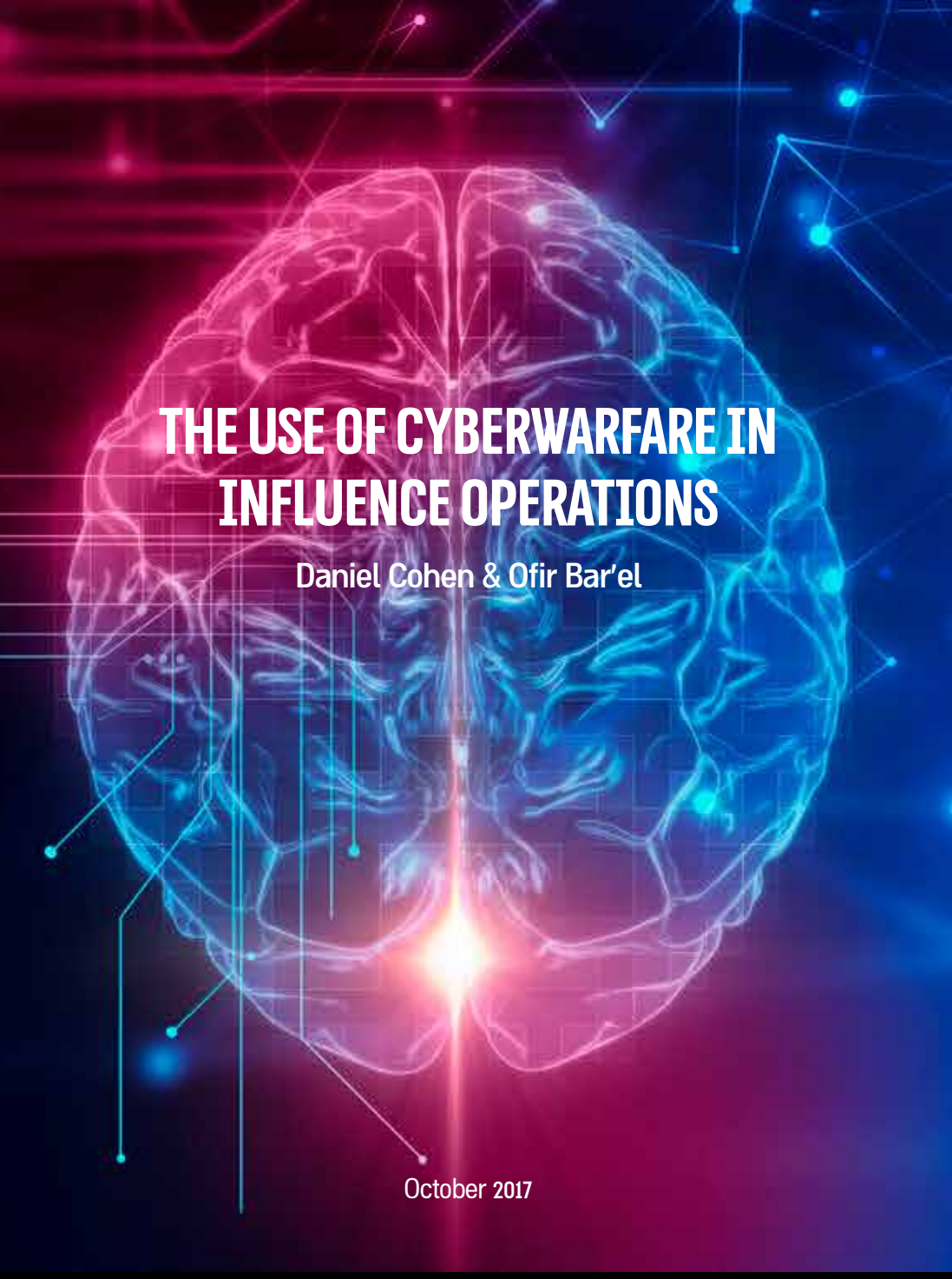

THE USE OF CYBERWARFARE IN INFLUENCE OPERATIONS

Daniel Cohen & Ofir Bar'el

October 2017

ICRC
Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University

THE USE OF CYBERWARFARE IN INFLUENCE OPERATIONS

Daniel Cohen & Ofir Bar'el

October 2017

ICRC
Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

Table of Contents

Foreword

In the world of cybersecurity, collaborative efforts are difficult, even in areas where the common interest is indisputable. It is even more difficult to collaborate in the fight against ideological terrorism, especially when this terrorism is perpetrated by cyberattack. This has led to the state of uncertainty that exists today with regards to cyberattacks.

In the 2016 U.S. presidential elections, and immediately thereafter in France, a new age was marshalled in the field of cyber warfare. The heads of major U.S. intelligence agencies signed a joint declaration notifying the public they were confident that Russian operatives had meddled in the recent elections. According to their assessment, it was very likely these actors had operated under the direction of the Russian government. Their technique was simple: they hacked into the DNC computer network (as well as Hillary Clinton's personal computer), ultimately leaking thousands of documents (allegedly) retrieved from these databases; this included several documents pointing to Clinton's health issues and suspicion of corruption. We now know that most of these incriminating documents were fake. Nonetheless, in the heat of the elections, they landed on fertile ground and had an impact on voters. Russia has a long, illustrious history of planting false information. For example, the author of The Elders of Zion (written over a hundred years ago) was none other than the Okhrana, the pre-revolution Russian intelligence services. Later changing their name to the KGB – and now known as the FSB – disinformation has always played a major role in the Russian intelligence doctrine; cyber has simply granted it a more convenient tool for implementation.

The Yuval Ne'eman Workshop for Science, Technology and Security ventures to researches all aspects of cyber affairs, including its impact on both individual and societal security. This article examines the effect of cyber on the perceptual dimension, illustrating the new world in which we live. It leads us to the conclusion that Israel must be prepared not only for conventional cyber threats, but for unconventional cyber interference aimed at shaping public perception. This could potentially amplify existing discord within Israeli society, undermining the trust of Israeli citizens in their leadership, exposing other potential threats.

Professor Isaac Ben-Israel
Chairman of the Yuval Ne'eman Workshop for Science,
Technology and Security
Head of the Blavatnik Interdisciplinary Cyber Research Center

Introduction

Information has been manipulated for political purposes throughout the history of mankind. However, revolutionary technological advances since the creation of the internet – and the subsequent participation of both state and non-state actors in cyberwarfare – present new possibilities and allow for additional components that did not previously exist. Today both state and non-state actors use cyberspace in general – and social media in particular – as a tool to effect social and political change and to shape perception.[1]

A comparison of countries active in the field of Influence Operations[2] (IO) points to stark differences in their use of power via an array of methods and tools. These include the mobilization of intelligence resources, psychological warfare, public diplomacy, political and legal channels and cyberwarfare.[3] When countries do not assign clear boundaries or constraints on cyberspace activity or social media platforms, integrating the use of technology in the for real-world influence via the internet constitutes a powerful tool in Information Warfare (IW).[4] The use of this weapon will hereinafter be referred to as *cyber perception warfare*.

---

1 Continuous activity in the sphere of consciousness allows the reduction and/or disruption of the legitimacy of enemy activity, with the potential to foil or disrupt their offense initiatives.

2 Influence Operations, also known as Information Operations and warfare, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent. In the U.S., the more common definition to explain these phenomena is Information Operations (IO). See for example: The RAND Corporation definition for Information Operations: https://www.rand.org/topics/information-operations.html

3 A study by the University of Oxford found 28 countries operating in the sphere of influence on social media, investing hundreds of millions of dollars and with operating systems employing thousands. See: Samantha Bradshaw and Philip Howard, Troops, "Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," (working paper no. 2017.12, University of Oxford, 2017); http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

4 Information Warfare is the strategic and tactical use of information to gain an advantage.

The dimension of influencing perception discussed in this paper is the manner that subjective reality is perceived (pursuant to worldviews) by a variety of groups examining information regarding physical occurrences. Perceptions of reality are impacted by the reporting authorities and by the uncontrollable affiliations between different target audiences.[5] Consequently, our proposed definition of cyber perception warfare is "operations between two or more players, where one side disrupts the computerized and electromagnetic information environment that the opponent relies upon, and which is comprised of both human and technological sources. With this action, the initiator disrupts the opponent's ability to direct objective content to its target audience, to properly grasp reality and to establish effective defensive action capability." In this manner, the instigator grants itself an advantage in the overall campaign and neutralizes or disrupts the target's capacity to carry out a response.

The need to conceptualize this type of activity as distinct from more 'traditional' operations (such as psychological warfare) lies in the fact that key features of cyberspace activity include targeting opponents anonymously (without directly identifying the attacker as responsible for the attack) and at times autonomously (disseminating information through botnets, distributed-denial-of-service attacks, etc.). Operations conducted online facilitate a decentralization of information, offering a significant capacity for online distribution to either a focused or a broad target audience. The internet has shifted the traditional model of information dissemination via the media and government entities to the dispersal of information by individuals and small groups, who (at times) operate without a clear hierarchal model, and are mostly lacking rules, regulation or government enforcement.

The manipulation of information for political purposes is not a new phenomenon. Nonetheless, ongoing technological advances facilitate the accelerated sophistication of IO[6] and add elements that did not previously exist. Soviet IW, for example, was designed to

5 Shay Shabtai and Lior Reshef, "Influence Operations in the IDF", Maarachot 457 (October 2014), 34-39.

6 Information warfare combines electronic warfare, cyber warfare and psychological operations into a single fighting organization.

disrupt enemy activity through disinformation. Russian IW now makes use of the internet to disseminate false information to its enemies. At the same time, technological advancements add two elements to Russian IW. First, there is improved coordination between offensive, attack-oriented cyber warfare units (in comparison to what existed in the Soviet era) and IO units. Second is the Russian government's capacity to sabotage its enemies' information infrastructure, thereby disrupting operations of critical infrastructure in the target country.[7]

Many entities worldwide – military, government and private – plan and implement operational tools for IW. Herein we argue that directing effective influence operations in response to threats necessitates collaboration with influence operations and cyber warfare units, thus amplifying the force of state and military strategic Information Warfare (IW) operations on both tactical and strategic levels. Currently, state and security systems in Western countries do not possess full integrational cyber warfare capabilities for directing operations on a strategic level. In other words, the ability to influence wide or focused targeted audiences relating to a political conflict requires a systemic approach integrating cyber warfare and IW to perform systemic Information Warfare operations.

This article reviews the establishment of influence operations entities in several major countries, and examines two case studies demonstrating offensive IW campaigns that integrate influence operations and cyber warfare. The first case study examines the online offensive the U.S. mounted against the Islamic State (ISIS) with relatively limited use of cyber warfare as part of an IW offensive. The second case study explores Russia's offensives against the Ukraine – which included both a relatively extensive use of cyber and influence operations – as well as Russia's IW offensive campaigns against the U.S. These case studies illustrate the differences between two types of offensives: 1) where the security forces' approach entails a military/tactical operative dynamic on the ground and, 2) a political/diplomatic dynamic expressed where they are integral and intertwined components of the

7 Maria Snegovaya, *Russia Report I: Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington: Institute for the Study of War, 2015), 10, 14

offensive's approach. The evidence is clear that cyber warfare and influence operations are a combined effort.

An additional case in which the U.S. conducted an online influence offensive against (ISIS) illustrates an approach whereby cyber and influence operations are conducted as two distinct offensives against a singular opponent. Furthermore, there is a basic asymmetry in rules of engagement when conducting influence operations. Characteristically, liberal democracies are committed to adhering to laws of governmental responsibility. They are marked by domestic disagreements that prevent the formulation of a uniform message, and by bureaucratic and political complexities. Conversely, some non-Western actors believe the rules decided by democracies produce a world order that must be disrupted and altered. Those actors manipulate the media with no qualms, and their relative homogeneity enables both the creation of a singular message and the quick adaptation of operations in the disinformation campaign to change reality and mechanisms.[8]

8 Yossi Kuperwasser, "Battling for Consciousness", *Strategic Assessment* 12, no. 2 (2009): 37-44.

Toolbox for shaping perception in cyberspace

In cyberspace, we see how the internet and social media have had a deep impact on human behavior. Our online and offline lives have melded into one single entity. The 'traditional' hierarchal centralization model of information has been replaced by a decentralized model where information rapidly traverses physical and national borders with no laws restricting its flow. Cyberspace has substantially narrowed the geophysical dimensions of our environment, with both technological and perceptual changes caused by present-day computer networks. When browsing the internet, the nervous system's reaction emanating from the user's body and incoming information from the internet reach the user's consciousness simultaneously.[9] The internet allows users to concurrently exist both "everywhere and nowhere."[10] Our smartphones' internet connection has made every form of information and communication almost continuously accessible, regardless of our physical location. This principle is clearly evident when comparing internet penetration in Africa – and its impact on the local population – to other places in the world. Currently, African internet users amount to nine percent of total internet users worldwide, with a rate of penetration lower than all other continents (28 percent). Nonetheless, Africa's rate of increase in internet access since 2000 is higher than any other continent over the same period (approximately 7,700 percent in contrast with a global average of some 940 percent).[11] Accordingly, the forecast is that by 2020 Africa's rate of internet usage will reach 60 percent.[12] The use of cellular internet in Africa is considered a significant factor in their improved quality of life, more so than in

9 Avi Rosen, "Compressing Space and Time in Cyberspace Art" (PhD diss., Tel Aviv University, 2009).

10 Roy Ascott, "From Appearance to Apparition: Communications and Consciousness in the Cybersphere," *Leonardo Electronic Almanac* 1, no. 2 (1993): 3-9.

11 World Internet Usage and Population Statistics", Internet World Stats, accessed October 1, 2017; http://www.internetworldstats.com/stats.htm

12 Mani James, "Business Impact in Africa: Mega Trends Driving Mega Opportunities in Sub Sahara Africa", *Team Finland Future Watch*, September 11, 2014; https://www.slideshare.net/futurewatch/mega-trends-driving-mega-opportunities-in-sub-saharan-africa slide no. 19.

certain Western countries. This contribution is multifaceted and can be seen in the fields of education, employment, and health.[13]

The architecture of the internet enables the creation and distribution of information using a personalization model. In other words, information is made accessible to individual users or to groups through engagement tools according to segmentation by behavior, geography, fields of interest, needs, wants and desires. In such a reality, where barriers between the physical and cyber worlds are eliminated, the combination of emotions with online content can potentially influence consciousness to create a sense of fear, uncertainty and doubt among target audiences. In this context, we introduce a term borrowed from the business world: Fear, Uncertainty, and Doubt (FUD). This marketing technique is implemented by various companies to dissuade clients from purchasing products sold by their competitors. Companies utilizing the FUD technique publicize information on competing products that may trigger a sense of fear, uncertainty and doubt regarding the products.[14] In doing so, companies dissuade potential clients from purchasing them. FUD techniques are not limited to the business world, and they are also implemented to shape public opinion for political purposes. In political disputes between two or more nations, FUD is used to undercut the legitimacy and credibility of the other side's claims by sowing negative feelings towards them.

Any type of communication can serve as the basis for one entity's influence upon another. When one party delivers information to the other, the recipient chooses how it reacts. At times, the entity delivering a message hopes to frame the other party's actions, directing them to act according to their own aspirations, or to stop them from acting against them. Since incoming information affects actions, one of the actors may strive to impact the other's actions by distribution of information.

13 "Impact of the Mobile Internet in Africa vs. UK", On Device Research. Updated October 22, 2014; https://www.slideshare.net/OnDevice/impact-of-the-mobile-internet-in-african-lives/2-Mobile_internet_is_genuinely_improving.

14 For example: Fear, Uncertainty and Doubt", Changing Minds.org, accessed October 1, 2017; http://changingminds.org/disciplines/sales/articles/fud.htm.

Strategic communication is a process comprised of several stages. The first stage is preliminary research. Preliminary research allows the initiator of the measure to define the subject of the communication, to characterize the target audience of the messages and to determine goals that the action must achieve. Findings in this preliminary stage serve as the basis for formulation of the messages and for the manner in which they are to be dispersed.[15] This is followed by the feedback stage, which includes examination of the target audience's response to the messages, resulting in feedback on the quality of the strategic communication.[16] For our purposes, strategic communication includes influence operation and perception management.

Influence operation is a catchall phrase for any action intended to galvanize a target audience – an individual, a prominent group, or a broad audience – to accept approaches and to adopt decisions that mesh with the interests of the instigators of the operation. At the core of influence operation lie the actions that impact the cognitive and psychological perceptions of the target audience. These actions can be executed through various means: military, economic, political and others.[17]

Influence operation places a heightened emphasis on the planning aspect. For a successful influence operation, the planning process should include nine elements:

1. Goal creation – what are the goals of the initiator of the operation? Are these goals attainable? If they can't be fully reached, what potential results will be considered a success?
2. Target audience definition – who is the target audience for an effective operation?

15 Carl Botan, "Ethics in Strategic Communication Campaigns: The Case for a New Approach to Public Relations," *The Journal of Business Communication* 34, no.2 (1997): 188.

16 Carsten Bockstette, *Jihadist Terrorist Use of Strategic Communication Management Techniques* (Garmisch-Partenkirchen: The Marshall European Studies for Security Studies, Center Occasional Paper Series, no. 20, 2008), 9.

17 Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz and Cathryn Quantic Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (California: RAND Cooperation, 2009), 2-4.

3. Scheme outline – what strategies have the greatest impact on the target audience to ensure the desired results?
4. Hierarchal/leadership relationships – to what extent do the group leaders influence their members?
5. Information sources – what information sources are used by the target audience? What information sources do they consider credible?
6. Intellectual attitudes – how are the opponent's attitudes constructed, and how steadfast are they in their beliefs?
7. Alternative information – what messages do the target audience already receive on the subject matter?
8. Advocating change – what types of messages or information sources should be utilized to advance the desired change?
9. Quantity of transmitted information – how much information should be delivered to the opponent to affect change? What other steps should be taken to achieve the desired result?[18]

Perception Management describes a system for disseminating specific information to a distinct target audience to control its responses. Perception management is distinguished by a mode of action directed towards the international political arena in times of peace.[19] For instance, perception management operations can be implemented in areas recovering from war. They can offer legitimacy for new leadership in the area and can help restore infrastructure demolished during the war.[20]

Information lies at the core of the process of managing communications with the opposing side. As such, the key to implementation of this process is **Information Warfare** or **Information Operations**. These two terms express the collective steps taken by the initiator to influence the type and quantity of the information exposed to the adversary. When the initiator disrupts the information environment that the adversary

18 Ibid., XV-XVI.

19 Khyber Zaman*, Perception Management: IO Capability* (California: Naval Postgraduate school, 2007), 18.

20 Noelle J Briand, *How to Win Friend and Influence People- Planning Perception Management at the Division and Corps Level,* (Kansas: school of advanced military studies, 2004), 19.

relies upon, which is comprised of both human and technological sources, they disrupt their capacity to accurately grasp reality and to establish effective counteractions. In this manner, the initiator grants itself an advantage in the overall conflict, and can use IW to make substantial gains or even to decisively tip the scales to win the campaign. In order to avoid a parallel response by their opponent, IW also incorporates a component of defense – the instigator of the influence operations activates the defense capabilities of its databases.[21] Influence operations are usually identified with technological capabilities from the world of computers, but in effect, each of its operations that combines elements of trickery and deceit (such as delivering false declarations to the media) would be considered an act of IW.[22]

Accurate and quality information are important components in forging the path of action for any individual or organization. However, it is not the only component: the recipient decides how to act (or not to act) not only based on the presented facts, but also based on how these facts are interpreted; emotional reactions have a considerable impact on shaping final response. Consequently, strategic communication is also used to evoke certain emotional reactions, which lead to desired responses.

Psychological warfare is a broad term for directing the emotional aspect of strategic communication. When specific information involving psychological components is delivered to a defined target audience, this audience experiences a shift in its emotions and outlook.[23] As a result, there is a shift in the target audience's behavior, tarnishing its ability to reach the goals it has set for itself.[24] Messages used in psychological warfare may include promises, threats, asserting

21 Blaise Cronin and Holly Crawford, "Information Warfare: Its Application in Military and Civilian Contexts," *The Information Society* 15, no.4 (1999): 258.

22 Robin Brown, "Information Operations, Public Diplomacy & Spin: The United States & the Politics of Perception Management," *Journal of Information Warfare* 1, no.3 (2002): 41.

23 Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* (Washington: Congressional Research Service, 2007), 3.

24 Alfred Vasilescu, "Evolution of Pathological Communication's Military Domains, from Propaganda to Information Operations," Scientific Research and Education in the Air Force Volume 2011, 282.

conditions for the conclusion of fighting or of surrender, encouraging defection and so forth.[25]

All information has the potential to evoke an emotional response in those exposed to it, especially if this information comes from war zones. Nevertheless, not all dissemination of this type of information is considered psychological warfare. An operation is only seen as an act of psychological warfare if it is performed with premeditation, and with the intent to psychologically affect the other side.

Psychological warfare operations can be executed in both times of war and peace, and are referred to as **psychological operations**. There are several distinct types of such operations. For example, **tactical psychological operations** mounted against fighters on the opposing side differ from **consolidation psychological operations**, which are directed towards civilians on the opposing side.[26] They differ in timing, are directed towards a defined target audience and are meant to evoke certain emotions in their target audience.

One such type of operation with a psychological impact is **Computer Network Influence (CNI)**. In contrast with standard attacks launched against computer networks, CNI is designed to create the sense of a momentous strike without actually executing one. CNI attacks are meant to instill a sense of insecurity and a lack of control, compromising sovereignty with an inability to safeguard a normative way of life. Examples of such attacks include crippling government sites, sending damaging messages to civilians and shutting down media sites for limited stretches of time.[27]

Cyberattacks not only instill a sense of insecurity, they also attempt to disrupt the opponent's information environment by striking their cyber information infrastructure. These activities are mounted against computer systems designed to impact the target population's access, behavior and decision-making processes by controlling information distributed through these systems. This category of attacks includes

25 "OPNAV Instruction 3434.1: Psychological Operations," (Washington Naval Yard: Department of the Navy, Office of the Chief of Naval Operations, 1997),1–2; http://www.iwar.org.uk/psyops/resources/us/3434_1.pdf

26 Ibid.

27 Ofer Assaf & Gabi Siboni, *Guidelines for a National Cyber Strategy,* Memorandum No. 153 (Tel Aviv: Institute for National Security Studies, 2016), 18-19.

distributed denial-of-service attacks (crashing a particular site by flooding it with information, or DDoS attacks[28]), exposing the classified/personal details of an organization or of individuals by publishing confidential documents (doxing), hacking into information systems, as well as more sophisticated and strategic attacks on critical infrastructure core operational systems.[29]

28 "Definition- distributed denial-of-service attack (DDoS)," *TechTarget,* accessed October 1, 2017; http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

29 Pascal Brangetto and Matthijs A. Veenedaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations* (Tallinn: NATO Cooperative Cyber Defence Centre for Excellence, 8th International Conference on Cyber Conflict, 2016): 117, 121–122, 124.

Prominent operational units in the field of cyber perception warfare

There are a variety of military, governmental, and private entities currently operating in the planning and implementation of IW and influence operations. This chapter reviews some of these entities, distinguishing between military and political bodies, with an understanding that military units conduct perception exercises to promote operational activities in areas of confrontation. In Israel, for example, military awareness efforts at times of emergency or war coincide with a campaign and its subsequent efforts; it is intended to work in conjunction with the military operation to secure the campaign's strategic accomplishments.[30] In contrast, the Israel Ministry of Foreign Affairs uses the field of influence as a tool to support the execution of the state's foreign policy (and potentially contributing to its design).[31] The entities selected for this chapter must: a) demonstrate an extensive effort to adapt cyber warfare tools and force to both tactical and strategic challenges, and b) exert a notable effort in the field of IW and influence operations to promote operational activities in the areas of conflict in which they operate.

Military Units

Worldwide military units operating in the field of cyber perception warfare include:

NATO

NATO makes a clear distinction between the organization responsible for planning strategic communication and the forces responsible for its implementation in real time. The organization responsible for defining NATO's strategic communication principles is the NATO Strategic Communications Centre of Excellence. Located in Latvia, ten countries, which are also NATO Member States, participate in the

30 An example can be found here: "Israel Defense Force Strategy Document", *Belfer Center for Science and International Relations- Harvard Kennedy School* https://www.belfercenter.org/israel-defense-forces-strategy-document

31 This type is known as "strategic communications" or "public diplomacy."

organization.[32] Its objective is to improve the process of development, learning and implementation of strategic communications, within the scope of the operations of NATO Member States and institutions. To this end, it provides ongoing professional assistance to interested parties; some of its activity is theoretical and some tends to current affairs as it relates to Member States.[33]

It is important to note that NATO does not have a permanent division assigned with executing IW. The Combined Joint Psychological Operations Task Force (CJPOTF) is an ad hoc operational entity tasked with implementing psychological warfare. The scope of its authority and configuration vary in accordance with the task and the available manpower in the organization. Yet the composition of these task forces is invariable. Each is comprised of several departments that address various aspects of the implementation of psychological warfare: a research center, a product development center, tactical teams and others. In each task force, one country has manpower dominance and is referred to as the lead nation.[34]

The United States

The Joint Information Operations Warfare Center has been operating in the U.S. since its establishment in 1999. The center is subordinate to the Joint Chiefs of Staff and is manned by experts operating throughout the U.S. military, government and private sector.

The center operates on two levels: tactical, and strategic. On the tactical level, the center sends teams of IW experts to interface with globally positioned U.S. joint task forces, in accordance with the requirements of the Joint Chiefs of Staff. The teams advise combat forces on the ground on how to carry out IO strategies.[35] To this end, the center utilizes sociocultural analyses of populations situated in

32 Additionally, France and Canada have seconded staff.

33 "About Us," NATO Strategic Communications Centre of Excellence (StratCom), accessed October 1, 2017; http://www.stratcomcoe.org/about-us

34 "Allied Joint Doctrine for Psychological Operations," Ministry of Defense (UK), September 14,(3-1)–(3-6); https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

35 "Information Operations," *The Information Warfare Site*, accessed October 1, 2017; http://www.iwar.org.uk/iwar/resources/jtf-cno/jioc.htm

conflict zones.[36] On the strategic level, the center serves as an IW authority for all U.S. Department of Defense (DoD) agencies. The center is responsible for disseminating information through journals and position papers, and for establishing the best practices to achieve (IO) goals and promote the comprehensive administrational learning process of the execution of these plans.[37]

The U.S. Army Ground Forces is comprised of three divisions (two regular and one reserve) that plan and implement psychological warfare. Each division contains five regiments responsible for the planning, production and dissemination of psychological warfare in accordance with combat characteristics. In most cases, U.S. Armed Forces psychological warfare targets civilian populations in conflict zones, seeking to redirect their support from guerilla forces to U.S. forces.[38]

The U.S. Central Command of the U.S. Army (CENTCOM) is one of the main entities tasked with organizing influence operations. WebOps, CENTCOM's psychological warfare department, has a team of 120. Psychological warfare has three key elements:

1. Disrupting the opponent's propaganda,
2. Distributing incidences of the enemy's hypocrisy and criminality in its contact with at-risk populations
3. Mobilizing the enemy's adversaries to resist more effectively with the use of media.

CENTCOM also directs the Digital Engagement Team (DET), a special task force that includes 11 people fluent in languages such as Arabic, Urdu, Persian and Russian. Members of the unit manage Twitter, Facebook and Instagram accounts that speak to the populations of 20 countries in the Middle East and Central Asia.[39]

---

36 "Joint Information Operations Proponent," Chairman of the Joint Chiefs of Staff Instruction, February 14, 2014, (C-4), http://www.jcs.mil/Portals/36/Documents/Library/Instructions/3210_01.pdf?ver=2016-02-05-175024-017

37 "Information Operations," *The Information Warfare Site*.

38 Tal Tobi, "A War of Persuasion", *Maarachot* 352 (2013): 44-51.

39 Karen Parrish, "Centcom Counters ISIL Propaganda," *U.S Department of Defense*, July 6, 2016; https://www.defense.gov/News/Article/Article/827761/centcom-counters-isil-propaganda/

Russia

In recent years, the Russian military establishment has adopted an approach by which tactical military field operations, and political, diplomatic strategy across various international forums are integrated and interwoven components of the systemic concept.[40] As a derivative of this approach, cyber warfare and IO are combined efforts aimed at manipulating the victims' behavior. These include systemic attacks on digital networks, psychological warfare, fraud, misdirection and disinformation. These means bombard the opposing system with a flood of information that combines digital, electronic, and perceptual elements.[41]

When Russia launches a military strike, it does so under a heavy guise of secrecy regarding both the actual existence of the strike and its objectives. All Russian military operations are staged as peace-making activities or as interventions in humanitarian crises.[42] The obscuration of Russia's true goals contributes not only to weakening the opponent, but also to empowering Russia's image. If Russia fails to achieve a goal it holds in high regard, it can choose another goal without this being overtly considered a failure. As such, this obfuscation gives Russia an image of superiority.[43]

The various forms of IW and psychological warfare play a substantial role in Russia's military strategy. The heavy reliance on IW stems from Russia's acknowledgment of its military and economic inferiority, especially in comparison to the U.S. and China. Consequently, Russia considers IW to hold a double benefit: on the one hand, it can confuse the enemy regarding its true intentions, and on the other hand, in terms of cost-effectiveness, it substantially reduces the economic investment required in the case of a military confrontation in comparison with the use of kinetic means.[44]

---

40 Dima Adamsky, "The Russian Intervention in Syria: Strategic Significances and Systemic Lessons" *Eshtonot* 12 (2016), 22 http://maarachot.idf.il/PDF/FILES/5/113925.pdf

41 Ibid, 62.

42 Snegovaya, *Russia Report I*, 12.

43 Ibid., 15.

44 Snegovaya, *Russia Report I*, 11.

Russia's IW doctrine is mostly based on the corresponding Soviet doctrine. It is defined by the term *reflexive control*, which means the delivery of certain information to a certain entity to elicit them to carry out the instigator's desired actions.[45]

Accordingly, the messages Russia delivers to its opponents in the context of IW and disinformation campaigns is intended to reinforce a sense of desperation and cases of defection.[46] Russia also targets various forms of critical infrastructure (such as communications infrastructure), attempting to undermine the opponent's political, financial and social constructs.[47]

Israel

Israel has three military entities operating in the fields of strategic communications and IO with various populations. The Center for Consciousness Operations (abbreviated "Malat" in Hebrew) was established in 2005, and reports to the Operations Branch (in terms of command) and to the Military Intelligence Directorate (from a professional perspective).[48] For example, in Operation Cast Lead, the center mounted psychological warfare in the Gaza Strip against Hamas fighters and civilian populations. Most of these messages were delivered through newscasts broadcast across different types of media.[49]

The Psagot Battalion (an IDF Electronic Warfare unit) of the C4I Corps (Teleprocessing Corps) is primarily tasked with launching IW against the enemy. The battalion seeks to gain control of the enemy's electromagnetic devices, thereby disrupting (command and control) communication between terrorists and preventing them from

45 Ibid.,10.

46 Ibid.,11.

47 Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict", *Military Cyber Affairs,* 1, no.1 (2015): 2; http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1001&context=mca

48 Amos Harel, "IDF Reviving Psychological Warfare Unit", *Haaretz*, January 25, 2005 https://www.haaretz.com/idf-reviving-psychological-warfare-unit-1.148134

49 Ron Schleifer, "Psychological Warfare during Cast Lead", *Maarachot* 432 (2010): 18-23.

performing hostile acts against Israel. The battalion operates in the air, on sea and on land.[50]

The third military body demonstrates the implementation of perception management. The PR branch of the IDF Spokesperson's Unit manages operations directed towards various overseas audiences. The branch initiates and organizes visits to Israel by key figures (foreign military personnel, government officials, academics, etc.), coordinates PR missions for a variety of overseas conferences and helps pen studies overseas written about the IDF. These activities are performed under the premise that creating a pro-Israel stance overseas will propel foreign leaders to adopt a friendlier stance towards Israel.[51]

United Kingdom

The 77th Brigade was created in 2015 with the objective of executing psychological warfare through a variety of media channels worldwide (including social media). It operates in global locations where the British Armed Forces are involved in ongoing military operations.[52] The brigade is comprised of six columns; each column is charged with one aspect of psychological operations. Column 1, for example, is responsible for behavioral analysis of select target audiences.[53] One of the brigade's modes of operation is targeting outfits combatting Britain by spreading malicious rumors among their supporters and potential supporters.[54] The brigade employs regular soldiers and reservists from across the British Army, civilians with a background in cyber, as well as psychologists and media personnel. The brigade also works on reconstruction of civilian infrastructure and provision of humanitarian support in combat zones, with the intent of garnering

50 Merav Weiss, "The C4I Corps Activity during Protective Edge", *The C41 Coprs News,* September 1, 2014 https://archive.is/MKk18

51 Israel Tal Saranga, "Military Public Diplomacy", *Maarachot* 446 (2012): 11-19.

52 Military 'mask': British Army gets 'information warfare' focus, says top general," *RT*, February 18, 2015; https://www.rt.com/uk/233367-british-army-information-warfare

53 "77 brigade", global security, https://www.globalsecurity.org/military/world/europe/uk-army-77-bde.htm (accessed May 17 2018).

54 Corfield Gar "Army Social Media Psyops Bods Struggling to Attract Fresh Blood, " *The Register*, January 3, 2017; https://www.theregister.co.uk/2017/01/03/77_brigade_struggling_recruit_40_pc_below_establishment/

public support in these regions.[55] The brigade's command structure was originally designated to employ 1,500-2,000 workers, 40 percent reservists (the enlistment goal for 2016 was 448 recruits). In effect, there currently are only 276 people serving in the brigade, with 125 soldiers recruited in 2016.[56] To date, a handful of its workers have taken part in a scattering of operations. The brigade is planning on reaching full operating capability by late 2019.[57]

Another division of the British security outfit supporting military IO efforts is the Joint Threat Research Intelligence Group (JTRIG), a subsidiary of the intelligence agency and Signals Intelligence (SIGINT) of the Government Communications Headquarters (GCHQ). The group employs hundreds of people acting in various fields (cyber, psychology and intelligence), content and language professionals in three operative departments (counter-terrorism, internal defense and an international division), as well as several departments offering operational support in fields such as cyber, law and economics. The group supports military missions spanning the globe, with defense and intelligence operations both inside and outside Britain. The group conducts offensive cyber warfare as part of its counterterrorism campaign (DDoS, site defacement, etc.), and uses tactical tools in the conflict zones where Britain operates.[58]

Government Entities

There are numerous government entities (non-military) operating in the sphere of cyber perception warfare.

55 "New British Army Elite Unit to Hone Social Media and Psychological Warfare," *RT,* January 31, 2015; https://www.rt.com/uk/228227-british-army-psychological-warfare/

56 Gareth Corfield, "Army Social Media Psyops Bods Struggling to Attract Fresh Blood", The Register, January 3, 2017; https://www.theregister.co.uk/2017/01/03/77_brigade_struggling_recruit_40_pc_below_establishment/

57 George Allison, "What does the secretive 77th Brigade do?," *UKDJ*, June 21, 2016; https://ukdefencejournal.org.uk/secretive-77th-brigade/

58 Most of the information gathered about the unit was taken from a GCHQ organizational development document classified as top secret and leaked to the internet in 2011. See: http://www.statewatch.org/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf

Britain

The Research, Information and Communications Unit (RICU) is a British governmental department working in the field of strategic communications. Established in 2007, The center's objective is to coordinate British government efforts in its war against ideologies that promote terrorist activity. They advise security and law enforcement agencies, providing them with tools to comprehend/counter extremist messages and formulate feasible alternatives.

The center is comprised of three teams that compose and broadcast the desired messages: a monitoring and coordination team (to analyze means of communication, offer practical insight and understand public responses), a domestic and international campaign team (to implement strategic communication techniques both inside and outside the digital sphere),and an insight and research team (specifically focused on understanding the target audiences for these messages). The center employs multi-disciplinary professionals from an array of fields including social psychology, anthropology, marketing and counterterrorism.[59] It is important to note that a portion of the center's operations is outsourced to PR firms such as Breakthrough Media Network, a private media firm in London that builds websites, Facebook pages, flyers, video segments, radio broadcasts and Twitter feeds, all in accordance with RICU guidelines.[60]

The EU

The RICU was the model for establishment of the Syria Strategic Communications Advisory Team,[61] bringing together 25 EU Member States. Following terror attacks launched in France by Islamist radicals

59 "Case Study Report: Research, Information and Communication Unit," *The Institute for Strategic Dialogue*; https://www.counterextremism.org/resources/details/id/413/research-information-and-communications-unit-ricu

60 Ian Cobain Alice Ross, Rob Evans and Mona Mahmood, "Revealed: UK's covert propaganda bid to stop Muslims joining Isis," *The Guardian,* May 2, 2016; http://www.theguardian.com/uk-news/2016/may/02/uk-government-covert-propaganda-stop-muslims-joining-isis

61 Patryk Pawlak, *EU strategic communication with the Arab world (*Brussels: European Parliamentary Research Service, May 2016): 8; http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581997/EPRS_BRI(2016)581997_EN.pdf

in early 2015,[62] the team was formed to establish techniques for Member States to counter social media messages encouraging Muslim European civilians to join terrorist organizations fighting in Syria; several Member States have reported positive results in countering these messages.[63] In October 2016, the Belgian-led multinational European Strategic Communications Network (ESCP) was established as a follow-up project, and was expected to operate for a period of one year. Like its predecessor, the ESCP is responsible for gaining insight and strategic communication practices to counter radicalization potentially leading to terrorist activity.[64]

In November 2015, the European External Action Service (EEAS) established the Disinformation Review, a special task force charged with countering Russian disinformation campaigns.[65] The task force documents disinformation efforts directed by the Russian government towards European civilians, informing them and their governments on the nature and scope of Russian disinformation. The documentation of instances of disinformation for the special task force is collected by a network of some 400 journalists, civil society organizations, and academic institutions located in 30 European countries. Information gathered by the Disinformation Review offers the EEAS a longitudinal examination of trends that characterize Russian IO.[66]

---

62 "Establishment of a European Anti-Propaganda Agency to Fight Radicalization", *European Parliament*, Parliamentary Questions, August 3, 2015; http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=P-2015-003103&language=EN

63 "The Syria Strategic Communication Advisory Team (SSCAT) and the Role of Counter-Narratives in Preventing Radicalization," *European Parliament*, Parliamentary Questions, May 17, 2016; http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-000505&language=EN

64 *Implementation of the Counter-Terrorism Agenda set by the European Council* (Brussels: Council of the European Union, 2016): 24; http://data.consilium.europa.eu/doc/document/ST-14260-2016-ADD-1-EXT-1/en/pdf

65 European Union in Ukraine. "Disinformation Review" – new EU information product." Facebook, November 4, 2015; https://www.facebook.com/EUDelegationUkraine/posts/1019727421405219

66 "Disinformation Review," *European Union External Action (EEAS*), September 2, 2016; https://eeas.europa.eu/headquarters/headquarters-homepage_en/9443/Disinformation%20Review

Moreover, in April 2017, the ECE-CHT (European Center of Excellence for Countering Hybrid Threats) was established in Finland, one year after its proposal by the EU. The center is tasked with promoting a comprehensive, multidisciplinary global policy to counter hybrid threats. The center is to serve as the base for ongoing collaboration between EU Member States and NATO, for establishing a doctrine and for conducting training and certification programs aimed at enhancing participants' individual capacity and interoperability between and among other participants.[67] The center's budget for 2017 was €1.5 million, half financed by Finland and half by other Member States.[68]

Israel

The Israeli Ministry of Foreign Affairs and its various departments stand out among Israeli government ministries for their work in the sphere of strategic communications. The ministry's Media and Public Affairs Division maps organizations involved in the boycott against Israel, trains Israeli ambassadors on suggested messaging and distributes pro-Israel messages across various social media platforms. Moreover, the department creates a system for collaboration between the Israeli government and civil organizations active in presenting Israel's foreign policy.[69]

In addition, in early 2016 a special department was created to counter the boycott and delegitimization of Israel (a subdivision of the Ministry of Strategic Affairs); this department serves as the main Israeli governmental authority for understanding the status of the Boycott, Divestment, Sanctions (BDS) movement, establishing a response to the movement and representing the government in working with other

67 "EU Welcomes Establishment of the Finnish Centre of Excellence for Countering Hybrid Threats," *European Union External Action*, updated April 11, 2017; https://eeas.europa.eu/headquarters/headquarters-homepage_en/24572/EU%20welcomes%20establishment%20of%20the%20Finnish%20Centre%20of%20Excellence%20for%20countering%20hybrid%20threats

68 Aleksi Teivainen, "EU's Hybrid Threat Centre to be set up in Helsinki," *Helsinki Times,* April 12, 2017; http://www.helsinkitimes.fi/finland/finland-news/domestic/14686-eu-s-hybrid-threat-centre-to-be-set-up-in-helsinki.html

69 The Diplomatic-Media Struggle in the Boycott Movement and Anti-Semitism Abroad" *State Comptroller of Israel's Report*, (May 2016): 866,877 ,871 ,868 , 881 http://go.ynet.co.il/pic/news/mevak-861-883.pdf

civil organizations fighting the boycott. The department's activities against the boycott can be divided into three categories: gathering overt and covert information about entities involved in the movement; taking legal action against them; and, guiding civil organizations on the messages worth focusing upon in countering the boycott.[70]

Russia

We can learn much about Russia's approach to shaping public opinion from Dmitry Kiselyov, the Russian government's chief propagandist: "The age of neutral journalism has passed. In our present reality, neutrality is impossible because what you select from the huge sea of information is already subjective." Russia runs a national news outlet called *Rossiya Segodnya*, which produces a continuous stream of subjective information. The Kremlin outsources an army of trolls to argue in the comments sections of Western news sites and social media such as Facebook and Twitter. This includes a network of thousands of bots operating on social media and other forms of spam with the purpose of disrupting competing content. The influence campaign has always played a role in disputes between countries and societies, but its magnitude has skyrocketed in recent years. Democratic nations have demonstrably begun allocating notable resources in fashioning and improving their capabilities in perception warfare.

70 Tzvika Klein, "Israel's Secret Messages: "This is how you will respond to BDS activists" *NRG*, February 22, 2016 http://www.nrg.co.il/online/1/ART2/756/389.html

Case study analysis

This chapter analyzes case studies on influence operations, psychological warfare and cyber warfare units, cases that occurred within the context of disparate military campaigns. Beyond the differences between the two armies examined in the analysis, there are also differences in methods of force implemented on the field: covert and overt U.S. campaigns mounted against ISIS in Syria and Iraq, as opposed to a covert Russian campaign in Ukraine using forces that were not officially fighting (supposedly only pro-Russian Ukrainian forces fought the Ukrainian army). Another key distinction is that while the U.S. was trying to address an outlet influencing cyberspace (ISIS and its efforts to recruit, impact and spread propaganda), Russia itself was making its mark in cyberspace. What these two case studies have in common is the use of an integrated campaign incorporating IW, IO and cyber warfare; however, these were evident on different levels of power and force. An analysis of these case studies will illustrate these distinctions, pointing to the basic asymmetry between Russia and the West's use of cyber tools in IW.

U.S. cyber perception warfare against ISIS

The U.S. government's imperative to fight organizations such as ISIS and al-Qaeda in the spheres of perception and intelligence stems from these organizations' increasing capacity to act via social media networks. They have successfully utilized social media to target and enlist potential recruits by leveraging a massive number of websites and social media profiles appealing to young people across the globe; some of these sites have even used service providers situated in the U.S. As they expand their activity to the dark web, their capabilities are expected to become even more sophisticated in the future.[71] The fight against this trend relies upon a network of organizations – military, government and private – addressing various aspects of strategic communications in general and IW in particular.

71 Dan Verton, "Pentagon Gets Authority to Fight Online ISIS Propaganda," *Meritalk,* November 30, 2015; https://www.meritalk.com/articles/pentagon-gets-authority-to-fight-online-isis-propaganda/

The incorporation of IO in the campaign

One of the main entities organizing IO against ISIS is CENTCOM, operating out of the MacDill Air Force base in Tampa, FL. CENTCOM's Digital Engagement Team (DET) of 11 professionals fluent in languages such as Arabic, Urdu, Persian and Russian. Members of the unit manage Twitter, Facebook and Instagram accounts that speak to the populations of 20 countries in the Middle East and Central Asia.[72] According to CENTCOM, their content is viewed by some 100,000 people a week.[73]

WebOps, CENTCOM's psychological warfare department, has a staff of 120. According to the DoD, WebOps raisons d'être are: 1) to disrupt adversary propaganda; 2) to expose adversaries' hypocrisies and crimes through engagements with at-risk target audiences; and, 3) to mobilize the adversaries' opponents to more effectively combat the adversary online. For example, WebOps has targeted ISIS defectors who provide testimony that could subvert messages that ISIS wants to disseminate. According to several such accounts, these defectors state that they had joined ISIS to fight the Syrian regime and infidels, but in practice they found themselves fighting Muslims (and opposition groups) like themselves.[74]

Alongside messaging aimed at undermining the opponent's credibility, the unit also works to forge an affinity between their target audiences and Western values. Accordingly, the unit's messages evolved from oppositional to those aimed at creating dialogue and sparking intrigue. The premise is that sharing facts about the West sparks the target audience's curiosity, ultimately instilling Western attitudes.[75] The mobilization of ISIS detractors is performed in cyberspace, with teams search for several key phrases common to ISIS opposition members

72 Karen Parrish, "Centcom Counters ISIL Propaganda."

73 Peter Cary, *The Pentagon and Independent Media–an Update*, (Washington: CIMA- Center for International Media Assistance, 2015), 10. https://www.cima.ned.org/wp-content/uploads/2015/11/CIMA-The-Pentagon-and-Independent-Media-Update.pdf

74 Parrish, "Centcom Counters ISIL Propaganda."

75 Cary, *The Pentagon and Independent Media–an Update*, 10.

and supporters. The WebOps group includes an assessment unit whose role is to evaluate the effectiveness of the unit's operations.[76]

In addition to these efforts, the U.S. Army uses ISIS social media posts to its own advantage. For example, a post shared by an ISIS fighter included photos of ISIS command headquarters. The Air Force was able to identify its location and demolished it within 24 hours.[77] Another facet of U.S. military operations is destroying ISIS's communications infrastructure on the ground.[78]

On the state level, there is robust activity by government departments and agencies including the State Department, the National Security Agency (NSA) and the Department of Homeland Security (DHS). The State Department's Center for Strategic Counterterrorism Communications (CSCC) operated from 2011 to 2016, after which it was replaced by the Global Engagement Center (GEC). These two organizations have operated online by delivering messages (to U.S. residents and to foreign countries) aimed at preempting the recruitment of civilians to ISIS. To this end, these organizations have distributed two types of information. The first is identical to information used by CENTCOM, including a series of messages (mostly acquired by defectors) attempting to undermine the esteem and credibility of ISIS.[79] The second type addresses those contemplating joining ISIS on a more personal level. This type of messaging requires potential recruits to consider the ramifications of such an undertaking on their family, community and life.[80]

---

76 Parrish, "Centcom Counters ISIL Propaganda."

77 Michael Hoffman, "U.S. Air Force Targets and Destroys ISIS HQ Building Using Social Media," *Defensetech,* June 3, 2015; http://www.defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/

78 Lynne O'donnell, "U.S Airstrikes Have Destroyed an Islamic State- Operated Radio Station in a Remote Part OF Eastern Afghanistan," *U.S.News*, February 2, 2016; http://www.usnews.com/news/world/articles/2016-02-02/airstrikes-in-eastern-afghanistan-destroy-is-radio-station

79 Kristina Wong, "How the U.S. is working to defeat ISIS online," *The Hill,* June 25, 2016; http://thehill.com/policy/defense/284826-how-the-us-is-seeking-to-defeat-isis-online

80 Patrick Tucker, "Meet the Navy SEAL Leading the Fight Against ISIS Messaging*," Defense One*, June 9, 2016; http://www.defenseone.com/technology/2016/06/navy-seal-isis-messaging/128938

The most notable difference between the operations of these two organizations is the source of their messages. When the CSCC was operational, messages were shared via the U.S. government's Twitter, Facebook, and YouTube accounts.[81] In 2015, the State Department decided to use a no logo strategy. Under this approach, messages were not posted under its own profile, rather they were shared them through a network of entities and individuals not identified with the U.S. government – including foreign governments and moderate Muslim communities – critical of ISIS's potential supporters.[82] This decision was taken because these organizations and individuals are better able to reach those target audiences that the U.S. government is trying to impact. As such the GEC, in contrast with the CSCC, serves as the focal point of a global network that coordinates technical and conceptual messaging.[83]

From a strategic standpoint, the Office for Community Partnerships (OCP), formed in September 2015, heads operations at the DHS. The mission of the OCP is to prevent the radicalization of U.S. citizens by fostering government relationships with a myriad of communities dispersed throughout the U.S.[84] The OCP was founded under the belief that the way to lessen the appeal to radical ideas is through reinforcement of alternative messaging promoting tolerance and peace.[85] The OCP provides substantive support to communities interested in running programs to prevent radicalization from within. In May 2016, the OCP announced its appropriation of $10 million in grants for

81 Asawim Suebsaege, "The State Department Is Actively Trolling Terrorists on Twitter," *MotherJones*, March 5, 2014; https://www.motherjones.com/politics/2014/03/state-department-cscc-troll-terrorists-twitter-think-again-turn-away/

82 Cary, *The Pentagon and Independent Media–an Update*, 9.

83 Patrick Tucker, "Meet the Navy SEAL Leading the Fight Against ISIS Messaging."

84 "Statement by Secretary Jeh C. Johnson on DHS's New Office for Community Partnerships," *U.S Department of Homeland Security*, September 28, 2015; https://www.dhs.gov/news/2015/09/28/statement-secretary-jeh-c-johnson-dhs%E2%80%99s-new-office-community-partnerships

85 Michael A. Brown and Christopher Paul, "Inciting Peace," *RAND Cooperation,* March 30, 2016; http://www.rand.org/blog/2016/03/inciting-peace.html

communities to develop programs for promoting tolerant messaging to counter violence.[86]

Another team charged with DHS operations is the Countering Violent Extremism Task Force (CVE) founded in early 2016. The task force has a broader, more comprehensive role: it develops a variety of intervention programs to counter extremism; it synchronizes collaboration between ten federal outfits (the Justice Department, the FBI and others) for the execution of the programs; it directs operations with participating extra-governmental entities; and, it manages research and feedback mechanisms on efforts being conducted in the field.[87]

In the cyberspace war against ISIS, the DHS is involved in several initiatives. One such initiative is a competition encouraging talented university teams to create new media campaigns underlining messages of positivity and tolerance. Thousands of students across the globe take part in this competition, which is heavily funded by Facebook. In parallel, the task force seeks to strengthen ties with a variety of tech companies with the goal of helping the task force establish a working cyberspace strategy that can be used by other government agencies. To this end, U.S. government officials met with tech executives in New York (in November 2015) and in San Francisco (in January 2016).[88]

Activating cyber warfare in the campaign

In April 2016, the U.S. Cyber Command mounted an attack against ISIS's computer network. The attack objective was to strike ISIS's command and control capabilities, disrupting its ability to carry out logistical operations within the organization such as recruiting new

86 George Selim, "OCP and CVE Task Force Welcome President Obama's Top Homeland Security Advisor," *U.S Department of Homeland Security*, May 6, 2016; https://www.dhs.gov/blog/2016/05/06/ocp-and-cve-task-force-welcome-president-obamas-top-homeland-security-advisor

87 "Written Testimony of DHS Office for Community Partnerships Director George Selim for a Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations hearing titled 'ISIS Online: Countering Terrorist Radicalization & Recruitment On the Internet & Social Media'," *U.S Department of Homeland Security*, July 6, 2016; https://www.dhs.gov/news/2016/07/06/written-testimony-ocp-senate-homeland-security-and-governmental-affairs-permanent

88 Ibid.

operatives, paying its fighters and issuing orders.[89] The most well-known, sophisticated attack carried out by U.S. forces was the disruption of pro-ISIS propaganda by the NSA and the U.S. Cyber Command in Operation Glowing Symphony. In this operation, executed during 2016, U.S. cyber units obtained the passwords and access codes of ISIS operatives, later using them to block access to internet assets and to delete content used for propaganda and recruitment. The operation was deemed a success, but this success was fleeting as ISIS moved to more secure servers.

The Cyber Command has also launched integration operations with forces on the ground. These have included locking detected operatives out of their accounts, forcing them to use less secure tools and exposing their position to facilitate drone attacks.[90] In late 2016, the Cyber Command hacked into the accounts of ISIS propaganda specialists, changed their passwords and deleted propaganda content including video recorded in the battlefield.[91] Other than technical damage, these operations inflict psychological damage as well: when ISIS leaders and operatives realize their activity is not secure, their sense of confidence is undermined. Operations have also included placing various 'implants' in ISIS's networks to study the habits of its operatives.[92] Activity is seen both in the disruption of operative command and control, and in actions carried out against ISIS's media network designed to recruit terrorists.

These operations spark two points of contention within the U.S. government. The first relates to the effectiveness of these cyberattacks,

89 David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times*, April 24, 2016; http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=2

90 David E. Sanger and Eric Schmidt, "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS," The New York Times, June 12, 2017; https://mobile-nytimes-com.cdn.ampproject.org/c/s/mobile.nytimes.com/2017/06/12/world/middleeast/isis-cyber.amp.html

91 Ellen Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies," *The Washington Post,* May 9, 2017; https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.30d3d00d99fb

92 Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat."

posing the question of whether U.S. cyber operations have truly succeeded in disrupting the enemy's web activity. While the Cyber Command and the DoD have deemed these operations a success, former intelligence officials (speaking on condition of anonymity) question their success. The reason for this debate lies in the definition of successful cyber operations: while the DoD and the Cyber Command define success as a temporary disruption of enemy activity, intelligence experts look for the infliction of long-term damage, which they claim is hard to achieve in these operations. For example, these intelligence experts state that ISIS activity can be partly restored or transferred to other servers, rendering the impact of these operations null and void.[93]

Another point of contention relates to the impact of this type of warfare on the relationship between the U.S. and its allies. Some ISIS servers are located in countries that are allies of the U.S. As such, actions against these servers are, in effect, offensive operations conducted in ally territory. For this reason, the U.S. government continuously debates whether it should alert its allies before mounting these operations. The FBI, the CIA and the State Department claim that such operations, launched without advance coordination, could impair counterterrorism and intelligence collaboration between the countries. On the other hand, the DoD claims that alerting states in advance of cyber operations could lead to the leaking of sensitive details, potentially hindering success.[94]

Russian influence operations against Ukraine

The Russian military establishment has recently adopted an approach whereby tactical, operative, military dynamics on the ground – along with political, diplomatic dynamics in various international forums – are integral and interwoven components of a comprehensive concept.[95] Consequently, cyber warfare and IO are combined efforts aimed at manipulating victims' behavior. These include attacking digital

93 Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies."

94 Ibid.

95 Adamsky, "The Russian Intervention in Syria: Strategic Significances and Systemic Lessons", 22

networks, psychological warfare, fraud, deception and systemic disinformation. These means blast the opposing system with information that combines digital, electronic and perceptual elements.[96]

In February 2014, Russia invaded the Crimean Peninsula and annexed it within just a few days. Prior to the infiltration, the peninsula was Ukrainian territory, but it served the Russian Navy in the Black Sea. Long after the invasion, Russia continued to deny its military involvement in the region. The Russian army conducted a broad military exercise on its border with Ukraine, far from the Crimean Peninsula, before the offensive. That exercise served as a distraction, impairing the ability of Ukrainian and Western authorities to accurately predict Russia's action.[97] In April 2014, pro-Russian separatists launched a violent uprising in the Ukrainian districts of Donetsk and Luhansk, declaring the establishment of independent republics with the intent of uniting with Russia in the future. The separatists' announcement led to a large-scale military response by the leadership in Kiev. In January 2015, long after the military infiltration of the Crimean Peninsula, Foreign Minister of Russia Sergey Lavrov stated, "I say every time: if you allege this so confidently, present the facts. But nobody can present the facts or doesn't want to. So before demanding from us that we stop doing something, please present proof that we have done it." Putin also vehemently denied Russian military involvement, claiming that the forces operating in the peninsula were local militias (even though some fighters were dressed in Russian military uniform). Only in April 2015 did Putin admit that Russian special military forces were involved in military activity in the peninsula.[98]

In actual war, Russian intelligence operations are not slated to win in the early stages of combat, rather they work towards victory by dragging out the conflict. By doing so, Russia increases its ability to

96 Ibid, 62.

97 Ulrike Frank, *War by non-military Means- Understanding Russian Information Warfare*, (FOI: Swedish Defense Research Agency, 2015), 46; http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf

98 Snegovaya, *Russia Report I*, 17.

impact the war and can choose when to end its involvement at any given point in time that suits it.[99]

By acting in this manner, Russia made great strides in both military and diplomatic/perception management arenas: denying the military invasion shortened the reaction time of the Ukrainian side and hindered its ability to mount a suitable military response. Russia's denial was meant to complicate efforts to monitor its activity and make it difficult for opponents to plan their next steps.

In 2015, the Russian government increased its investment in the state TV station RT by 50 percent, to $300 million. That year, its news outlet *Rossiya Segodnya* (Russia Today) was allocated a budget of $89 million. While some of this growth relates to the drop in the ruble's value, it also reflects the increasing importance that Russia attaches to its media messaging. In 2015, the cost of these broadcasts amounted to 34 percent of Russia's entire media spending, in contrast with the 25 percent it had allocated the previous year.[100]

State TV stations are the primary source of information for almost all residents of Russia,[101] so these stations are viewed as representative of the mainstream. As such, reports on the war in Ukraine would have been as broad and abstract as possible, sparing its viewers the unnecessary details. These stations justified the invasion of the Crimean Peninsula by stating that it would protect the Russian minority living there at the time.[102]

Nonetheless, Russian TV stations also express the narrative of atrocities and violence waged by Ukrainians in the region.[103] They have referred to Ukrainian fighters as Bandarites (partisans who colluded with the Nazis) or fascists.[104] An important objective in depicting Ukrainians in such a fashion is to complicate the West's

99 Ibid.,12.

100 Stephen Ennis, "Russia in 'Information War' with West to Win Hearts and Minds," *BBC* September 16, 2015; http://www.bbc.com/news/world-europe-34248178

101 Snegovaya, *Russia Report I*, 15.

102 Ilya Yashin and Olga Shorina, eds., Putin. War – An Independent Expert Report (Moscow: Free Russia Foundation, 2015), 10; http://4freerussia.org/putin.war/Putin.War-Eng.pdf

103 Unwala and Ghori, "Brandishing the Cybered Bear," 8.

104 Snegovaya, *Russia Report I*, 13–14.

efforts to intervene in Ukraine's favor.[105] By portraying Ukrainians as Nazis, Russia alienates Ukraine from the West. This portrayal is especially designed to deter countries with a Nazi past, e.g. Germany, from continuing their support of Ukraine.[106]

Russian media has presented the Ukrainian government to the Russian people in another "derogatory" way: after a new government was established in Ukraine in February 2014, Russian media released a detailed account of "original emails" illustrating the new government's special affinity to the West. These emails were supposedly leaked by "anonymous Ukrainian sources."[107]

Over time, these messages were unsuccessful in swaying global public opinion in favor of a justification of the Russian action.[108] There are less viewers exposed to messages broadcast on RT than there are viewers exposed to messages broadcast on other international stations. An example of this is Al Jazeera English: while in 2012 viewership of the two stations was more or less equal, in 2015, RT had less than half the viewership of Al Jazeera English.[109] Nonetheless, TV broadcasts have a substantial impact on audiences in post-Soviet states: many Russians who volunteered to take part in the war against Ukraine did so due to the influence of Russian TV broadcasts.[110] Civilians in many post-Soviet states view Russian media as more credible than Western media. Many people exposed to both Western and Russian media coverage on events unfolding in Ukraine prefer Russian coverage.[111]

105 Galeotti, "Hybrid War' and "Little Green Man'," 153.
106 Unwala and Ghori, "Brandishing the Cybered Bear," 7.
107 Frank, *War by non-military Means,* 45.
108 James Andrew Lewis, "'Compelling Opponents to our Will': The Role of Cyber Warfare in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 2015), 45. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf
109 Stephen Ennis, "Russia in 'Information War'."
110 Snegovaya*, Russia Report I*, 15.
111 Neli Esipova and Julie Ray, "Information Wars: Ukraine and the West vs. Russia and the Rest", *Harvard International Review,* May 6, 2016; http://hir.harvard.edu/information-wars-ukraine-west-vs-russia-rest/

Mounting influence operations

Russia makes use of three primary cyber tools: bots (software that imitates human activity), trolls and hackers. Bots are programs that disseminate short messages, which are at times identical to those spread by trolls. Russian trolls try to meddle in a variety of debates, where they post comments, including spam, to spread disinformation and express pro-Russian sentiments.[112] They also comment regularly in response to articles on Western news sites that are critical of Russia.[113] Russian trolls can be quite unconvincing, but their activity grants them a notable online presence. Their goal is not to try to persuade others of a certain worldview, but rather to control the flow of information to create a sense of fear and uncertainty for the other side – Europeans.[114] Another one of its goals is to undermine the credibility of opposition websites as information sources.[115]

Often, the activity of trolls on social media is designed to promote news stories that were first published on Russian news stations. The widespread publication of pro-Russian stories on social media causes the servers of these networks to identify these stories as 'trending' using algorithms, thereby increasing the likelihood that these stories will also be covered by traditional Western media.[116]

The Internet Research Agency (IRA) in St. Petersburg employed trolls under the direction and funding of the Russian government until late 2016.[117] By the end of the year, in an attempt to be considered a legitimate news agency, it was renamed the Federal News Agency

112 Snegovaya, *Russia Report I*, 14.

113 John B. Emerson, "Exposing Russian Disinformation*", Atlantic Council*, June 29, 2015; http://www.atlanticcouncil.org/blogs/ukrainealert/exposing-russian-disinformation

114 Snegovaya, *Russia Report I*, 14.

115 Emerson, "Exposing Russian Disinformation."

116 Craig Timberg, "Russian Propaganda Effort Helped Spread 'Fake News' During Election, Experts Say", *The Washington Post,* November 24, 2016; https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html?utm_term=.ea80d3d009a3

117 Dmitry Volchek and Daisy Sindelar, "One Professional Russian Troll Tells All" *Radio Free Europe, Radio Liberty*, March 25, 2015; http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html

(FAN). The agency oversees 16 news sites[118] that routinely spread pro-Russian propaganda.[119]

In addition to broadcasting on TV, the largest global media stations also make us of social media. This creates an interesting scenario: on one hand, the number of Twitter and Facebook users of the most prominent Western stations such as CNN and BBC is substantially higher than the number of RT users. On YouTube, however, this is not the case: in 2015, RT's official YouTube channel had 1.5 million subscribers and 1.5 billion views.[120] Sites that are unable to sway public opinion are often shut down. For example, the online Sputnik news channels addressing Scandinavia were taken down after less than a year due to their low appeal in these countries.[121]

Launching cyber warfare campaigns

A relatively high number of cyberattacks was recorded during Russia's invasion of Crimea, when Ukrainian phone networks and news sites were disabled for three days. In the early days of the Ukraine invasion, several Ukrainian websites were shut down after having been hacked, including the Ukrainian Independent Information Agency (UNIAN), the National Security and Defense Council of Ukraine and the Crimean Supreme Court.[122] These were Distributed Denial of Service attacks (DDoS).

---

118 Sam Webb, "Vladimir Putin's Notorious 'Troll Factory' Attacked with Molotov Cocktails Amid Reports it Employs an Army of Teens to Flood Social Media with Praise for Russia", *The Sun,* October 28, 2016; https://www.thesun.co.uk/news/2068935/vladimir-putins-notorious-troll-factory-attacked-with-molotov-cocktails-amid-reports-it-employs-an-army-of-teens-to-flood-social-media-with-praise-for-russia/

119 Alexey Kovalev, "Russia's Infamous 'Troll Factory' Is Now Posing as a Media Empire", *The Moscow Times,* March 24, 2017; https://themoscowtimes.com/articles/russias-infamous-troll-factory-is-now-posing-as-a-media-empire-57534?utm_source=push

120 Stephen Ennis, "Russia in 'Information War'."

121 Neil Macfarqhar, "A Powerful Russian Weapon: The Spread of False Stories", *Atlantic Council,* August 29, 2016; http://www.atlanticcouncil.org/blogs/natosource/a-powerful-russian-weapon-the-spread-of-false-stories

122 Andrew Foxall, *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*, Policy Paper No. 9 (London: Russia Studies Centre at the Henry Jackson Society, 2016), 4, https://relayto.com/the-henry-jackson-society/YDD2kgI1

This situation caused a great deal of harm to the Ukrainian side. Firstly, as the Ukrainian government was unable to contact authorities in the peninsula, it could not accurately assess the scope of the Russian attack. Secondly, the Ukrainian government struggled to create a mechanism for making decisions regarding the unfolding crisis. Thirdly, Ukrainians were unable to contact Western authorities to seek help or to formulate a response to Russia.[123]

Even after the annexation, Russian cyberattacks continued, targeting the West as well. For example, in March 2014 access to several NATO websites was blocked in an attack launched by pro-Russian Ukrainians. That same month, the Federal Service for Supervision of Communication, Information Technology and Mass Media (*Roskomnadzor*) blocked access to websites that were pro-Ukrainian or run by Russian opposition figures such as Alexei Navalny and Garry Kasparov.[124]

Russia succeeds in undermining its opponents' decision-making mechanisms by launching attacks through radio broadcasts, radar and GPS systems. The Russian army has large units with the capacity to mount these types of attacks. The Ukrainian army is in an inferior position to that of the Russian army in this respect, finding it difficult to defend itself against Russian attacks. When the Russian army attacks the Ukrainian army, the Ukrainian army scrambles to formulate an appropriate response. The major problem facing the Ukrainian army is that its soldiers and commanders are simply untrained to counter attacks on their communications network. Given the common Soviet history it shares with Russia, the Ukrainian army should better understand how Russia fights. These Russian tactics are not only attractive because of their effectiveness, but also because such attacks are difficult to trace, thereby limiting the ability to blame Russia for the aggression.[125]

Russia also possesses the capability to attack its enemies through strategic cyber offensives mounted against critical infrastructure. In

123 Unwala and Ghori, "Brandishing the Cybered Bear," 6–7.

124 Ulrike Frank, *War by non-military Means,* 46.

125 Joe Gould, "Electronic Warfare: What U.S. Army can Learn from Ukraine," *Defense News,* August 2, 2015; http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/

2015-2016, there were two wide scale attacks of this nature. In the first attack, in December 2015 hackers managed to cut the power supply to roughly 230,000 Ukrainian civilians by targeting three local energy distribution centers. The attack left Ukrainians without power for up to six hours.[126] The second attack was mounted in Kiev in December 2016, striking the power supply of Ukraine's capital. This attack left people without power for a shorter time span of a few minutes, as hackers successfully took out 200 megawatts of capacity, representing 20 percent of Kiev's nighttime energy consumption.[127]

The pattern of these two attacks is identical: several months beforehand, hackers used a spear phishing campaign targeting a range of government institutions (including the Ukrainian power grid). Emails with malware were delivered, and downloaded by the email recipients. Once the spyware was downloaded, hackers gained an up-close understanding of the power facilities, enabling a more effective attack. The spear phishing campaign was conducted with such sophistication that according to estimates, nearly all recipients of these emails opened them and downloaded the attached malware.[128] The 2015 attack used the sophisticated "BlackEnergy" malware, allowing hackers to launch cyberattacks through a variety of means including DDoS and information-stealer plugins.[129]

According to estimates, the intent of these cyberattacks was not necessarily to interfere with civil life in Ukraine, rather they were used to analyze Russia's ability to mount these types of attacks against other

126 Kim Zetter, "The Ukraine Power Grid was Hacked Again", *MotherBoard*, January 2, 2017; https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report

127 Jamie Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks", *MIT Technology Review*, December 22, 2016; https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks

128 Zetter, "The Ukraine Power Grid was Hacked Again."

129 "Frequently Asked Questions: BlackEnergy", *Trend Micro*, February 11, 2016; https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy

countries across the globe[130] – even brief power outages in Ukraine can have a significant psychological impact on Europe and the U.S.[131]

Russia does not limit the use of its cyber offensive capabilities to Ukraine; it also makes use of these capabilities against many Western countries, primarily the U.S. Reports on Russian cyberattacks targeting the U.S. came to a head in 2016 during the U.S. presidential elections, but the attacks began much sooner than this. In 2014, Russia recruited and trained trolls to work against leading U.S. news sites. The Russian premise behind the initiative was that Western media, greatly affected by its consumer audience, could not withstand a large-scale onslaught of pro-Russian messaging. In turn, this would force it to change the direction of its coverage to accommodate Russia and to appease pro-Russian readers. In effect, the initiative was not all that successful: most users exposed to Russian messages flooding these platforms assumed that they had been written for ideological reasons or that they were sponsored messages.[132]

Throughout the course of 2016, Russia accelerated its cyber efforts through two primary routes. The first was perceptual: pro-Russian media sources flooded the internet with a multitude of false reports designed to sow disinformation and uncertainty regarding the election campaign and its candidates. A U.S. intelligence investigation discovered that during the campaign, about one thousand Russian staff members operated to spread unfounded news reports against Democratic candidate

130 Zetter, "The Ukraine Power Grid was Hacked Again."

131 Sheera Frenkel, "The New Handbook for Cyberwar is being Written by Russia", *Buzzfeed News*, March 19, 2017; https://www.buzzfeed.com/sheerafrenkel/the-new-handbook-for-cyberwar-is-being-written-by-russia?utm_term=.eyw1G8q8V#.agy8kM6M2

132 Alexander Fokin, *Internet Trolling as a Hybrid Tool: the Case of Latvia,* (Riga: NATO Strategic Communications Centre of Excellence, 2015), 20 https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

Hillary Clinton.[133] For example, in August 2016, unfounded reports were spread to exacerbate concerns regarding Clinton's health.[134]

At the same time, hackers launched a range of cyberattacks against the U.S. election campaign infrastructure. In July 2016, Russian hackers broke into the Democratic National Committee's computers, leaking tens of thousands of hacked emails. The following month, hackers breached the voter databases of Arizona and Illinois, accessing the information of roughly 200,000 voters.[135] The breaches were carried out by hackers bundled into six different groups.[136]

According to the U.S. intelligence community, there were several motives behind the Russian-directed efforts in advancing the election of Donald Trump for the U.S. presidency. Putin felt that Clinton had personally backed protests organized against him that erupted throughout Russia in late 2011 and early 2012. In contrast, based on his positions, Russians considered Trump to be a potential partner in creating a global coalition to ramp up the fight against ISIS.[137]

Russian involvement, however, not only stemmed from its support of Trump. Distribution of 'fake news' against Clinton – and disruption of the various election campaign infrastructure networks – were part of Russia's broader strategic effort: when U.S. citizens are exposed to voting system glitches and the president is elected under a cloud of suspicion, they develop a general sense of distrust, not only doubt

133 "The Senate will investigate: '1000 Russian hackers spread Fake News against Clinton'", *Ynet*, March 30, 2017 https://www.ynet.co.il/articles/0,7340,L-4942627,00.html

134 Andrew Weisburd, Clint Watts and JM Berger, "Trolling for Trump: How Russia is Trying to Destroy our Democracy," *War on the Rocks*, November 6, 2016; https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy

135 Clint Watts, "Why Russia Wants the U.S to Believe the Election was Hacked," *Public Broadcasting Service*, October 26, 2016; http://www.pbs.org/wgbh/nova/next/tech/election-cybersecurity/

136 Chris Strohm, "Russia Weaponized Social Media in the U.S Elections, FireEye Says", *Bloomberg,* December 1, 2016; https://www.bloomberg.com/news/articles/2016-12-01/russia-weaponized-social-media-in-u-s-election-fireeye-says

137 *Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution*, (Washington: Office of the Director of National Intelligence, 2017), 1 https://www.dni.gov/files/documents/ICA_2017_01.pdf

in their leadership. When the credibility of American democracy is tarnished, the ability of the U.S. to build and bolster democratic governments in Eastern Europe – a delicate issue for Russia – is damaged as well.[138] This also contributes to undermining the credibility of legitimate and relatively objective moderators such as the media, academia and content experts. The ability of these entities to counter Russian operations is hampered, and as such, there is an ongoing process of information disruption along with diminished public trust in the content to which they are exposed.

138 Dana Priest, Ellen Nakashima and Tom Hamburger, "U.S. Investigating Potential Covert Russian Plan to Disrupt November Elections", *The Washington Post,* September 5, 2016; https://www.washingtonpost.com/world/national-security/intelligence-community-investigating-covert-russian-influence-operations-in-the-united-states/2016/09/04/aec27fa0-7156-11e6-8533-6b0b0ded0253_story.html?postshare=8261473103304697&tid=ss_tw

Case study comparative analysis

The case studies reflect the fundamental asymmetry characterizing the rules of the game in conducting an influence campaign. Liberal democracies like the U.S. are inherently obligated to adhere to rules of political accountability; this is typified by internal disagreement preventing the formulation of a uniform message, and by bureaucratic and political complexities. In contrast, countries such as Russia regard rules set by democracies as the existing world order that must be rattled and transformed. As such, Russia manipulates the media without a hint of hesitation, presenting a uniform narrative and allowing for the swift adaptation of influence campaign operations. For the U.S., its military operations against ISIS set a precedent because it was the first time that the cyber command was activated the in a military campaign. Resultantly, technological developments (such as cyber weapons) and different modus operandi were tried in real time, and several limitations of integrated influence operations and cyber warfare were identified:

No Logo Strategy

While the cyber offensive dimension is classified, the synchronization of overt IO is a challenge; according to overt material on the matter, the American IO was conducted without creating concealed or fake internet assets. In contrast, Russian operations performed in collaboration with military intelligence, Signal Intelligence (SIGNIT) units and outsourcing, have less restrictions, allowing for covert operations without needing to trace the operatives behind it. The resulting assumption is that covert U.S. cyber operations (and probably British operations as well) are performed by intelligence bodies such as the CIA, or via outsourcing. Accordingly, it appears that the U.S. Army's options are limited in terms of their sphere of influence and restricted with regards to the operative tools necessary for mounting cyber and IO overtly or covertly (in contrast with classified operations that offer flexibility in operating low signature cyber weapons).

Global collaboration

As aforementioned, the fact that ISIS servers are physically located in U.S. ally states necessitates a collaborative effort that results in low effectiveness in attacking ISIS assets controlled by other countries' servers. These servers have blocked the ability of the U.S. to conduct classified operations, due to the requirement to alert other entities and to request authorization before launching cyberattacks (such as shutting down servers located in other countries). Moreover, while the U.S. has restricted itself and avoids covert operations in other countries, Russia does not limit or restrict its cyber and IO campaigns against other countries or against internet assets located in third-party countries.

Synchronization operations

In contrast with the Russian synergy and close cooperation between various actors in the field, the coordination of disparate military units and diplomacy outfits has hampered the U.S. effort, complicating the ability to wage successful cyber perception warfare; this is not surprising given that the responsibility for coordinating and integrating efforts changed hands between numerous departments (from the State Department to the DoD) during the course of the web campaign launched against ISIS. Conversely, Russia's outlook is integrative and incorporates both political and military efforts in its cyber, psychological and IO.

Routine vs. emergency

While the U.S. has typically only waged psychological cyber warfare in times of conflict (and as part of the global coalition against ISIS), Russian efforts have been ongoing, garnering a lasting impact on a diverse target audience (not only before the Ukraine crisis, but also on other countries with an indirect effect on the situation in Ukraine, such as NATO Member States).

The use of offensive cyberattacks

The U.S. has focused its campaign on 'soft' targets such as social media sites and accounts, with the purpose of disrupting communications between ISIS operatives, gathering dedicated intelligence and breaching communication with potential recruits. In contrast, Russia's offensive

operations have also been directed at physical targets such as power grids, proving its success in damaging systems defined as critical infrastructure.

Summary

An effective information warfare campaign features cooperation between social media, intelligence and cyber units to amplify the tactical and strategical impact of military and political influence. The internet and social media have become highly instrumental in impacting social behavior, serving as key tools in influencing public perception and shaping our consciousness. In conflicts between countries – when one nation disrupts the information environment that its opponent depends upon – it is disrupting the enemy's ability to accurately grasp reality and establish an effective response. In this manner, the aggressor grants itself an advantage in the overall campaign. It delegitimizes the enemy, undercutting its credibility by sowing negative feelings, doubt, uncertainty and fear among the public perception; alternately, it can create positive feelings towards the aggressor. This also undermines the credibility of legitimate, relatively objective moderators such as the media, academia and content experts.

The architecture of the internet facilitates the creation and distribution of information through a 'personalization' model, whereby information is made accessible to individuals or groups through categorized engagement based on behavior, geography, interest, need, desire and passion. This enables social media to exploit algorithms that provide increased exposure to a narrative designed to disrupt the opposition's information environment. When such an operation is conducted – along with offensive cyber operations to disrupt the opponent's communications – the synergy between cyber and Influence Operations amplifies the aggressor's capacity, offering a new array of capabilities to target the adversary's digital information systems; this includes information leaks, blackmail and information deletion to disrupt the supply chain.

In the digital age, military and political organizations seeking to attain their goals must develop cyber capabilities to allow for timely change and flexibility, adapting their messaging to the relevant target audience and developing offensive cyber capabilities to influence their opponent. To meet operational objectives within the context of this type of warfare, it is necessary to conduct campaigns integrating

proactive cyber warfare activity and Influence Operations tools. To succeed, these organizations must assemble a range of capabilities that includes the development of dedicated cyber warfare tools tailored to the digital world in general and social media in particular.

This article defines the use of cyber tools for impacting the sphere of perception and influence as 'cyber perception warfare.' Both state and non-state actors use cyberspace in general - and social media in particular - as a tool to effect social and political change, and to shape consciousness. In the digital age, military or political organizations striving to meet targets and goals must develop 'soft' cyber capabilities to maintain flexibility and adapt quickly, altering messages for narrow or broad audiences. On the one hand, countries do not assign clear boundaries or set constraints on cyberspace activity or social media platforms; yet on the other hand, there is a need to meet operational goals in the domain of influence operations. It is imperative to conduct campaigns that combines proactive cyberwarfare with influence operations.

Daniel Cohen is a researcher at the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University. In addition, he is a Director of Intelligence and Strategy at the Abba Eban Institute for International Diplomacy at the Interdisciplinary Center (IDC) in Herzliya, and serves as a consultant/expert on CVE in the Organization for Security and Co-operation in Europe (OSCE).

Ofir Bar'el is an innovation in diplomacy researcher for the IDC in Herzliya, and a former research assistant at the Institute for National Security Studies (INSS) and at the Center for Political Research at the Ministry of Foreign Affairs.

Yuval Ne'eman Workshop for Science, Technology and Security was launched in 2002 by Prof. Isaac Ben-Israel in conjunction with the Harold Hartog School of Policy and Government and the Security Studies Program with the intention of exploring the link among security policy, technology and science. For this reason The workshop holds annual series of conferences and conducts research. The workshop covers various topics such as international relations and strategy, missiles and guided weapons, robotics, space policy and security, cyberspace and cyber warfare, the interplay between society and security, nuclear energy, homeland security, force build-up policy, government decision-making processes, and more.

ICRC
Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University