DOI: 10.53477/1842-9904-22-6

INFORMATION OPERATIONS CONDUCTED BY ARMED FORCES – CONCEPTS, METHODS AND POTENTIAL DEVELOPMENTS

Mihai VLAICU*

The increased level of integration of electrical and electronic-based devices and systems in the military field has led to the development of better methods of using information in real time, but at the same time has introduced new vulnerabilities to exploit, degrade and deny the information flow between military units and/or different types of weapon systems. The purpose of this paper is to identify key concepts and methods of using information warfare, specifically, CEMA (Cyber Electromagnetic Activities) operations by the armed forces of various nations (the United States of America, People's Republic of China and Israel) and to formulate several potential developments with regards to the future of information operations.

Keywords: *information operations; cyber operations; electronic warfare; Cyber Electromagnetic Activities (CEMA).*

Introduction

Basically, information warfare is a concept that has been used for centuries, in order to discredit or deceive an adversary's forces or population (Nick-Brunetti-Lihach 2018). However, with the acceleration of technological progress that characterizes the 20th and 21st centuries, information warfare has been expanded in order to integrate new methods, based on electronic or electromechanical devices. The first types of these devices were computers based on vacuum tubes, such as

**** Mihai VLAICU is a Master Student in the field of Security and Diplomacy within the National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania. E-mail: vlaicumihai@gmail.com***

Colossus (Crypto Museum n.d.), based on electrical circuits (Ellsbury 1998). Thus, it can be argued that from its very inception, the cybernetics domain has intertwined with the electrical domain, the research and development (R&D) efforts being poured into one of those having a considerable amount of importance on the R&D efforts of the other. One of the things that needs to be clarified is that the aforementioned device was used by organisations focused on military intelligence processing (in this case, the Government Code and Cypher School(GC&CS) (Marsh 2019), the military being thus the primary customer of electronics-based information processing technology.

The development of the transistor has given ways for electronics to become miniaturized, cheaper, more energy-efficient, more modular, and most importantly, able to transmit, receive and manage a growing level of data, in a multitude of formats. Some of the well-known transistor-based innovations in the electronics domain that were and still are important in the cyber domain, are the integrated circuit and the programmable logic device (Dobriceanu 2012), the development of the information-based society being impossible without multiple principles developed in electrical engineering.

The proliferation of integrated circuits has led to their integration in security and military oriented organisations, these types of institutions often being at the forefront of technological development in electronics. This integration manifested itself in many ways, from computers to satellite-based systems. One of the common traits in the adoption of these devices in the military field, irrelevant of their type, is the measure-countermeasure cycle, the military of one nation introducing precision guided munitions, while the armed services of another developing and implementing principles and methods for degrading the efficiency of, or completely disabling, the aforementioned type of weapon systems. It should be noted that, although largely overlooked, computer networks are also a type of weapon systems, even though their effects could be interpreted mostly as non-kinetic. Thus, the information field started being acknowledged as an equal part of military operations (Kozloski 2009). Information operations are an evolving type of concepts, with different armed services having different interpretations of these actions.

The methodology used has been that of researching the development of cyber and electromagnetic capabilities of three case studies (US military forces, Iran and Israel), and the development of prospective studies, with regards to countering the mass usage of these capabilities, in the case of a large scale conflict between superpowers.

1. United States Armed Forces

Some of the first armed forces to take the lead in information warfare are those of the United States. By itself, this is an unsurprising fact, considering:

- that most of the innovations described in this paper were developed in the U.S.;

- one of the agencies of the U.S. Department of Defense, the Advanded Research Projects Agency, developed the first type of computer network in the world and proceeded to integrate it into the armed services (Norman n.d.).

The United States Armed Services are the first to introduce the concept of information operations, being mentioned in JP 3-13, as the "integrated employment of electronic warfare, computer network operations, psychological operations, military deception and operations security" (Joint Chiefs of Staff 2006). For the purpose of this paper, emphasis will be placed on the first two types of actions.

According to JP 3-12, cyber operations consist of three main categories (Joint Chiefs of Staff 2018):

- offensive (OCO);
- defensive (DCO);
- administrative (DODIN).

Firstly, the US Armed Forces, in contrast with the other examples in this paper, postulate the fact that cyber administrative duties, related to the processing of information into data and data dissemination is a type of action different from defensive actions.

Secondly, the reason for such a difference in this military system must be considered. Some of the first orders regarding the organizing of the military structure responsible with conducting cyber operations may present a valuable clue. Thus, military cyber offensive capabilities and DoD networks defence capabilities were allocated to the U.S. Cyber Command (United States Strategic Command 2018), cyber and signals intelligence operations, cryptographic activities and national cyber defensive actions were delegated to the National Security Agency (National Security Agency Central Security Service n.d.), whilst maintaining the developing DoD information processing and communications infrastructure remained under the leadership of the Defense Information Systems Agency (Defense Information Systems Agency n.d.).

Offensive cyber operations carried out by the US Armed Forces, or as they are more commonly known computer network operations, are conducted through multiple organisations, the most important of which is the US Cyber Command. This Command, although designated as a unified combat command (United States Cyber Command 2018), is actually composed of the cyber command of each service (United States Cyber Command n.d.), being responsible for creating the framework and distributing resources for the subordinate commands to execute specific operations. For the purpose of this paper, it should be mentioned the fact that although mostly known for the strategic level, offensive actions taken against various non-state actors, US Cyber Command has also the mission, per USCYBERCOM Announcement Message to "planning Operational Preparation of the Environment (OPE), and as directed, executing OPE or synchronizing execution

of OPE in coordination with the Geographic Combatant Commanders (GCC)." (National Security Agency Central Security Service n.d.). As such, the US Cyber Command is tasked with executing military, tactical and operational level cyber offensive operations against designated targets, in close coordination with kinetic, military operations conducted during a war.

It should be noted that, although at the level of the GCC and the armed services, cyber and electronic operations are to be employed in an unified manner (Joint Chiefs of Staff 2006), the organizational chart of the organizations supporting joint electronic warfare from JP 3-13.1 (Joint Chiefs of Staff 2006) or through that of the US Cyber Command (United States Cyber Command n.d.) shows the fact that these types of operations are not to be conducted from the same military unit or agency of the DoD, thus raising questions regarding the level of coordination that these types of operations would be characterized of, during an interstate, declared conflict.

Electronic warfare is one of the oldest types of electronics based military actions, its foundation being laid in the Second World War, with the development of radar type systems and of electronic countermeasures in order to degrade the capabilities of these weapons. As described in ATP 3-36, electronic warfare "involves the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy" (Headquarters, Department of the Army 2014). As already mentioned, EW is associated with two other types of operations, "cyberspace operations and spectrum management operations" (Headquarters, Department of the Army 2014), forming a distinct type of operations being known as "cyber electromagnetic activities." (Headquarters, Department of the Army 2014). In one other publication, FM 3-12, the U.S. Army reinforces the degree of connectivity between electronic and cyber types of operations, cyberspace being defined as a multitude of "networks that make information globally available through wired and wireless connections" (Headquarters, Department of the Army 2017), whilst electronic warfare being described as having "effects by affecting devices that operate in and through wired and wireless" (Headquarters, Department of the Army 2017), both of these types of actions operating, thus, through the same media. From these examples, it can be concluded that there is a consensus, at least among United States Army senior command staff, on the integrated usage of cyber warfare, electronic warfare, and spectrum management types of actions. The United States Armed Forces can be considered the first to realize the potential of bringing together cyber and electronic warfare operations into a single, general operational domain.

In contrast with the conduct of cyber operations, electronic warfare operations are not employed by a single command or military unit, being distributed across the United States Armed Forces. Also to be noted is the fact that most electronic operations conducted by these armed services were mainly directed towards degrading or denying adversary forces of communication and coordination, electronic defence measures are mainly composed of encrypted communications.

The platforms used by the US military for conducting information operations, in general, and CEMA type of operations, in particular, are varied, ranging from air assets such as EC-130 or EA-18G to land based forces such as Terrestrial Layer System. One fact to be taken into consideration is that whilst the first two types of platforms are used mainly in electronic warfare and signals intelligence (SIGINT) type of operations, the latter, composed of two distinct subsystems, the TLS-EAB and TLS-BCT, is created with the main purpose of integrating cyber and electronic operations. Thus, the stated objectives of the TLS system-of-systems are the provision of "defensive electronic attack" (Pomerleau 2020) and of "radio frequency-delivered cyber effects" (Pomerleau 2020), representing, in itself, the integration of principles in the aforementioned publications, bringing the first such merger of cyber and electronic warfare actions at the operational level. To be noted that the two aforementioned types of operations could be used to infiltrate, degrade or destroy the components of an adversary's weapon systems', ranging from avionics to electronic fuse.

One of the earliest implementations of CEMA-type operations took place during the 1991 Desert Storm and Desert Shield operations. Even though the airstrikes conducted during this campaigns remained representative of US involvement in the Gulf, they were preceded by a significant level of electronic warfare actions directed against Iraq's air defence systems (Mann 1994), thus diminishing their level of effectiveness in the early hours of military operations. One of the key issues, overlooked by CEMA operations was the usage of the BLU-114/B bomb by the United States Armed Forces in order to destroy Iraq's electrical power grid (BBC News 2003). The usage of a weapon of this sort, in conjunction with the use of electromagnetic pulses, would most likely affect a future adversary's capability to wage war.

However, the cyber component of the US Armed Forces was not used until recently during a military conflict or in conjunction with kinetic military operations against another state. Thus, in 2019, with an increased level of tension between the United States and Iran, President Donald Trump ordered the armed forces to conduct cyber operations against a series of Iranian military and paramilitary targets (Hanna 2019). Although it is one of the first direct examples of a state using cyber weapons in order to destroy targets of another state, it was conducted as a stand-alone measure.

As a conclusion, the United States has a capable military system that could execute CEMA activities in order to degrade or destroy an adversary's military capabilities. Although employed, at the time of writing this paper, as stand-alone measures, electronic and cyber operations conducted by the US Armed Forces have proven to be effective, integration of these methods being planned for the near future.

2. People Liberation's Army

The "Shock and awe" campaign led by the coalition forces in the First Gulf War had a long-lasting effect on the military and political elites in the People's Republic of China, leading to emphasis being placed on "informatizing" the formations of the People's Liberation Army. The military and, overall, the national strategy used in the last 20 years, is available to be discovered through informal publications, such as Unrestricted Warfare, by colonels Qiao Liang and Wang Xiangsui, or the "Challenge of Information Warfare", by Major General Wang Pufeng. The overarching theme of these papers is the fact the PRC does not necessarily make a clear distinction between tactical, operational and strategic use of information warfare, thus continuing the concept of "people's war", developed by Mao Zedong. However, in both of these papers there are elements that show a logical evolution of the comprehension of "information warfare" as a concept.

First of all, general Pufeng sees Information Warfare as "offensive" (Pufeng 1995) and "defensive" (Pufeng 1995). In the first category, he places actions that could be regarded, in our time, as non-kinetic elements of C4 ISTAR such as "information reconnaissance" (Pufeng 1995) or "electronic interference" (Pufeng 1995), or as kinetic ones, such as "information suppression by using counter radiation guided missiles to destroy air defence radar stations" (Pufeng 1995) or "information attack by using precision guided-warheads to attack pre-set targets" (Pufeng 1995). While the first and second type of actions could be presented as elements of information warfare, the third and fourth are mainly kinetic actions which do not, by themselves, constitute parts of information warfare, precision-guided munitions being a part of warfare since, at least, World War I. With regards to defensive information warfare, the general uses actions such as "counter reconnaissance" (Pufeng 1995), "multiple-communication methods" (Pufeng 1995), "resist viruses" (Pufeng 1995) in order to describe IW, elements that could be classified as part of modern-day information operations, together with the more ambiguously termed "information counterattack" (Pufeng 1995). One of the facts that should be remembered is that this paper was published in 1995, four years after the US-led Coalition removed the Iraqi Armed Forces from Kuwait, this period of time being a possible reason for why the PLA did not have a clearly defined concept regarding information warfare.

A remarkable leap forward is represented by "Unrestricted Warfare", published in 1999. This paper shows a clear cognitive evolution, presenting "weapons" that are nowadays associated with information operations such as "computer logic bombs, network viruses, or media weapons" (Liang and Xianqsui n.d.) as information weapons. Even more interesting is the fact that it acknowledges the importance of CEMA operations, regarding "the network space" (Liang and Xianqsui n.d.) as being formed from "electronics technology, information technology and the application of

specific designs." (Liang and Xianqsui n.d.). Another aspect of this paper is that it illustrates the willingness of the PLA, at the turn of the century, to combine various types of warfare in order to achieve the CCP's and its goals, acknowledging the fact that every one of these combinations are "all determined based upon a specific target" (Liang and Xianqsui n.d.). This last quote is particularly important because it illustrates modern Chinese military thinking. Thus, in sharp contrast with NATO and US military thinking, in which almost every crisis is met with a mixture of information warfare and, accordingly, precision strikes, the PLA understands the fact that in every situation, whether considering, for example, the South China Sea or Central Asia, it deals with a different type of opponent, with a different set of tools and, ultimately, mentality to counteract. In essence, this approach represents the most capable and adaptable implementation of information warfare, using all available systems to disrupt, degrade or destroy an opponent's information and decision-making cycle.

One of the most important contributions to the development of information warfare in the PRC was that of Major General Dai Qingmin, who introduced the concept of Integrated Network Electronic Warfare. By itself, INEW can be perceived as the Chinese equivalent of CEMA activities, the differentiating factor between the two being the fact that whilst the second one ensured a balanced approach with regards to the conduct of military operations, the first one places emphasis on offensive actions (Krekel, Bakos and Barnet 2009). INEW must, at the same time, be seen in context. Western military thinking since the early 2000s has attached increasing importance towards the development and deployment of network centric warfare doctrines, systems and tactics. As such, Chinese military thinkers acknowledged this fact and, besides applying the concept for their own forces, developed possible avenues in order to counteract its advantages. NCW is built around the concept of shooters and sensors (Thales Group n.d.), the information and data from each platform being shared amongst the other deployed troops. In order to ensure its proper usage, the military force that uses this kind of doctrine has to ensure the security and integrity of its information sharing and processing capabilities, the Chinese thus, correctly, observing the fact that the most efficient method of countering this type of actions is by using CEMA activities, such as intercepting and jamming data links and exploiting any kind of vulnerabilities in the information security architecture of the adversaries' systems.

One of the turning points of recent Chinese military and strategic history is, without a doubt, the ascension of Xi Jinping to power. Whether considering the purges in the ranks of the PLA that took place under his leadership (BBC News 2017), the replacement of Jiang Zemin's Three Represents with his Four Comprehensives policy (Reuters 2015) and by placing his thought in the PRC Constitution, amongst the line of thought of other important Chinese autocrats, such as Mao Zedong and

Deng Xiaoping (Phillips 2017), Xi Jinping's ultimate goal is to ensure both his status as China's leader and the country recognition as a great power. In order to achieve both of this tasks, Xi Jinping recognized the importance of reforming the armed forces, initiating a purge in the ranks of military officers perceived as affiliated with the Jiang Zemin group and modifying the structural organization of the PLA.

Relevant to the subject of this paper, is the 2015 integration of the PLA's cyber, space and electronic warfare capabilities under the control of one organisation, the PLA Strategic Support Force (Ni and Gill 2019). The PLASSF has been created with regards to PLA's continued efforts to create a "smart force", but, in the same time, its potential could be more than that. One answer regarding its purpose could be by observing the basis and development of a similar organisation from abroad, in this case, the US STRATCOM. Until 2009, STRATCOM was the functional combatant command tasked with maintaining the US's main capabilities of strategic deterrence, the nuclear triad, the cyber capabilities and the space warfare capabilities. PLASSF is responsible for the main PLA units focused on cyber warfare, space warfare and electronic warfare, being the nucleus of a possible counterpart of the 2000-level STRATCOM, focused on providing an adequate level of deterrence for the PRC.

The PLASSF branch responsible for conducting cyber and electronic warfare capabilities is the Network Systems Department (Ni and Gill 2019), thus representing the importance granted by the PLA leadership towards creating a synergy of the service's CEMA capabilities.

PRC's alleged hacking actions were largely directed towards acquiring classified military and industrial secrets from foreign computer networks. The fact that the PLA has not taken part, recently, in any military conflicts abroad presents researchers of the topic with the open question of assessing this organization's cyber warfare capabilities during an open conflict, against another state's army.

While the military cyber capabilities of the PRC have been more documented, so far less emphasis has been placed on PLA's electronic warfare capabilities. One of the things to be noted is the fact that also, in this area, China's possible strategy closely matches US' doctrine and developments, with emphasis being placed on China's geographical location. Electronic warfare variants of JH-7 and J-16 aircraft platforms have been developed and could emphasise that the PLA plans to use EW capabilities in a tactical, potentially limited, role in a future, regional conflict.

3. Israel Defense Forces

Israel's approach to information warfare has to be seen in the light of its geopolitical situation. Israel has two types of opponents:

− state-based, with no direct border with Israel, such as Iran and Turkey;

− hybrid organisations that occupy territories directly bordering Israel, such as Hamas and Hezbollah.

After years of civil warfare, Syrian territory hosts Russian and Iranian military units. Also, in Syria, a significant number of Turkish and American military assets regularly conduct military operations. In the South and East, Egypt and Jordan have a balanced approach with regards to Israel, maintaining cooperation with the Jewish state on security related issues.

Other two important sources of instability are represented by the presence of Hamas and other militias on Palestinian Administration's territory and by the fact that the militant Shiite group Hezbollah continues to maintain its stronghold in Lebanon. The potential for cooperation between these two groups has increased recently, with cooperation ranging from political statements (Al Jazeera 2008) to sharing military equipment in order to test and degrade Israel's national security (Ahronheim 2018).

Although well known for their missile attacks towards Israeli territory, in recent years, both groups have diversified their methods of action, mainly in the information field. Both Hamas and Hezbollah have official, active cyber methods of promoting their causes among their members and possible adherents, mobilizing groups (Keyser 2018) (Martinez 2019) in different countries in order to attack Israel's perceived aggression against their interests. Information operations conducted by both these groups, in the past, have had two types of goals:

- extracting information, either from human or technical sources, through either infiltrating social media profiles or groups of interest (Perper 2018) or hacking into the live feeds of various information systems used by the Israeli government (The Times Of Israel 2016);

- manipulating Israeli public perception, conducted through defacing cyberattacks, DDoS, Zero-day or viruses (Shamah 2015).

One of the most notable characteristics of the actions of these groups is represented by the fact that, they have so far not used electronic warfare against Israeli targets or Israeli society. One possible explanation is that an electronic operation is much harder to conceal than a cyber-operation, IDF having the ability to trace back and destroy an EW target with a dedicated anti-radiation missile, a type of weapon that does not have an equivalent for a cybernetic target, the IDF having to use joint operations in order to track in real time and hit an opponent's cyber formations (Groll 2019).

On the other hand, Israel's strategic conflict with Iran (and, in the future, with Turkey) is largely limited, based on proxy forces and information operations. Iran has been the alleged source of a growing number of cyber operations against the Israeli society (AFP 2021) (Deutsche Welle 2022). Israel is also alleged to have deployed cyber weapons on multiple occasions, such as Stuxnet (The Times of Israel 2020) and the 2020 explosions which took place in Iranian strategic targets (The Times of Israel 2020).

The Israeli military-political leadership has used a different approach than the United States with regards to information warfare, establishing information

warfare, in particular, CEMA capabilities, both in the combat support forces and the intelligence services of the IDF. However, Israel has chosen to place emphasis on the development of cyber warfare and signal intelligence capabilities, with less information available to its electronic warfare capabilities.

The offensive cyber capabilities of the IDF have been placed within the competence of the Intelligence Corps (Stavridis 2019), its most well-documented unit being Unit 8200 (Stavridis 2019). Publicly available data on Unit 8200 presents the fact that, besides conducting cyberattacks, it also conducts signal intelligence tasks (spacewatch.global 2017), collecting data about the electronic communications and electronic signatures of potentially hostile Armed Forces, the unit being oriented towards employing CEMA capabilities in the case of a conflict.

The organisation tasked with the cyber-defence of the IDF is the Cyber Defense Directorate (Israel Defence Forces n.d.).

Conclusions and potential developments

All of the countries that were part of the case studies of this paper have developed their capabilities to a considerable level, where these can be used effectively both during peace and wartime. At the same time, the methods these countries have used for the development of their CEMA-centric information operations have been different, the US, China and Israel developing institutional frameworks in order to sustain and develop separately these capabilities.

The increased level of integration of electronic equipment in the military will increase exponentially in the coming years, and its effects on information warfare could be classified in the short-term, with an emphasis on the integration of EW, EMSO and cyber operations in order to gather intelligence or conduct remote hacking of an adversary's systems; increased use of cell phone simulators in information attacks targeting military and paramilitary personnel, in order to obtain intelligence or cause them to question orders; the continued pace of adapting existing weapon systems to, together with the design and use of new weapon systems focused around, concepts such as data/information exchange, will lead to vulnerabilities in the electronic field, more specifically, a system's ability to perceive the battlefield and share data with other platforms will be severely diminished, in case of a joint, sustained CEMA attack; in the medium term, the increased level of importance granted to EW and EMSO warfare will, most likely, determine either a communication "arms race", based on A.I., or the reintroduction of traditional methods of war communications, such as couriers, in case of long-term, strategic-level military operations; further research and development where the focus will be placed on the production, (wireless) distribution and storage of electricity, in order to combat the effects of an adversary's usage of electromagnetic impulse-effect or BLU-114/B type weapons.

BIBLIOGRAPHY:

AFP. 2021. *Iran-linked hackers attack Israeli targets: company.* 12 16. Accessed 04 11, 2022. https://www.france24.com/en/live-news/20211216-iran-linked-hackers-attack-israeli-targets-company.

Ahronheim, Anna. 2018. *Report: Hezbollah is helping Hamas build rocket factories, training camps.* Report: Hezbollah is helping Hamas build rocket factories, training camps.

Al Jazeera. 2008. *Hezbollah, Hamas chiefs meet to discuss Israel-Arab ties.* https://www.aljazeera.com/news/2020/9/6/hezbollah-hamas-chiefs-meet-to-discuss-israel-arab-ties.

BBC News. 2017. *Charting China's 'great purge' under Xi.* Accessed 10 18, 2020. https://www.bbc.com/news/world-asia-china-41670162.

—. 2003. *Fact file: Blackout bombs.* http://news.bbc.co.uk/2/hi/americas/2865323.stm.

C.M. Melliar-Smith, M.G. Borrus, D.E. Haggan, T.Lowrey, A.S.G. Vincentelli, W.W. Troutman. 1998. "The transistor: an investitor becomes big business." *Proceedings of the IEEE,Vol.86, Nr.1.* IEEE. 86-110.

Crypto Museum. n.d. *Colossus Birth of the digital computer.* https://www.cryptomuseum.com/crypto/colossus/index.htm.

Defense Information Systems Agency. n.d. *Our work, DISA 101.* https://disa.mil/About/Our-Work.

Deutsche Welle. 2022. *Apparent cyberattack on Israel disables government websites.* 03 14. Accessed 04 11, 2022. https://p.dw.com/p/48TT7.

Dobriceanu, Mircea. 2012. *Sisteme cu Microprocesoare.* Craiova: Editura Universitaria.

Ellsbury, Graham. 1998. *The Enigma Machine Its Construction, Operation and Complexity.* http://www.ellsbury.com/enigma2.htm.

Groll, Elias. 2019. *The Future Is Here, and It Features Hackers Getting Bombed.* https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Hanna, Andrew. 2019. *The Invisible U.S.-Iran Cyber War.* https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.

Headquarters, Department of the Army. 2014. "ATP 3-36 (FM 3-36) Electronic warfare techniques." *Headquarters, Department of the Army.* http://www.bits.de/NRANEU/others/amd-us-archive/atp3_36%2814%29.pdf.

—. 2014. "Field Manual 3-38 Cyber electromagnetic activities." *Federation of American Scientists.* https://fas.org/irp/doddir/army/fm3-38.pdf.

—. 2017. "FM 3-12 Cyberspace and electronic warfare operations." *Berlin Information-center for Transatlantic Security.* http://www.bits.de/NRANEU/others/amd-us-archive/FM3-12%2817%29.pdf.

Israel Defence Forces. n.d. *C4I and Cyber Defense Directorate.* https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/.

Joint Chiefs of Staff. 2006. "Joint Publication 3-13 Information Operations." *HSDL.* https://www.hsdl.org/?view&did=461648.

—. 2018. "JP 3-12 Cyberspace Operations." *Berlin Information-center for Transatlantic Security.* http://www.bits.de/NRANEU/others/jp-doctrine/jp3_12%282018%29.pdf.

—. 2006. "JP 3-13 Information Operations." *HSDL.* https://www.hsdl.org/?view&did=461648.

—. 2006. "JP 3-13 Information Operations." *Joint Chiefs of Staff.* http://www.bits.de/NRANEU/others/jp-doctrine/JP3_13.1%2812%29.pdf.

Keyser, Zachary. 2018. *The under-reported use of Hezbollah's Internet recruitment tactics.* https://www.jpost.com/middle-east/the-under-reported-use-of-hezbollahs-internet-recruitment-tactics-606682.

Kozloski, Robert. 2009. "The Information Domain as an Element of National Power." https://www.hsdl.org/?view&did=232244.

Krekel, Bryan, George Bakos, and Christopher Barnet. 2009. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." *National Security Archive.* Accessed 10 18, 2020. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

Liang, Qiao, and Wang Xianqsui. n.d. *Unrestricted Warfare.* 1999: PLA Literature and Arts Publishing House.

Mann, Edward. 1994. "Desert Storm: The First Information War?" *Aerospace Power Journal, Volume 8, Nr.1*, 9-15. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-08_Issue-1-Se/1994_Vol8_No4.pdf.

Marsh, Allison. 2019. *The Hidden Figures Behind Bletchley Park's Code-Breaking Colossus.* Accessed 10 18, 2020. https://spectrum.ieee.org/the-hidden-figures-behind-bletchley-parks-codebreaking-colossus.

Martinez, Hector. 2019. *Hashtaggers For Hezbollah? How Social Media Fundraising Can Skirt The Rules.* https://www.bellingcat.com/news/2019/08/27/hashtaggers-for-hezbollah-how-social-media-fundraising-can-skirt-the-rules/.

National Security Agency Central Security Service. n.d. *Mission & Values.* https://www.nsa.gov/about/mission-values/#:~:text=The%20National%20Security%20Agency%2FCentral,order%20to%20gain%20a%20decision.

—. n.d. "Mission & Values." *National Security Agency Central Security Service.* https://www.nsa.gov/about/mission-values/#:~:text=The%20National%20Security%20Agency%2FCentral,order%20to%20gain%20a%20decision.

Ni, Adam, and Bates Gill. 2019. "The People's Liberation Army Strategic Support Force: Update 2019." *China Brief, Volume 19, Nr.10.*

Nick-Brunetti-Lihach. 2018. *Information Warfare Past, Present and Future.* https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html.

Norman, Jeremy. n.d. *ARPANET Splits into ARPANET and MILNET.* https://www.historyofinformation.com/detail.php?id=976.

Perper, Rosie. 2018. *Hamas reportedly created a fake dating app to lure Israeli soldiers and steal security information.* https://www.businessinsider.com/hamas-fake-dating-app-scam-israeli-soldiers-honeypot-glancelove-2018-7.

Phillips, Tom. 2017. *Xi Jinping becomes most powerful leader since Mao with China's change to constitution.* Accessed 10 18, 2020. https://www.theguardian.com/world/2017/oct/24/xi-jinping-mao-thought-on-socialism-china-constitution.

Pomerleau, Mark. 2020. "US Army to upgrade bigger units with new electronic warfare gear." *C4ISRNET.* https://www.c4isrnet.com/electronic-warfare/2020/10/01/us-army-to-upgrade-bigger-units-with-new-electronic-warfare-gear/.

Pufeng, Wang. 1995. "The Challenge of Information Warfare." *China Military Science.* https://irp.fas.org/world/china/docs/iw_mg_wang.htm.

Reuters. 2015. *After the 'Three Represents', China pushes 'Four Comprehensives'.* 2020 10. Accessed 18. https://www.reuters.com/article/us-china-doctrine-idUSKBN0LU0A620150226.

Shamah, David. 2015. *Official: Iran, Hamas conduct cyber-attacks against Israel.* https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

spacewatch.global. 2017. *ISRAEL'S CYBER WARFARE OUTFIT-UNIT 8200 GETS NEW COMMANDER.* https://spacewatch.global/2017/04/israels-cyber-warfare-outfit-unit-8200-gets-new-commander/.

Stavridis, Virginia. 2019. *Six Cybersecurity Questions Answered by the 8200 Unit.* https://www.cybintsolutions.com/six-cybersecurity-questions-answered-by-the-8200-unit/.

Thales Group. n.d. *Sensor to Shooter.* Accessed 10 18, 2020. https://www.thalesgroup.com/en/sensor-shooter.

The Times Of Israel. 2016. *Hezbollah: We hacked into Israeli security cameras.* https://www.timesofisrael.com/hezbollah-we-hacked-into-israeli-security-cameras/.

The Times of Israel. 2020. *Israel's alleged Natanz strike 'as complex as Stuxnet', a major blow to Iran.* https://www.timesofisrael.com/israels-alleged-natanz-strike-as-complex-as-stuxnet-a-major-blow-to-iran/.

United States Cyber Command. 2018. "Achieve and Maintain Cyberspace Superiority." *United States Cyber Command.* https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf.

—. n.d. “Components.” *United States Cyber Command.* https://www.cybercom.mil/Components.aspx#:~:text=Components&text=United%20States%20Army%20Cyber%20Command,the%20same%20to%20our%20adversaries.

—. n.d. *Components.* https://www.cybercom.mil/Components.aspx#:~:text=Components&text=United%20States%20Army%20Cyber%20Command,the%20same%20to%20our%20adversaries.

United States Department of Defense. 2020. “United States Department of Defense Electromagnetic Spectrum Superiority Strategy 2020.” *United States Department of Defense.* https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.

United States Department of Defense-Joint Chiefs of Staff. 2021. “DOD Dictionary of Military and Associated Terms.” *Joint Chiefs of Staff.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

United States Strategic Command. 2018. *JP 3-12 Cyberspace Operations.* https://nsarchive.gwu.edu/dc.html?doc=2692108-Document-6.