2011
MOP 30. (1993) Memorandum of Policy Number 30. Chairman of the Joint Chiefs of Staff, March 1993
Pomerleau M. (2019) How the Air Force has reorganized its cyber staff, Fifth Domain, September 20, 2019
NSD-42. (1990) National Security Directive 42, July 5. 1990
PDD-63. (1998) Presidential Decision Directive/NSC-63 May 22, 1998
RAND. (2019a) Information Operations, https://www.rand.org/topics/information-operations.html,
RAND. (2019b) Cyber Warfare, https://www.rand.org/topics/cyber-warfare.html
Reimer J. (2010) U.S. Cyber Command preparations under way, general says, American Forces Press Service, March 17, 2010
Smart S. J. (2011) Joint Targeting in Cyberspace, Air & Space Power Journal, Winter 2011
TRADOC. (2018) The U.S. Army Concept for Cyberspace and Electronic Warfare Operations 2025-2040, Pamphlet 525-8-6, January 2018
Tuck C. (2019) Technology, Uncertainty, and Future War, RealClearDefense, March 11, 2019
USAF. (2008) Air Force Cyber Command Strategic Vision, February 2008
Wardrop C. (2018) Bridging the gap between cyber strategy and operations: a missing layer of policy, Australian Defence Force Journal, No. 204, 2018, pp. 61-69
Wilson C. (2007) Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues, CRS Report for Congress, March 20, 2007
Wooding C. (2019) The Rise of Cyber and the Changing Nature of War, Grounded Curiosity Blog, September 1, 2019

Ion A. Iftimie is an Eisenhower Fellow at the NATO Defense College in Rome. Formerly, he served as a Senior Cyber Planner at the United States Cyber Command. He is a graduate of the Harvard Kennedy School Executive Program in Cybersecurity Policies and of the Swedish Defense University Senior Course on Security Policy.

Abdul Bashiru Jibril is a PhD Candidate at the Faculty of Management and Economics, Tomas Bata University in Zlin, Czech Republic. He received his MSc. in Management and Marketing from the same University in 2018. He is a senior research assistant and a team leader of a Faculty-wide project. His main research areas are internet marketing, consumer behavior, and brand management.

Mr. Abiud Jimenez is a principal electrical engineer at Dynetics, Inc. He received his Master in Systems Engineering from SMU in 2006 and his BSEE from UTRGV. His main research involves studying effects on wireless communications systems caused by intended and unintended interference from electromagnetic waves.

Dr Keith Joiner joined the Air Force in 1985 and became an aeronautical engineer, project manager and teacher over a 30 year career before joining the UNSW in 2015 as a senior lecturer in test and evaluation. His expertise includes Defence Test and Evaluation of complex systems and platforms, their acquisition, design acceptance and operational acceptance, including to varying extents land, maritime, aerospace and joint systems and platforms.

Jennyphar Kahimise is a Master of Computer Science student at the Namibia University of Science and Technology (NUST). Her research interests includes Human Computer Interaction, Children safety online and cybersecurity.

Omer Faruk Keskin is a Ph.D. Student in Engineering Management and a Graduate Assistant in Old Dominion University. He holds an MS Degree in engineering management and a BS degree in systems engineering. His research is focused on risk and reliability analysis of critical infrastructure cyber physical systems.

Minchul Kim is a researcher of Agency for Defense Development, South Korea. He is currently in an integrated PhD program in Korea University. His main research areas are integrated cyber situational awareness system and algorithmic optimization.

Mr. Neal Kushwaha is the founder and CEO of IMPENDO Inc, a cyber security and data centre consulting firm in Canada. Annually, he hosts a conference in Ottawa, Canada called DCAR. During his spare time, he climbs big mountains in the Himalayas. Neal is also a recipient of the Silver Medal of Bravery.

Dr Michael Adu Kwarteng is an Assistant professor of Marketing and Management at Tomas Bata University in Zlin, Czech Republic. He received his PhD in Marketing from Tomas Bata University in 2018. His research interest is primarily centred on the application of internet in marketing and currently researching on online buying behaviour of customers in both developed and developing economies

Maxime Lagrasse is a French student from the Bordeaux Institute of Technology (Bordeaux-INP) working towards a five-year engineering degree, in the form of a special curriculum, with half-time lecture attendance and half-time work in a company as a system and network administrator.

Mr. Hyong Lee is a Senior Policy Analyst with NDU's Center for Applied Strategic Learning. His career includes being a Presidential Management Intern with the Army Cost and Economic Analysis Center and Chief, Decision Support Branch at US Pacific Command. He joined NDU in 2002 and provides gaming support to the College of Information and Cyberspace.

Dr. Martti Lehto, (Military Sciences), Col (GS) (ret.) works as a Professor (Cyber security) in the University of Jyväskylä. He has over 40 years' experience in C4ISR Systems in Finnish Defence Forces. Now he is a Cyber security and Cyber defence researcher and teacher and the pedagogical director of the Security and Strategic Analysis MSc. program. He is also Adjunct professor in National Defence University in Air and Cyber Warfare. He has over 140 publications on the areas of C4ISR systems, cyber security and defence, information warfare, artificial intelligence, air power and defence policy.

Naemi Gerson is a Master of Computer Science student at Namibia University of Science and Technology (NUST). She is a holder of Bachelor of Computer Science (Honours) in Information Security, Bachelor Degree in Information Technology majoring in System Administration and Networks as well as a Diploma in Information Technology from the same university.

Prof. Virginia Greiman is an international scholar and expert in the fields of International Law and Development, National Security, and Global Cyber Law and Governance. She holds academic appointments at Boston University and Harvard University Law School, and has held high level appointments in the U.S. Department of Justice.

Dr. Ahmad Ghafarian has a B.S. in mathematics a M.SC. and Ph.D. in computer science. He is Professor of computer science and teaches computer science and cybersecurity courses at the University of North Georgia, USA. Dr. Ghafarian's research interests include various areas of cybersecurity and has several publications to his credit.

Gayne Grigoryan is a Ph.D. student and a graduate project assistant in the Engineering Management and Systems Engineering Department at Old Dominion University (ODU). She received her master's degree in Economics from ODU. Her research focuses on game theoretical analysis of employee generated cyber risk with an emphasis on economics of employee misbehavior.

Gerhard Henselmann, Dipl.-Ing. MBA, graduated Flight test Engineer was educated in Aerospace Engineering at Technical University of Munich/Germany and is working over 35 years in aerospace with expert experience in testing, flight testing of airborne military platforms and has a wide experience in avionics, electronic warfare and self-defense of military platforms. He started his PhD studies in summer 2016 at the University of Jyväskylä on Cyber Security.

Vincent Homburg is associate professor in Public Administration at Erasmus University Rotterdam. He has written nearly one hundred journal articles, book chapters and books on topics at the corner stones of public management and e-government.

Michael Bennett Hotchkiss has research interests in the study of Information Warfare, Propaganda, Disinformation, and the History of Espionage. Michael possesses a Master of Organization Development degree (M.O.D.) from Bowling Green State University (USA), and a Bachelor of Arts in Industrial Psychology (minor Criminal Justice, Phi Beta Kappa honors) from University of Connecticut (USA).

Guy Howard has worked at IntelliGenesis for 12 years, 3 as Lead AI Engineer. Prior to that he was lead engineer and team lead for multiple software development projects. Primary areas of responsibility are technical leadership, mentoring, and professional development for engineers within the company. Holds a BS degree in Computer Engineering and an MS in Technical Innovation Management.

Nicolas Hughes is an assistant public defender at the Harris County Public Defender's Office in Houston, Texas. He is currently pursuing a master's degree in Digital Forensics at Sam Houston State University. His work focuses on the use and misuse of forensic science in the courtroom. His main research areas interests are the application of metrology and formal validation to digital forensics.

Dr. John Hurley has over 35 years' experience in ICT. He is currently Professor, National Defense University (NDU), focused on Data Analytics and Cyberspace Strategy. He is former Senior Manager, Distributed Computing in the NSD, at Boeing. He is a 2015 Seminar XXl Fellow. Hurley heads NDU initiative on Emerging and Disruptive Technologies Leadership.

Gazmend Huskaj is former Director of Intelligence at the Swedish Armed Forces on cyber-related issues. Previously, he was Head of the United Nation's Intelligence unit in a mission area for several years. He is currently a Doctoral student at the Swedish Defence University and holds a Master of Science (MSc) in Information Security from Stockholm University in Stockholm, Sweden, and a MSc in Security and Risk Management from the University of Leicester in Leicester, U.K. He is also an ISACA Certified Information Security Manager (CISM).

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.