The Future Fight: Cyberwar at the Operational Level of War

A Monograph

by

MAJ Anthony J. Mattazaro
US Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2020

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 21-05-2020	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* JUN 2019 - MAY 2020

4. TITLE AND SUBTITLE The Future Fight: Cyberwar at the Operational Level of War	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Major Anthony J. Mattazaro, USA	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Advanced Military Studies Program	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The US Army's concept for multi-domain operations relies on cyberspace operations to support other domain operations. A question arises “How do militaries incorporate cyberspace operations to support operations in other domains?” To answer the question, Operation Allied Force, Iranian suppression of civil dissidence, and the Israel-Hamas conflict are analyzed. The results of analysis is that cyberspace operations at the operational level of war support other domain operations by gathering intelligence on adversaries to support future operations; denying or disrupting delivery avenues within the virtual-information domain; and affecting entities residing in the physical domain.

15. SUBJECT TERMS
Cyberwarfare, Cyber Operations, Cyber Support to Corps and Below, US Army, Iran, Israel, NATO, Green Movement, Operation Allied Force, Operation Pillar of Defense, Operation Outside the Box, Operation Protective Edge

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			MAJ Anthony J. Mattazaro
					19b. TELEPHONE NUMBER *(Include area code)*
(U)	(U)	(U)	(U)	48	

Monograph Approval Page

Name of Candidate: MAJ Anthony J. Mattazaro

Monograph Title: The Future Fight: Cyberwar at the Operational Level of War

Approved by:

__________________________________, Monograph Director
Jacob Stoil, PhD

__________________________________, Seminar Leader
Travis A. Jacobs, LTC

__________________________________, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 21st day of May 2020 by:

__________________________________, Acting Director, Graduate Degree Programs
Prisco R. Hernandez, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Abstract

The Future Fight: Cyberwar at the Operational Level of War, by MAJ Anthony J. Mattazaro, US Army, 66 pages.

Early success of cyberspace operations opened possibilities of new avenues to deliver effects to an adversary. As the US Army begins to transition to multi-domain operations they rely on cyberspace and to support other domain operations. A question arises "How do militaries incorporate cyberspace operations to support operations in other domains?" There exist no practical planning principles backed by evidence on how to incorporate cyber operations into other domain operations. Based on initial research a hypothesis arose that cyberspace operations that support the operational level of war synchronize with physical domain and virtual-information domain operations. Using accepted US military definitions for levels of war and operating domains, case studies that have activities at the operational level are analyzed. Operation Allied Force, Iranian suppression of civil dissidence, and the Israel-Hamas conflict are analyzed by collecting the following information from each case: strategic context, cyberspace actors, cyberspace actions, and how cyberspace actions supported other domain operations. The results of analysis is that cyberspace operations at the operational level of war support other domain operations by gathering intelligence on adversaries to support future operations; denying or disrupting delivery avenues within the virtual-information domain; and affecting entities residing in the physical domain.

Contents

Acknowledgements

Thanks to my monograph director Dr. Stoil for helping me from abstract idea to words on paper. Thanks to my wife for her support and understanding during the late times in the library and the basement.

Acronyms

ARCYBER	Army Cyber Command
C4I	Command, Control, Computers, Communications, Intelligence
CEMA	Cyber Electromagnetic Activities
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CS	Cyberspace
CSCB	Cyber Support to Corps and Below
CSO	Cyberspace Operations
CYBERCOM	US Cyber Command
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial-of-Service
DoD	Department of Defense
DODIN	DoD Information Network
EA	Electronic Attack
FM	Field Manual
ICA	Iranian Cyber Army
IDF	Israeli Defense Forces
IO	Information Operations
IoT	Internet of Things
IRC	Iranian Cyber Army
IRGC	Islamic Revolutionary Guard Corps
ISA	The Israeli Security Agency
ISP	Internet Service Provider
IT	Information Technology
IXP	Internet Exchange Point

JP	Joint Publication
MDB	Multi-Domain Battle
MDO	Multi-Domain Operations
NATO	North Atlantic Treaty Organization
NETCOM	US Army Network Enterprise Technology Command
OCO	Offensive Cyber Operations
OOB	Operation Outside the Box
OPD	Operation Pillar of Defense
OPE	Operation Protective Edge
SAM	Surface-to-Air Missiles
SEA	Syrian Electronic Army
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
UAV	Unmanned Aerial Vehicle

Illustrations

Introduction

In October 1806, the French Army swiftly defeated the Prussian Army at the battle of Jena-Auerstädt. A Prussian officer Carl Philipp Gottfried von Clausewitz was present at the battle and the defeat deeply troubled and perplexed him.[1] The Prussian Army outnumbered the French Army, however, the French Army wielded superior tactics over Prussia's outdated linear battle style. Clausewitz witnessed the future of warfare and was determined to evolve the Prussian Army into a force that would be the envy of Europe again.[2]

During the Russo-Ukrainian War in July 2014 near the village of Zelenopillya, Ukraine, four brigades of the Ukrainian Army Ground Forces prepared for an offensive against separatists' forces near the Russian boarder. On July 11, 2014, an intense three-minute artillery barrage struck elements of the four Ukrainian Brigades and destroyed a battalion of the Ukrainian 79th airmobile brigade. Analysis of the attack revealed that Russian forces used unmanned aerial vehicles to locate Ukrainian units and provided the locations to indirect fire platforms. The time from identification to effects was so fast than the Ukrainian brigades could not take protective actions. This small period in the Russo-Ukrainian war was so significant that the US Army Capabilities Integration Center initiated the Russian New Generation Warfare Study to determine the impacts of the Russo-Ukraine conflict on the future of warfare.[3]

In 2015 during a speech at the US Army War College, Deputy Secretary of Defense Bob Work outlined the problems of twenty-first-century warfare and charged the US Army to develop AirLand Battle 2.0.[4] In December 2018, the US Army took a doctrinal evolutionary step and

[1] Roger Parkinson, *Clausewitz A Biography* (New York: Stein and Day, 1971), 80–81.

[2] Ibid., 64, 66, 81.

[3] Shawn Woodford, "The Russian Artillery Strike That Spooked The U.S. Army," *Mystics & Statistics*, March 29, 2017, accessed October 1, 2019, http://www.dupuyinstitute.org/blog/2017/03/29/the-russian-artillery-strike-that-spooked-the-u-s-army/.

[4] Kelly McCoy, "The Road to Multi-Domain Battle: An Origin Story," *Modern War Institute*, October 27, 2017, accessed February 22, 2020, https://mwi.usma.edu/road-multi-domain-battle-origin-story/.

published *The U.S. Army in Multi-Domain Operations 2028* to address how the Army fights within multiple layers and domains.[5]

The Battle of Jena-Auerstädt and the Russo-Ukrainian War, though centuries apart, displayed the power of superior tactics and arrangement of operations. Clausewitz and the US Army witnessed defeats and reacted similarly by conducting in depth battle studies to better their respective armies. The output of the studies was guiding documents for the future conduct of war.

The US Army's adoption of multi-domain operations as a future operational construct relies on cyberspace operations to support other domain operations. However, there exist no evidence based practical planning principles concerning how to incorporate cyber operations into other domain operations. The problem for the military planner is how to integrate cyberspace operations to support other domain operations without experiencing a crushing defeat. The thesis is that cyberspace operations support other domain operations by gathering intelligence on adversaries to support future operations; denying or disrupting delivery avenues within the virtual-information domain; and affecting entities residing in the physical domain.

Literature Review

There exist several different categories of literature concerning cyberwarfare. There are investigative stories of a cyber event, compendiums of known information of the cyber domain, future and ethical concerns of cyberwar, and doomsday predictions in relation to cyberwar. However, a gap exists concerning cyberwarfare and the professional military practitioner. The literature directed to the military practitioner concerns only the most senior level of a military. There exists no literature that provides anything of value to the military planner or commander concerning integration of cyber effects or forces at the operational level of war.

[5] US Department of the Army, TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Washington, DC: Government Printing Office, 2018), i.

David Sanger's investigative book *The Perfect Weapon War, Sabotage, and Fear in the Cyber Age* chronicles significant cyber events and the rise of cyber weapons since the early 2000s. Sanger tells how the United States, China, Iran, North Korea, and Russia employed cyber weapons. Sanger's overall message is that the world is growing ever complex and he uses cyber weapons to highlight the complex world and how nations are capitalizing on the complexity. Sanger's book is an introduction to cyberwarfare and the significant cyberspace events that frame the current nation-state cyberwarfare environment.[6]

Pieces of literature that address future and ethical concerns of cyberwar provide varying perspectives of cyberwar. However, they do not address the challenge of today's cyberwar. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* is a collection of literature focused on exploring the future of cyber and information warfare. Different authors from American and British government, academic, military, and private industry wrote the various sections of the book. The topics of the sections range from theories on information warfare, applications of information into future warfare, cyber and information strategies within the National Security Strategy, and psychological implications information war. The book presents varied perspectives and avenues of consideration during the rise of information and cyberwarfare. The book leaves more questions open then answered and does not address cyber and information operations at the operational level of war.[7]

The most prevalent pieces of literature concerning cyberspace are compendiums of information on cyberspace. These pieces focus on informing a wide audience and inform the reader of the very basic aspects of cyberspace to advanced topics. *Cyber Warfare and Cyber Terrorism* is a compendium organized into a reference book. The book covers more modern concepts of cyberwarfare and cybercrime and defines concepts and terms used within the cyber

[6] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, First edition. (New York: Crown Publishers, an imprint of the Crown Publishing Group, 2018).

[7] Alan D. Campen and Douglas H. Dearth, eds., *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (Fairfax, VA: AFCEA International Press, 2000).

security community. Compared to *Cyberwar 3.0, Cyber Warfare and Cyber Terrorism* is less future oriented, addresses topics of cybersecurity, and dives deep into cybersecurity tactics. *Cyber Warfare and Cyber Terrorism*'s audience is the civilian, military, or law enforcement cybersecurity practitioner and provides enhanced cybersecurity and investigative techniques. However, *Cyber Warfare and Cyber Terrorism* is both too broad and specific. The book addresses little about the integration of cyber effects at the operational level and is more focused on combating and investigating cyber events.[8]

The final category of literature is doomsday predictions of cyberwar. These books theorize the future of cyberwar in the most extreme cases. *On Cyber* is a contemporary book aimed at the military professional, policy makers, and cybersecurity practitioners. It is part future focused with undertones of a dooming future if the military does not address cyberspace. Two retired military service members with academic and military cybersecurity backgrounds co-authored *On Cyber*. The book is a leap towards an operational art for cyber conflict. It melds modern cybersecurity parlance with military doctrine to produce an operational art for the cyberwarfare practitioner. It is both broad and deep in certain topics. Key topics are cyber actors, advisories, environment, maneuver, capabilities, command and control, and a future perspective. Within each section the authors consider existing military and cybersecurity frameworks and attempt to meld the two with the purpose of generating discussion on how militaries fight and defend in cyberspace.[9]

Conti and Raymond push the bounds of military doctrine and cybersecurity practice with a look to the future of cyberwarfare and implications for the military leader and policy maker. *On Cyber* is one of the few books that attempts to provide the military cyber practitioner something solid with which to plan and integrate cyber operations into conventional military operations.

[8] Lech Janczewski and Andrew M. Colarik, eds., *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2008).

[9] Greg Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict* (Kopidion Press, 2017), v.

However, in the end, the authors purposely wrote *On Cyber* to generate conversation and stimulate the future of cyber operational art and not provide a roadmap or guide for the cyber professional.[10]

The literature review exposed a gap in the study of cyberspace battles and their integration into and with the military on the contemporary battlefield. This monograph aims to fill this gap by chronicling three accounts of cyberspace actions integrated with physical domain operations at the operational level of war.

Methodology

Clausewitz and the US Army identified a shift in the conduct of war and responded in similar fashion. Clausewitz's approach relied on in-depth examination of campaigns through research using primary sources.[11] Similarly, the US Army reacted to the Russo-Ukraine war by conducting a study of the conflict using the US Army Capabilities Integration Center. Though separated by centuries, their methodologies attempted to understand the changing conduct of war to evolve their militaries.

[10] Conti and Raymond, *On Cyber*.

[11] Christopher Bassford, "Clausewitz and His Works," *Clausewitz and His Works*, last modified March 8, 2016, accessed February 26, 2020, https://www.clausewitz.com/readings/Bassford/Cworks/Works.htm.

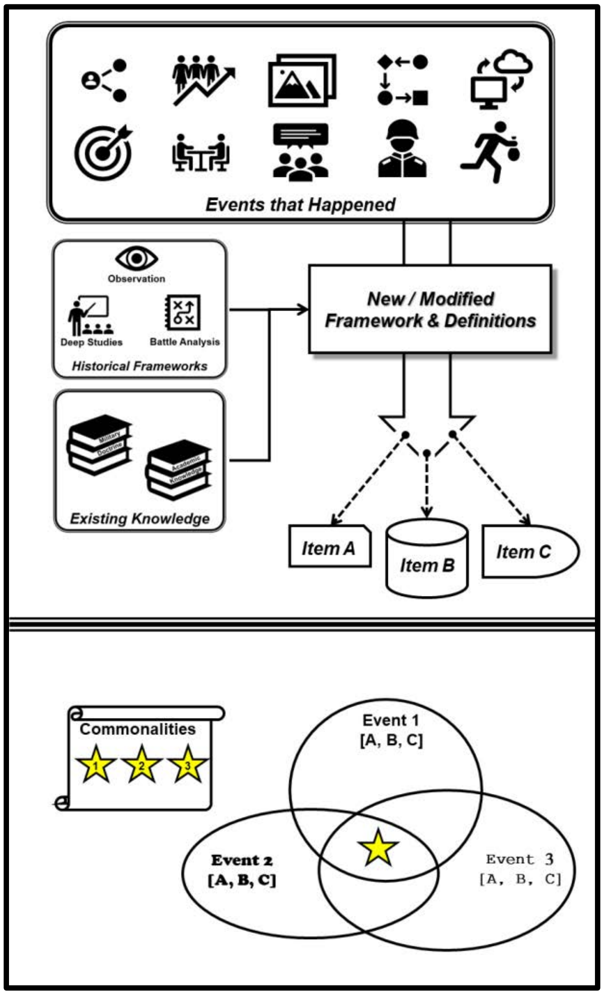


Figure 1. Case Study Methodology. Created by author.

This monograph uses case analysis of cyber operations at or that supported the operational level of war. Understanding operational domains, levels of war, and operational environments helps identify relevant cases for further study. Appropriate cases for further study have activities at the operational level of war and in cyberspace. The analysis of cases derives facts pertaining to the cyberspace actions which includes, the cyberspace actors and their actions in cyberspace and how the cyberspace actions supported other domains activities. Finally, overlaying the facts of all cases helps identify similarities between how cyberspace actions are executed and how they support other domain operations (see Figure 1).

Background

Multi-domain operations are more than an understanding of the complexity of each operating domain but understanding how operations in each domain integrate, support, and effect operations in other domains. Understanding the different levels of war and operating domains helps understand the convergence of domain in military operations.

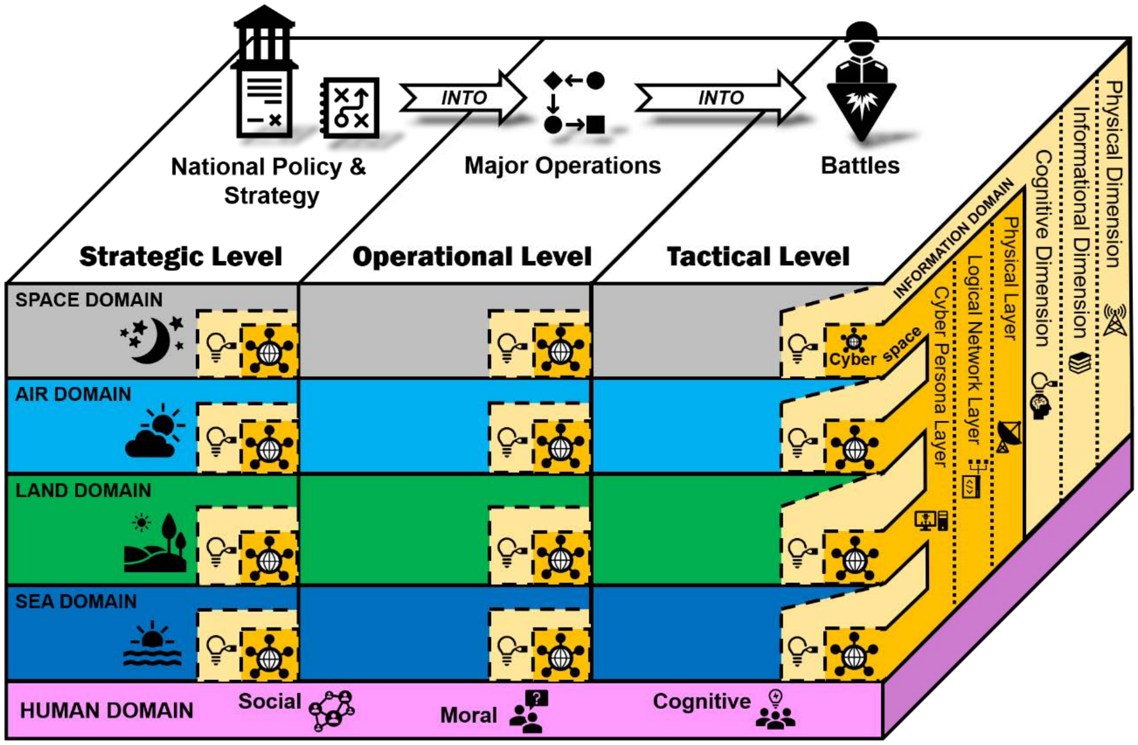


Figure 2. Convergence of Domains and Levels of War. Created by author.

Figure 2 depicts the convergence of the levels of war and operating domains. The convergence creates a complex space in which the militaries of the world conduct operations to achieve their objectives. The United States' Joint Staff's joint publication (JP) 3-0, *Operations*, defines three levels of war—strategic, operational, and tactical (see Figure 3).[12] At the strategic level of war leaders develop strategy to employ the instruments of national power in a

[12] US Department of Defense, Joint Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, 2017), xi.

synchronized and integrated way to achieve national objectives.[13] The strategic level of war addresses *why and with what* a nation fights against an adversary.[14] The operational level of warfare links and translates actions at the tactical level to national strategic objectives.[15] United States Army Field Manual (FM) 3-0, *Operations*, expands the definition of the operational level of war "At the operational level, commanders conduct campaigns and major operations to establish conditions that define that end state." A campaign is a series of operations within time and space aimed at achieving an objective. An operation is a series of tactical actions or battles coordinated in time and space to achieve an objective.[16] The Joint Staff's joint publication 3-0, *Operations,* defines the tactical level of war as where forces are employed, arranged, and interact with each other on the battlefield.[17] The tactical level of war is concerned with how a military fights to achieve objectives[18]

[13] Ibid., I–12.

[14] US Department of the Air Force, Basic Doctrine, *vol. I* (Maxwell AFB, AL: United States Air Force, 2015), 44.

[15] US Joint Staff, JP 3-0 (2017), I–13.

[16] US Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: Government Printing Office, 2008), 6–3.

[17] US Joint Staff, JP 3-0 (2017), I–13.

[18] US Air Force, Basic Doctrine, I:45.

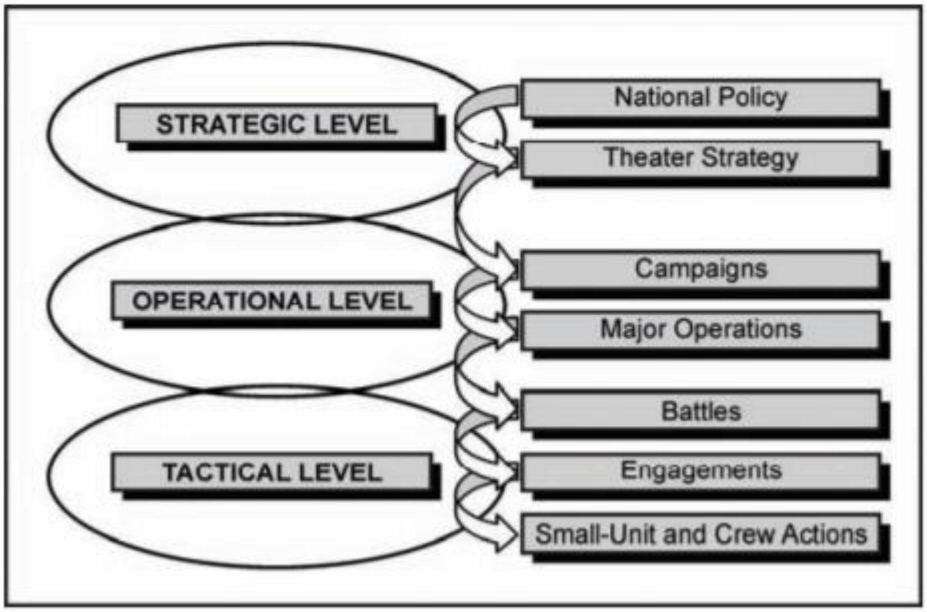


Figure 3. The Levels of War. US Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: Government Printing Office, 2008), 6–2.

In 2005 *Capstone Concept for Joint Operations,* the Joint Staff listed ten operating domains in three categories—physical, virtual, and human. The physical domain encompasses the land, sea, air, and space domains; the virtual domain encompasses the cyber and information domains; and the human domain encompasses the social, moral, and cognitive domains.[19] The overlay of military operations on top of the domains is called the operational environment. US joint doctrine defines the operational environment as the physical areas of the air, land, maritime, and space domains but also includes the information environment. Enemy, friendly, and neutral forces exist and operate within the operating environment.[20]

The information environment is a broad and transcends all physical, virtual, and human domains. The Joint Staff's joint publication 3-0, *Operations,* describes the information environment as the aggregate of numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, and actions of an individual or

[19] US Department of Defense, Joint Staff, *Capstone Concept for Joint Operations*, 2nd ed. (Washington, DC: Government Printing Office, 2005), 16.

[20] US Joint Staff, JP 3-0 (2017), IV–1.

group. The information environment is broad and touches all other domains in some way.[21] US Army field manual 3-13, *Information Operations,* further expands on the information environment by describing three dimensions of the information environment—physical, informational, and cognitive. The physical dimension supports the transmission, reception, and storage of information. The informational dimension is the content and flow of information and links the physical and cognitive dimensions. The cognitive dimension is the minds of those affected by the receipt of information.[22]

Within the information environment lies the cyber environment, also known as cyberspace. The Joint Staff's joint publication 3-12, *Cyberspace Operations*, defines cyberspace as "the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[23]

The Joint Staff's joint publication 3-12, *Cyberspace Operations*, further describes cyberspace as three connected layers—physical network layer, logical network layer, and cyber-persona layer. The physical network layer are the information devices and infrastructure in the physical domains that store, transport, and process information within cyberspace. The logical network layer are the components of the network related to one another through an abstraction. The cyber-persona layer is a further abstraction from the logical layer. It is the human or automated information user accounts and their interconnection to one another. Cyber-personas may relate directly to an actual person or entity. A single person can have multiple cyber-

[21] Ibid., IV-1-IV–2.

[22] US Department of the Army, Field Manual (FM) 3-13, *Information Operations* (Washington, DC: Government Printing Office, 2016), 1–2.

[23] US Department of Defense, Joint Staff, Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: Government Printing Office, 2018), I–1.

personas and a single cyber-persona can have multiple persons that use the persona to interact with cyberspace.[24]

The Joint Staff's joint publication 3-12, *Cyberspace Operations*, also considers cyberspace as part of the information environment and a medium through which information operations are executed.[25] Army field manual, 3-13, *Information Operations*, describes information operations (IO) as the integrated employment of information-related capabilities synchronized with operations to influence, disrupt or corrupt the decision-making of adversaries and potential adversaries.[26] The purpose for conducting IO is to create an effect in the information environment that provides the commander an advantage over adversaries.[27] The Joint Staff's joint publication 3-12, *Cyberspace Operations*, defines cyberspace operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[28] Cyberspace objectives and effects can be separate from physical domain objectives; however, most cyberspace operations are synchronized with other domain operations to create unified effects.[29]

Considering the levels of war and operating environments, a synthesized definition of the operational level of war is below and carried through the monograph to identify cyberspace operations at the operational level of war.

> At the operational level of war, organizations plan and execute campaigns and major operations to achieve strategic objectives within a specific time and space. One or several military branches, government agencies, and collectives work together to achieve a common strategic objective. Operations at the operational level translate tactical actions into achievement of strategic objectives.

[24] Ibid., I-2-I–4.

[25] Ibid., I–7.

[26] US Army, FM 3-13, 1–2.

[27] Ibid., 1–4.

[28] US Joint Staff, JP 3-12 (2018), I–1.

[29] Ibid.

Case Studies

Operation Allied Force

Strategic Context of Operation Allied Force

Operational Allied Force was a North Atlantic Treaty Organization (NATO) air campaign against the Federal Republic of Yugoslavia from March 24, 1999 to June 10, 1999. The campaign was in response to Yugoslavia's leader Slobodan Milošević's reduction of Kosovo's independent status and the 1989 cultural repression of the Albanian population within the state of Serbia (see Figure 4).[30]

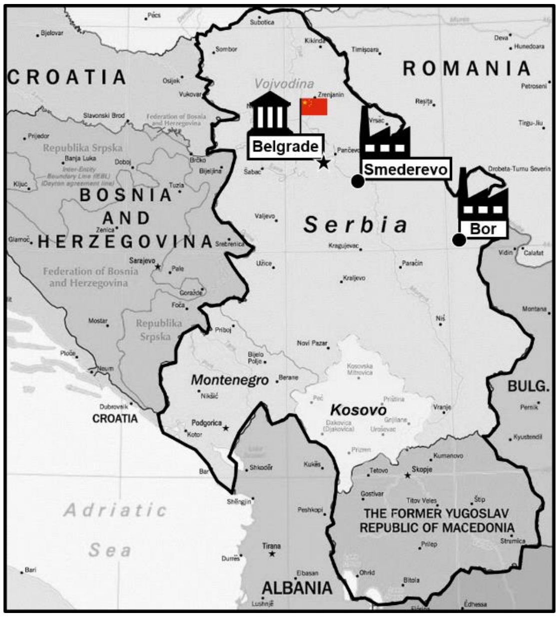


Figure 4. Operation Allied Force Area of Operations. Created by the author. Data for base map from https://archive.defense.gov/specials/kosovo/images/balkans1.jpg, accessed February 17, 2020.

The Federal Republic of Yugoslavia existed as a union of Serbia and Montenegro. Slobodan Milošević was the president of Serbia and then Yugoslavia from 1997 to 2000. Kosovo existed within the state bounds of Serbia but contained mostly ethnic Albanians. In 1998 war between Serbia and Kosovo broke out over ethnic tensions and Kosovo's declared its

[30] William Merrin, *Digital War: A Critical Introduction* (New York, NY: Routledge Taylor & Francis Group, 2019), 18.

independence. The conflict heightened when the Serbian military purposely killed forty-five Albanians living in Kosovo. The international community offered settlements to end the violence, but Serbia refused to accept any terms that led to an independent Kosovo.[31]

In response to Serbia's continued aggression towards Albanians in Serbia, NATO launched Operational Allied Force on March 24, 1999 with 1,000 aircraft and conducted 38,000 bombing missions against Serbian military targets in Yugoslavia for seventy-eight days. NATO limited operations to striking military targets in Yugoslavia with the use of air forces. On June 3, 1999, all parties agreed to a permanent cease fire.[32]

Cyberspace Actors of Operation Allied Force

The cyberspace actors of Operation Allied Force consisted of two groups: pro-Serbian and NATO military forces. NATO organized military forces to conduct information and cyberspace operations to support covert and overt military operations.[33] The prominent pro-Serbian group, The Black Hand (aka. Modern Black Hand), was a loose collective of non-military Serbians citizens with computing backgrounds.[34] Chinese hackers joined Serbian efforts to attack NATO in cyberspace after NATO forces bombed the Chinese embassy in Belgrade on May 7, 1999. Russian hackers also aided Serbian hackers by conducting cyberattacks against NATO.[35] Independent hacking groups such as The Chaos Hackers Crew and Hong Kong Danger Duo sporadically joined Serbian cyberattacks against the United States and NATO.[36]

[31] Ibid.

[32] Ibid.

[33] Andrew Rathmell, "Information Operations--Coming of Age?," *Jane's Intelligence Review* 12, no. 5 (May 2000): 53.

[34] "Net Warfare over Kosovo," *BBC News*, October 23, 1998, accessed August 25, 2019, http://news.bbc.co.uk/2/hi/science/nature/200069.stm.

[35] Nikola Milosevic, "Case of the Cyber War: Kosovo Conflict," *Inspiratron*, July 1, 2014, accessed August 25, 2019, http://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/.

[36] Douglas Thomas and Brian Loader, eds., *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age* (New York, NY: Routledge, 2000), 66; William Merrin, *Digital War: A Critical Introduction* (New York, NY: Routledge Taylor & Francis Group, 2019), 20.

Cyberspace Actions during Operation Allied Force

Pro-Serbian actions in cyberspace began after NATO started Operation Allied Force. Pro-Serbian hacking was overt, opportunistic, reactionary, and focused on delivery of pro-Serbian propaganda and disruption of NATO's websites. The Black Hand defaced NATO and western government websites, executed denial of service attacks, and delivered viruses to NATO countries via email.[37] Chinese hackers joined denial of service attacks against NATO's websites and networks.[38] The Hong Kong Danger Duo deleted the website *whitehouse.gov* and replaced it with anti-US propaganda. Black Hand downed NATO's public affairs website and email system—NATO acknowledged the website's interruption in a press briefing.[39] Pro-Serbian groups exploited any available gap in cyberspace to disrupt NATO operations.

Pro-Serbian hackers used a variety of methods to attack NATO's websites and networks. On March 27 and 28, 1999, Serbians disrupted access to NATO's public website with a ping bombardment (see appendix 1). NATO reported that its military operations network remained unaffected. NATO personnel also received several e-mails originating from Serbia that contained viruses. NATO network users received 2000 virus infected emails per day.[40] NATO was public about the effects of cyberattacks against their websites. They identified a ping saturation attack (see appendix 1) from Serbia as the cause for downing NATO's email server and *NATO.int* website. In April 1999, NATO suspected that the Serbian military was responsible for the

[37] Merrin, *Digital War*, 20.

[38] Milosevic, "Case of the Cyber War."

[39] Merrin, *Digital War*, 20.

[40] Niala Boodhoo, "NATO Gets Spammed," *PC World News*, April 1, 1999, accessed October 24, 2019, https://web.archive.org/web/19991009033442/http:/www.pcworld.com/pcwtoday/article/0,1510,10358,00.html.

network denial attacks.[41] NATO received the brunt of Serbian attacks in cyberspace and received multiple attempts to penetrate their public networks.

The Black Hand hacked *kosova.com* and made it inaccessible for days. In October 1998, Black Hand took control of an Albanian newspaper's website *Zik.com*.[42] On October 20, 1998, the Kosovo Information Centre (KIC), which supported the party of the Albanian leader Dr. Ibrahim Rugova, reported that the Black Hand hacked the KIC website.[43] A Serbian hacker posted anti-Kosovo Albanian messages to an online edition of the Kosovar newspaper *Glas Kosova*, forcing the internet provider to withdraw digital access to the newspaper.[44] Pro-Serbian hackers exploited successful hacks to spread Serbian propaganda within the Balkan region.

Pro-Serbian efforts denied propaganda outlets and spread their own propaganda worldwide. Non-military Russians hacked the US Navy's website, erased information on the website, and replaced the website with anti-US propaganda. They also hacked the website of Orange Coast college, a US based college, and posted anti-US messages on the website.[45] Additionally, pro-Serbian hackers disrupted access to and deleted content from the websites of the Federal Bureau of Investigation and US Senate.[46] Pro-Serbian hackers protested the United States' involvement in Operation Allied Force by attacking the United States in cyberspace and spreading anti-US messages on their websites.

From April 1 to 17, 1999, pro-Serbian hackers sent emails to businesses, organizations, and academic institutions in NATO and non-NATO member countries. The emails originated

[41] Ellen Messmer, "Serb Supporters Sock It to NATO, U.S. Web Sites," last modified April 6, 1999, accessed September 24, 2019, http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html.

[42] "Net Warfare over Kosovo," *BBC News*, October 23, 1998, accessed August 25, 2019, http://news.bbc.co.uk/2/hi/science/nature/200069.stm.

[43] "War of Words on the Internet," *BBC Monitoring*, last modified October 25, 1998, accessed September 24, 2019, http://news.bbc.co.uk/2/hi/world/monitoring/200708.stm.

[44] Ibid.

[45] Messmer, "Serb Supporters Sock It to NATO, U.S. Web Sites."

[46] Milosevic, "Case of the Cyber War."

from a range of Eastern European countries and contained anti-NATO messages, Serbian propaganda cartoons, and attachments containing multiple viruses. The email recipients included, newspaper publishers, academic institutions, internet service providers, and e-commerce companies in the United Kingdom, United States, Germany, Italy, Denmark, and Switzerland.[47] Pro-Serbian hackers turned their hacking efforts towards targets worldwide in an effort to bring further attention to their cause and the perceived injustice of Operation Allied Force.

The US military covertly established an information warfare group to support NATO's air campaign and information operations.[48] The US military conducted cyberattacks against Yugoslavian military air defenses from satellite and aircraft.[49] The cyberattacks placed false targets into Yugoslavian air defense systems using an air to ground vector of attack.[50] The commander of US air forces in Europe, confirmed the execution of the operations.[51] As part of NATO, the United States used specialized technology to affect systems in the physical domains through cyberspace.

To support Operation Allied Force, the United States developed an information operation named Operation Matrix to influence senior Yugoslav leaders to persuade Milošević to agree to NATO's demands. Operation Matrix originated in December 1998, with a meeting between the US envoy to the Balkans, the US President, and US Secretary of State's special adviser for

[47] "Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries," *Mi2g Cyber Warfare Advisory*, April 19, 1999, accessed October 24, 2019, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/170499.php.

[48] Merrin, *Digital War*, 20.

[49] David A. Fulghum, "Telecom Links Provide Cyber-Attack Route," *Aviation Week & Space Technology*, November 8, 1999, 82–83.

[50] David A. Fulghum, "Yugoslavia Successfully Attacked by Computers," *Aviation Week & Space Technology*, August 23, 1999, 31, 34.

[51] William M. Arkin, "The Cyber Bomb in Yugoslavia," *The Washington Post*, October 25, 1999, accessed August 28, 2019, https://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

Kosovo. They devised a strategy to undermine Milošević's authority and pressure him to agree to NATO's demands. However, the NATO commander denied the operation existed.[52]

The US Central Intelligence Agency targeted Milošević's cronies by intercepting their phone conversations and delivering messages to their cell phones, fax machines, and email accounts. The messages urged them to persuade Milošević to comply with NATO's demands.[53] These tactics became known as "crony targeting." NATO did not bomb the Serbian cell phone network, telephone switches, and computer control centers during the Operation Allied Force. NATO's decision to avoid destroying nodes in the physical layer of cyberspace supported the delivery of messages to Milošević's cronies and ensured that avenues remained open in the physical dimension to continue Operation Matrix. [54]

To support Operation Matrix, the United States modeled Milošević's inner circle and person to person connections using intelligence gained through cyberspace surveillance. The connectional relationships showed which cronies had the most influence on Milošević. They uncovered a kickback scheme at a steel plant in Smederevo where the head of the plant and ex-deputy leader of Milošević's political party, Dusan Matkovic, turned steel production into a source of money for Milošević's cronies. At a copper plant in Bor, Nikola Sainovic, a former deputy prime minister, used his management position to siphon gold from the plant. On the night of May 15, 1999, US bombers attacked the Serbian industrial facilities at Bor and Smederevo (see Figure 4). Before the raid, United States and British information warfare specialists sent messages through e-mail, fax, and cell phones to threaten the plant owners of the attack. The messages sent

[52] William M. Arkin, "Ask Not for Whom the Phone Rings," *Http://Www.Washingtonpost.Com*, last modified October 11, 1999, accessed September 25, 2019, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin101199.htm.

[53] Rodney P Carlisle, Encyclopedia of Intelligence and Counterintelligence (New York, NY: M.E. Sharpe, 2015), 457.

[54] Arkin, "Ask Not for Whom the Phone Rings."

to the cronies reinforced the effects of the air strikes and the air strikes gave creditability to the messages and any future messages.[55]

How Cyberspace Actions during Operation Allied Force Supported Operations in other Domains

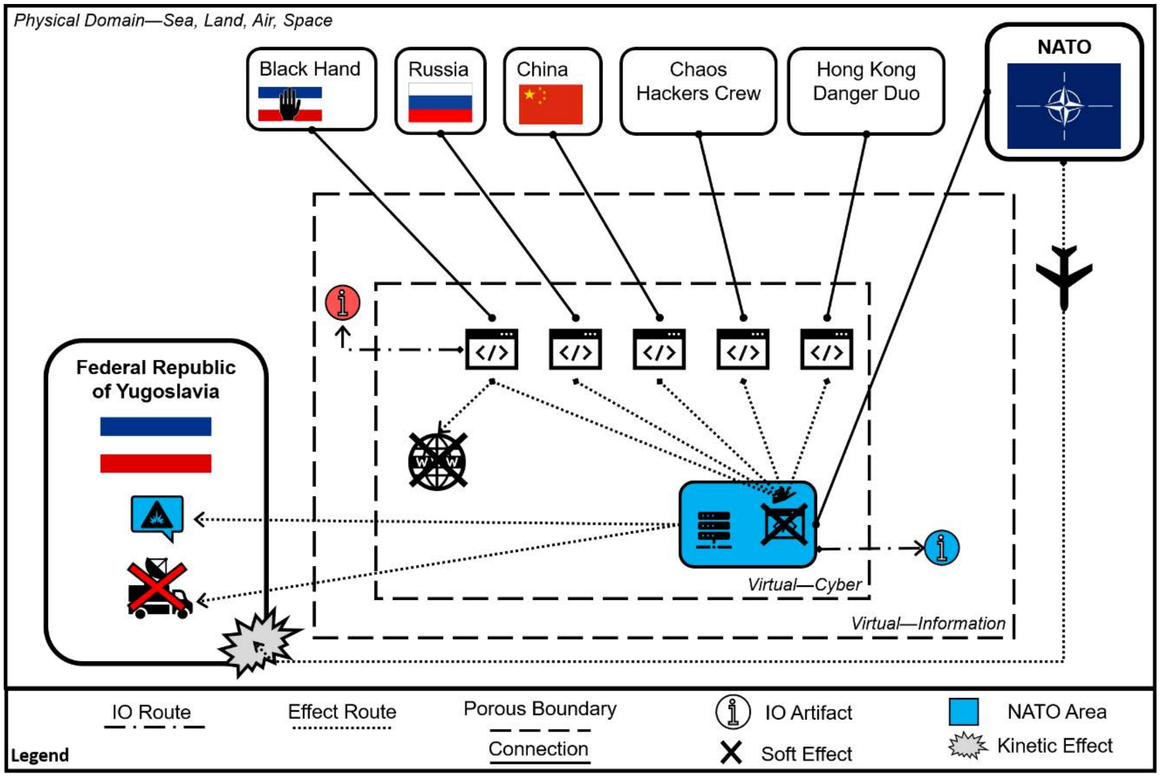


Figure 5. Operation Allied Force Cyberspace Operations. Created by the author using images from https://en.wikipedia.org/ distributed under CC-BY 2.0 license 2020.

The Serbian military lacked integration with independent pro-Serbian cyberspace actors. As a result, actions in cyberspace did not synchronously align with Serbian military operations. Additionally, effects realized by targets were short in duration and targets recovered quickly from pro-Serbian cyberattacks. Despite the mild effect of cyberattacks, pro-Serbian efforts disrupted NATO's ability to conduct operations in the virtual-information domain. They accomplished this by contesting NATO's ability to use the informational dimension of the information environment and the logical network layer of cyberspace to conduct information operations—compromising

[55] William M. Arkin and Robert Windrem, "The Other Kosovo War," InfoSec News, last modified August 29, 2001, accessed November 6, 2019, http://lists.jammed.com/ISN/2001/08/0196.html.

websites, attacking NATO's computer networks, and spreading pro-Serbian propaganda.[56] Serbians also attacked NATO member and western countries' ability to deliver information through cyberspace (see Figure 5). The effects limited the global avenues in the informational dimension that NATO could use to support information operations.[57] Pro-Serbian actions in cyberspace indirectly supported Serbian military operations by denying or disrupting NATO's ability to conduct information operations.

NATO coordinated their operations in the virtual-cyber domain to support NATO air strikes in the physical-air domain and used the physical and logical layers of cyberspace as avenues to conduct operations in the virtual-information domain. NATO used cyberspace as an avenue to manipulate the Serbian air defense systems to allow NATO air forces to penetrate air defenses and strike Serbian military targets.[58] NATO used the physical and logical layers of cyberspace to deliver influential information via cell phone, fax, and email messages to Milošević's cronies to influence them to support NATO's objectives. NATO also purposefully did not affect key nodes in the physical dimension of the information environment and physical layer of cyberspace to enable the execution of Operation Matrix.[59]

Iranian Suppression of Civil Dissidence

Strategic Context of the Iranian Civil Dissidence 2005-2019

From 1997 to 2005 Iran's president Mohammad Khatami's significantly relaxed government censorship and allowed reformist newspapers and journalists to operate in relative

[56] Kenneth Geers, Cyberspace and the Changing Nature of Warfare (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008), accessed October 20, 2019, https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf.

[57] "Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries," Mi2g Cyber Warfare Advisory, April 19, 1999, accessed October 24, 2019, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/170499.php.

[58] Andrew J. Bacevich and Eliot A. Cohen, eds., *War over Kosovo: Politics and Strategy in a Global Age* (New York: Columbia University Press, 2001), 196.

[59] William M. Arkin and Robert Windrem, "The Other Kosovo War," InfoSec News, last modified August 29, 2001, accessed November 6, 2019, http://lists.jammed.com/ISN/2001/08/0196.html.

freedom.[60] In August 2005 Iranians elected Mahmoud Ahmadinejad president of Iran. Ahmadinejad reversed Mohammad Khatami's liberalization of the Iranian media by tightening government control of all types of media and placing direct government control over key pieces of media infrastructure. On June 12, 2009 Iran held another presidential election and Ahmadinejad won in a surprise landslide. Thousands of Iranians fervently protested Ahmadinejad's election.[61]

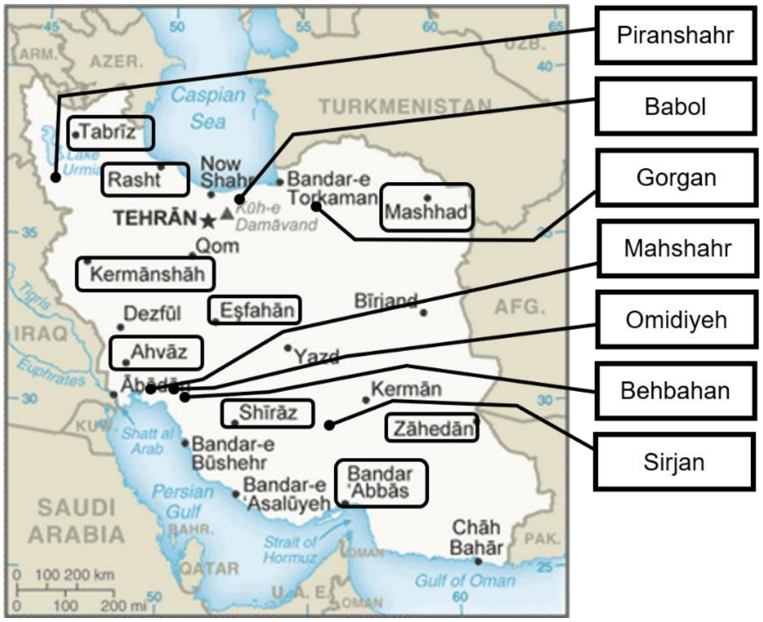


Figure 6. Locations of Iranian Protests 2005-2019. Created by the author. Data for base map from United States Central Intelligence Agency, Iran Map, (Washington, DC: Central Intelligence Agency, 1988), accessed February 17, 2020. Data for protest locations from United States Institute of Peace: The Iran Primer, Updated December 2018, 2019, accessed February 17, 2020, https://iranprimer.usip.org/blog/2019/nov/18/protests-overview.

Many Iranians believed Ahmadinejad's victory was fraudulent and were unhappy with his domestic changes. Progressive Iranians held public demonstrations and rallies in Iranian university campuses and major Iranian cities (see Figure 6). Internet-based mobilization was particularly important to organizing demonstrations and stirring anti-Ahmadinejad fervor.[62] The

[60] *Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election* (Santa Monica, CA: RAND, 2012), 13.

[61] Ibid., 14.

[62] Ibid., 1.

protests evolved into the Green Movement, also known as the Persian Awakening, Persian Spring, Green Revolution, or Jonbesh-e Sabz. The two reformist presidential candidates, former Prime Minister Mir Hussein Mousavi and former Parliament Speaker Mehdi Karroubi were the leaders of the Green Movement.[63] The Green Movement caused great concern for Iran's supreme leader Ayatollah Ali Khamenei and Ahmadinejad. They feared the consequences of internal dissidence but also feared that Iran's enemies would utilize the unrest to meddle in Iran's domestic affairs.[64]

The Cyberspace Actors during Iranian Civil Dissidence

The members of the Green Movement, also known as "greens," were composed mostly of Iranians citizens.[65] The Green Movement's goals was to delegitimize and expose the corruption of the Iranian government.[66] They relied on Twitter, Facebook, text messaging, and blogs to coordinate public demonstrations and spread political manifestos.[67]

The Iranian government founded the Islamic Revolutionary Guard Corps' (IRGC) Center for Investigating Organized Cyber Crimes in 2007 as an internet policing organization. They were responsible for combatting the Greens' cyberspace activities.[68] In 2005, Iranian hackers formed the Iranian Cyber Army (IRC) from well-established hacking groups such as the Ashiyaneh

[63] Ibid., 14.

[64] Karim Sadjadpour and Collin Anderson, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge* (Washington, DC: Carnegie Endowment for International Peace, 2018), 10, https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134.

[65] Michael Slackman, "On Anniversary, Ahmadinejad Boasts of Iran's Nuclear Prowess," *The New York Times*, February 11, 2010, sec. Middle East, accessed November 19, 2019, https://www.nytimes.com/2010/02/12/world/middleeast/12iran.html.

[66] "Iran: State of the Green Movement," *Foreign Policy Initiative*, last modified April 6, 2010, accessed November 19, 2019, https://web.archive.org/web/20160827141650/http:/www.foreignpolicyi.org/event/iran/greenmovement.

[67] *Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election*, 14.

[68] Ibid., 16.

collective.[69] The IRC grew during the 2009 elections to assist countering Green activity in cyberspace. IRC disrupted the Greens' ability to communicate using the internet and collected information on persons in within the Green movement.[70] The IRC initially was under the loose direction of the Iranian government but became more structured and integrated with the government as Iran embraced cyberspace operations.[71]

Cyberspace Actions during Iranian Civil Dissidence

The Green Movement's activism and protests heighted after the 2009 Iranian presidential election. As Green activity increased, the Iranian government also increased their efforts to combat the dissidence. In April 2009, the Iranian Parliament passed a bill that required all candidates to register their blogs and websites with the Ministry of Culture and Islamic Guidance.[72] One week before the elections, the Iranian government blocked Iranian internet users' access to social media websites.[73] From June 10 to 13, 2009, the Iranian government disconnected mobile phone and text messaging services before the polls opened. Access remained unavailable until after election day.[74] The Iranian government also increased filtering of social networking sites and mobile phones until the election concluded.[75] Iran's control the telecommunication infrastructure enabled them to restrict access to the logical layer of cyberspace and the information dimension of the information environment.

[69] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," *FRONTLINE - Tehran Bureau*, last modified February 26, 2010, accessed October 31, 2019, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html.

[70] Sadjadpour and Anderson, *Iran's Cyber Threat*, 11.

[71] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," *FRONTLINE - Tehran Bureau*, last modified February 26, 2010, accessed October 31, 2019, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html.

[72] *Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election* (Santa Monica, CA: RAND, 2012), 13.

[73] Somayeh Moghanizadeh, "The Role of Social Media in Iran's Green Movement" (Master of Communication, University of Gothenburg, 2013), 10.

[74] *Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election*, 14.

[75] Moghanizadeh, "The Role of Social Media in Iran's Green Movement," 10.

Iran's restriction on internet traffic affected the Greens' ability to organize through social media sites. Greens used social media sites as a trusted intermediary to share ways to communicate securely and anonymously. The Green's appealed to Twitter users to adjust their time zone settings to reflect the Iranian time zone. This caused the number of Twitter users that were physically located outside of Iran to logically appear in Iranian cyberspace—adding difficulty to Iran's effort to silence dissidence. The Greens also used proxy servers to bypass Iranian internet restrictions and reach blocked websites (see appendix 1).[76] Connectivity to the internet directly enabled the Greens' ability to organize protests and to spread their ideas quickly and widely.

In addition to filtering the internet, Iran began using the information collected from cyberspace to identify Green personnel and the locations of future protests. In June 2009, the government intentionally removed blocks to social networking sites and mobile phone data with the purpose of collecting information from users. The government monitored sites where Greens posted proxy server information and added the locations to an internet blocked list. Iran used the website of a state television show called *Gerdab* to expose Green bloggers. The *Gerdab* website showed photos of Iranian protestors to its visitors and asked visitors to identify them. In late 2009, Iran used their control of the physical layer of cyberspace to send potential protestors threating text messages and messages through social networking sites to dissuade them from attending rallies. Early after the elections, the Iranian government began using its control of the physical layer of cyberspace to collect information on protestors.[77] The government used the information to block Greens' access to the logical layer and target Greens' during information operations.

On December 19, 2009, the government blocked connections to Twitter's website and redirected users to a pro-government website. The Iranian Cyber Army compromised a Twitter

[76] *Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election*, 14-16.

[77] Ibid., 14-17.

employee’s computer with a virus and changed an administrative setting that caused the redirection (see appendix 1). On January 12, 2010, the ICA disabled access to a Chinese search engine called *Baidu* and directed users to a pro-government message. On January 30, 2010, the ICA hacked Radio Zamaneh’s website—an Amsterdam-based Persian language radio—and changed the front page to a picture of the Iranian flag with a pro-Iranian message. On February 12, 2010, the ICA posted a pro-government message on the front page of a Green website, *Jaras News*. The ICA also used DNS spoofing to redirect users away from anti-government websites (see appendix 1).[78] On February 12, 2010, Iran suspended access to Google’s Gmail to affect organization of a protest scheduled on the anniversary of the Islamic Revolution.[79] Throughout these actions, the government promoted the ICA’s activities on the media outlets *Voice and Vision*, *Kayhan*, and the Islamic Republic News Agency (IRNA).[80] Months after the 2009 elections Iran advanced their disruption of Green cyberspace activity. The ICA became more involved in denying access to social media sites through cyberspace attacks. They followed successful attacks to the logical layer of cyberspace with delivery of Iranian propaganda.

As Iranian efforts in cyberspace increased the need for more personnel to conduct cyberspace actions also increased. The government used private Iranian companies to recruit and train Iranian cyber personnel. In addition to surveillance in cyberspace, Iran began widespread offensive cyber operations against government adversaries and directed the Revolutionary Guards’ cyberwar defense section to oversee the ICA’s cyberspace operations.[81]

During the 2009 presidential election the Iranian government learned how to use cyberspace to quell mass civil disturbance and the control of cyberspace became standard practice for the government in the following years. During the 2013 presidential election the Iranian

[78] Rezvaniyeh, “Pulling the Strings of the Net.”

[79] Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election, 17.

[80] Rezvaniyeh, “Pulling the Strings of the Net.”

[81] Ibid.

government pre-planned to combat any rising the civil dissidence. Before the elections, the government tightened control on all forms of information and communication. They cut access to internet-based anti-censorship tools and slowed internet speeds until after the announcement of the election results.[82] Starting December 28, 2017, discontent and anger with the Iranian government began to rise again. The anger stemmed from Iranian citizens' expectation of improved quality of life after the United Nations lifted economic sanctions in 2015. Iran restricted access to social media apps and websites as Iranians begin to organize protests.[83] A few thousand protestors participated in six days of widespread protests in smaller cities across Iran. Protests eventually ended on January 4, 2018. The original Green Movement members did not organize this round of protests.[84] 2009 was the beginning of Iran's suppression of civil dissidence through cyberspace. They executed similar operations using cyberspace during the 2013 elections and 2018 protests to ensure that a "green-like" movements did not manifest again.

To avert Iranian government cyber surveillance during the 2018 demonstrations, protestors used an encrypted messaging app called Telegram. The government identified the rising popularity of the app and blocked access to Telegram to disrupt protesters ability to communicate.[85] In addition to blocking Telegram, the government compromised the Telegram accounts of political activists and gained access to the phone numbers and names associated with the accounts. The information gained through Telegram and information from the state-controlled phone company allowed the Iranian government to geo-locate political activists.[86] They also

[82] Sadjadpour and Anderson, Iran's Cyber Threat, 42.

[83] Phil Gast, Dakin Andone, and Kara Fox, "Here's Why the Iran Protests Are Significant," *CNN*, last modified January 2, 2018, accessed November 21, 2019, https://www.cnn.com/2017/12/30/world/iran-protests-issues/index.html.

[84] "In Response to Protests, Iran Cuts off Internet Access, Blocks Apps," *NPR.Org*, last modified January 3, 2018, accessed October 31, 2019, https://www.npr.org/2018/01/03/575252552/in-response-to-protests-iran-cuts-off-internet-access-blocks-apps.

[85] Ibid.

[86] Yeganeh Torbati and Joseph Menn, "Hackers Accessed Telegram Messaging Accounts in Iran," *Reuters*, August 2, 2016, accessed October 31, 2019, https://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM.

deployed the Revolutionary Guard to physically dissolve protests—21 people were killed and 450 were arrested at protest locations. In addition to breaking up and monitoring developing protests, the Iranian government replaced protests with pro-government rallies.[87] In 2018 the Iranian government reached a new height in their control of cyberspace. They conducted a cyberattack to gain access to protestor information; used the information to locate and arrest protestors; identify future protests; and deploy police to break up manifesting protests.

During the 2009 elections the Iranian government witnessed how cyberspace enabled the Greens' ability to organize and voice their anger towards the government. Iran quickly responded and began countering the Greens' activities in cyberspace using their control of the physical and logical layers of cyberspace. Iran used intelligence gained in cyberspace to arrest Green personnel and break up protests. During the 2013 and 2018 protests Iran evolved their operations in cyberspace by identifying protestors physical locations which enabled protestor arrests and locating future protests to break them up using police forces.

[87] Laura Smith-Spark, "UN Experts Urge Iran to Respect Rights, End Internet Crackdown," *CNN*, last modified January 5, 2018, accessed October 31, 2019, https://www.cnn.com/2018/01/05/middleeast/iran-protests-united-nations-intl/index.html.

How Cyberspace Actions during Iranian Civil Dissidence Supported Operations in other Domains

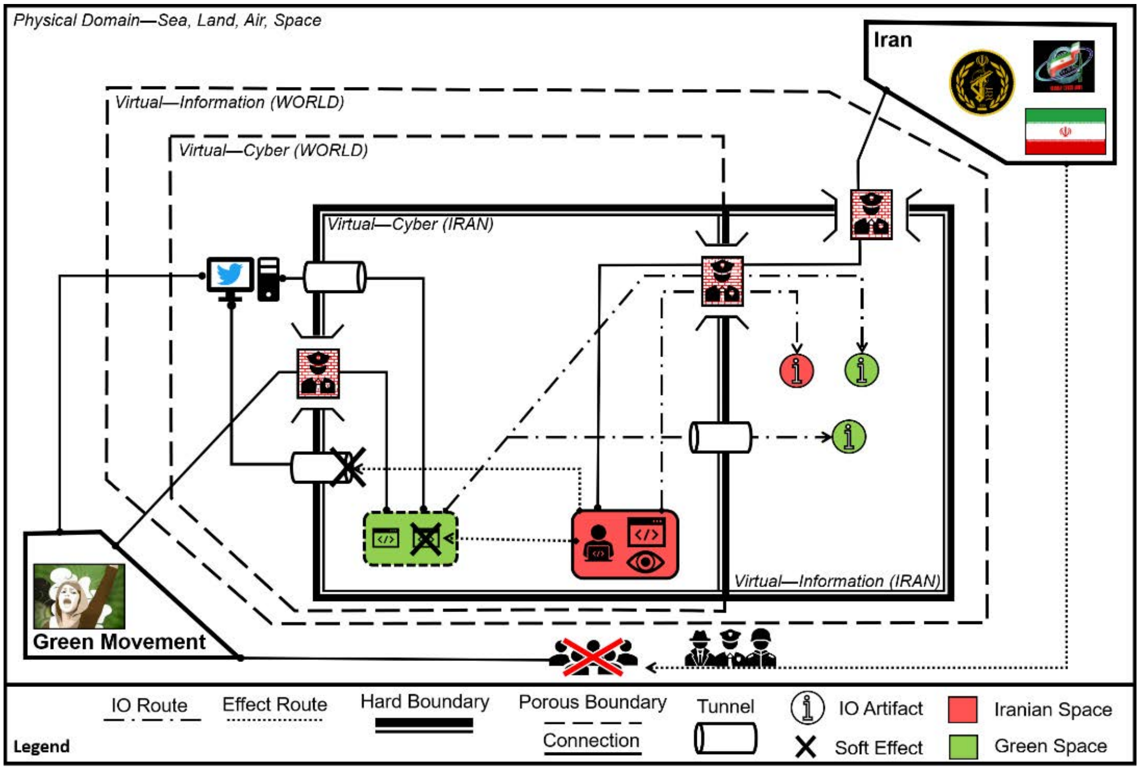


Figure 7. Cyberspace Operations and Iranian Civil Dissidence. Created by the author using images from https://en.wikipedia.org/ and https://fabiusmaximus.com distributed under CC-BY 2.0 license 2020.

Cyberspace enabled the members of the Green Movement to organize protests in the physical domain and to deliver anti-government information in the virtual-information domain. The Greens used cyberspace to obscure some of their internet activities and prevented some Greens from being located physically through cyberspace. The Greens used connectivity to cyberspace as a resource to transport their anti-government message to a worldwide audience. In addition, cyberspace was the primary method that the Greens used to organize millions of protestors to manifest collectively in the physical domain. However, the Iranian government contested the Greens in cyberspace, the virtual-information domain, and the physical domain.[88]

[88] Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election, 11-20.

The Iranian government focused their efforts in cyberspace to dissuade protestors from organizing in the physical domain, suppressing anti-government propaganda from entering the virtual-information domain, and on gaining information of Green members. Iran supported their efforts by exercising their control of the layers of cyberspace to limit access to the internet. Under President Ahmadinejad, Iran consolidated control over the virtual-cyber environment, specifically the physical and logical layers of cyberspace and the physical and informational dimensions of the information environment. The government gained control by nationalizing media, communication infrastructure, and regulating all forms of information delivery (see Figure 7).[89]

Iran used their control of the virtual-cyber domain to deny access to websites, gather intelligence, and enable execution of information operations. The intelligence Iran gained from surveilling Greens in cyberspace enabled locating and arresting Greens and anti-government journalists.[90] Iran linked successful cyberattacks to intelligence gathering operations within cyberspace which enabled locating and arresting protestors.[91] Eventually, Iran had a complete operational process that began with denying protestors ability to organize using cyberspace, dissuading protestors from attending protests, geo-locating key protest organizers, arresting protestors, deploying forces to physically break up protests, and rallying pro-government citizens to demonstrate in place of the anti-government protests.[92] An IRGC chief later said that suppressing the demonstrations required widespread arrests, massive repression, and cutting off means of mass communication, such as cellphones and the internet.[93]

[89] Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election, 17.

[90] Moghanizadeh, “The Role of Social Media in Iran’s Green Movement,” 10.

[91] Yeganeh Torbati and Joseph Menn, “Hackers Accessed Telegram Messaging Accounts in Iran,” Reuters, August 2, 2016, accessed October 31, 2019, https://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM.

[92] Laura Smith-Spark, “UN Experts Urge Iran to Respect Rights, End Internet Crackdown,” CNN, last modified January 5, 2018, accessed October 31, 2019, https://www.cnn.com/2018/01/05/middleeast/iran-protests-united-nations-intl/index.html.

[93] Sadjadpour and Anderson, *Iran’s Cyber Threat*, 11.

Israel-Hamas Conflict 2007-2019

Strategic Context of the Israel-Hamas Conflict

Israel's current sustained conflict is primarily against Palestine—specifically its militant group Hamas. Hamas, also known as the Islamic Resistance Movement or Harakat al Muqawama al Islamiyah, is both an Islamist party and a militia based in Gaza. Sheikh Ahmed Yassin, a popular cleric, founded Hamas in 1987 as the Palestinian branch of the Muslim brotherhood. Hamas originally grew out of a desire to destroy Israel and establish an independent Islamic state in Palestine.[94]

Tension between Israel and Hamas heightened when Hamas took control of the Gaza Strip in 2007. Israel declared the Hamas controlled Gaza Strip a hostile area and approved a series of sanctions that included power cuts, imports restrictions, and border closures.[95] Israel also organized a series of military operations aimed at reducing Hamas' military in the Gaza Strip. Operation Outside the Box in 2007, Operation Pillar of Defense in 2012, and Operation Protective Edge in 2014 were Israeli military operations directed at Syria and Hamas.

[94] Daniel Levin, "Iran, Hamas and Palestinian Islamic Jihad," *Wilson Center*, last modified July 9, 2018, accessed November 13, 2019, https://www.wilsoncenter.org/article/iran-hamas-and-palestinian-islamic-jihad.

[95] "Hamas - Conflict with Israel," *Encyclopedia Britannica*, last modified January 17, 2019, accessed November 13, 2019, https://www.britannica.com/topic/Hamas.

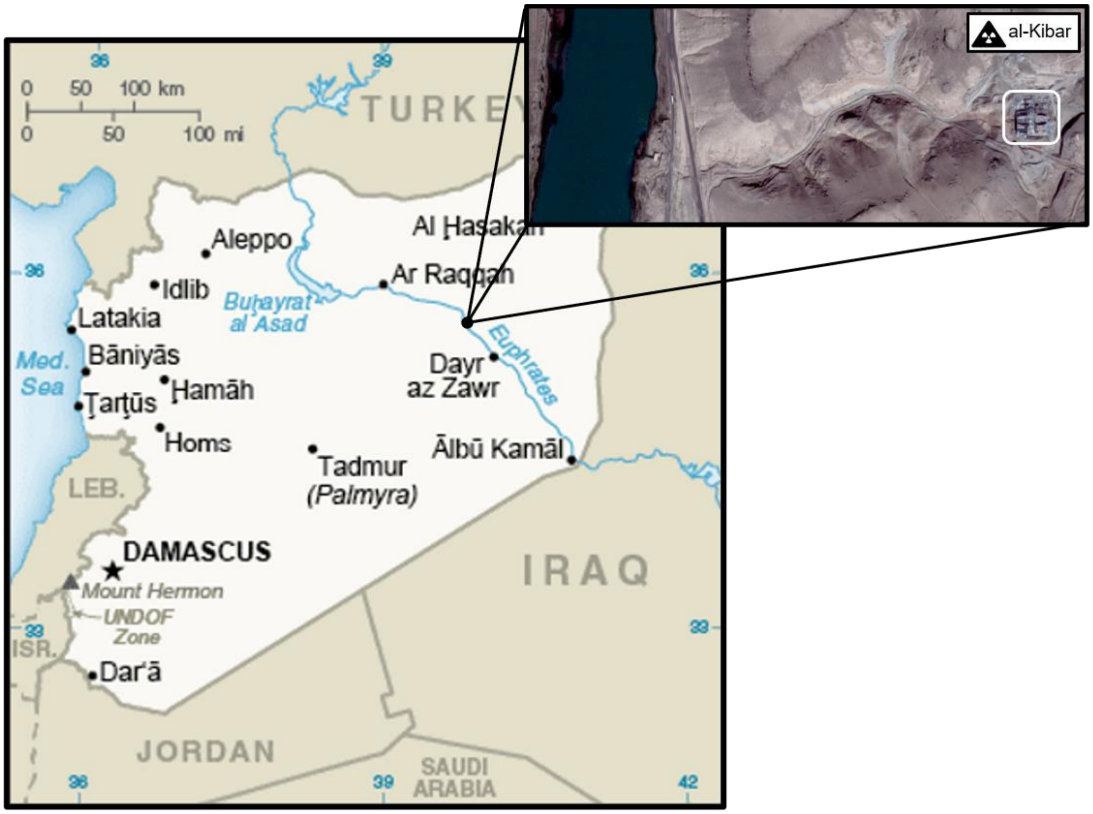


Figure 8. al-Kibar Nuclear Reactor in Syria. Created by the author. Data for base map from Google Maps and United States Central Intelligence Agency, Syria Map, (Washington, DC: Central Intelligence Agency, 1988), accessed February 17, 2020.

Operation Outside the Box was an airstrike executed on September 5, 2007 by the Israeli Air Force on a suspected Syrian nuclear reactor (see Figure 8). Israel generated the operation in 2001 when they identified that Syrian President Bashar Assad opened communications with North Korea. Israel deducted that Assad was building a relationship with North Korea to produce nuclear arms. However, Israel lacked definitive proof of the relationship before they could justifiably intervene.[96]

Israel continued to monitor Syrian and North Korean communications and in 2006 Israeli agents bugged the laptop of a Syrian official. The bug provided Israel with information which identified a Syrian nuclear facility named the al-Kibar site located in the Deir ez-Zor region of

[96] Yossi Melman, "OUTSIDE THE BOX: Israel's Strike on Syria's Nuclear Plant," *The Jerusalem Post*, last modified April 6, 2018, accessed December 5, 2019, https://www.jpost.com/Arab-Israeli-Conflict/OUTSIDE-THE-BOX-Israels-strike-on-Syrias-nuclear-plant-547870.

Syria. Israel also collected pictures of meetings between North Korean nuclear officials and Syria's energy director.[97]

In 2007 Israel learned that Iran and North Korea provided Syria with funding for nuclear projects and that Iran intended to use al-Kibar as a backup nuclear site. The intelligence gained from the laptop increased Israel's concern about the Syrian nuclear facility and in August of 2007 Israel deployed a covert team into Syria to collect soil samples from al-Kibar to confirm the presence of nuclear material. Eventually, Israel collected enough evidence to justify an attack and they conducted an airstrike which destroyed the al-Kibar facility.[98]

In 2012 Israel launched Operation Pillar of Defense as a response to increased rocket attacks from the Gaza Strip into southern Israel.[99] The operation began on November 14, 2012 when the Israeli Air Force killed the Hamas Izzadin Kassam Brigade commander Ahmed Jabari Gaza with an air strike.[100] The Israeli Air Force also destroyed over twenty underground rocket launchers in Gaza belonging to Hamas and Islamic Jihad.[101] On November 21, 2012 Egypt and the United States brokered a cease fire between Hamas and Israel.[102]

In 2014, Israeli Defense Forces (IDF) conducted Operation Brother's Keeper to locate kidnapped Israeli citizens. During the operation, Hamas increased rocket fire into southern Israel. Israel reacted by launching Operation Protective Edge on July 7, 2014. During the operation, the

[97] Noah Klieger, "A Strike in the Desert," *Ynetnews.Com*, last modified November 2, 2009, accessed December 5, 2019, https://web.archive.org/web/20121025090109/http://www.ynetnews.com/articles/0%2C7340%2CL-3799227%2C00.html.

[98] Ibid.

[99] Yaakov Lappin, "IAF Strike Kills Hamas Military Chief Jabari," *The Jerusalem Post*, last modified November 14, 2012, accessed December 5, 2019, https://www.jpost.com/Defense/IAF-strike-kills-Hamas-military-chief-Jabari.

[100] "Operation Pillar of Defense," *Israel Defense Forces*, last modified October 30, 2017, accessed December 5, 2019, https://www.idf.il/en/minisites/wars-and-operations/operation-pillar-of-defense-2012/.

[101] Lappin, "IAF Strike Kills Hamas Military Chief Jabari."

[102] Barak Ravid, "Netanyahu: Cease-Fire with Hamas Is the Right Thing for Israel," *Haaretz*, November 21, 2012, accessed December 5, 2019, https://www.haaretz.com/netanyahu-cease-fire-right-thing-1.5199481.

IDF conducted air strikes against Hamas military caches, rocket sites, and military infrastructure. The international community organized multiple cease fires but both belligerents never honored them.[103] Eventually, Egypt brokered a cease fire on August 26, 2014.[104]

The Cyberspace Actors of the Israeli-Hamas Conflict

From 2006 to 2019, IDF included different organized subdivisions focused on information and cyber warfare. The general staff's command, control, computers, communications, and intelligence (C41) branch held responsibility for defending all military communications and computer-based systems. Intelligence Unit 8200, focused on executing offensive cyber operations in conjunction with Israeli military operations and developed most of Israel's cyber weapons.[105]

Little is known about the composition or structure or Hamas' cyber forces. It is likely that Hamas leadership organized cyber forces under the Hamas intelligence service.[106] However, Hamas also organized cyber forces under the Hamas' Izz ad-Din al-Qassam Brigades when operations required actions in cyberspace to support military operations.[107] The Syria Electronic Army (SEA) and Iran's cyber forces are nation-state cyber organizations. The SEA is likely a

[103] "Operation Protective Edge," *Israel Defense Forces*, last modified October 30, 2017, accessed December 5, 2019, https://www.idf.il/en/minisites/wars-and-operations/operation-protective-edge-julyaugust-2014/.

[104] Attila Somfalvi, "Gaza Truce Deal: Crossings to Open under Israeli Supervision," *Ynetnews*, last modified August 26, 2014, accessed December 5, 2019, https://www.ynetnews.com/articles/0,7340,L-4564456,00.html.

[105] Matthew S. Cohen, Charles D. Freilich, and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17, no. 3 (August 1, 2016): 6.

[106] Avi Issacharoff, "Hamas Establishes New Intelligence Service in Gaza," *Haaretz*, January 8, 2007, accessed December 10, 2019, https://www.haaretz.com/1.4957530.

[107] "Hamas' Izz al-Din al-Qassam Brigades," *Australian National Security*, accessed December 10, 2019, https://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/HamassIzzal-Dinal-QassamBrigades.aspx.

loose collective of hackers that take direction and resourcing from the Syrian government while still maintaining anonymity.[108]

Anonymous is a worldwide loose collective of people with a focus on social activism. Anonymous has no leadership and organizes around popular events that the collective deems worthy of Anonymous' efforts. They coordinate their efforts using mediated web-based chat systems. Many members of Anonymous are digitally literate with skilled computer experts joining during high profile events. Anonymous numbers surge during high profile events that are socially controversial. Anonymous ramps down their actions in cyberspace upon meeting their objective or when the high-profile event ends.[109]

The Cyberspace Actions during the Israeli-Hamas Conflict

The first development of Operation Outside the Box began in December 2006 when a Syrian official visited London and Israeli Mossad agents covertly loaded spyware on the official's laptop. The spyware gathered information that led Mossad to believe that the Syrians were constructing a nuclear facility in al-Kibar with the purpose of developing nuclear capabilities.[110]

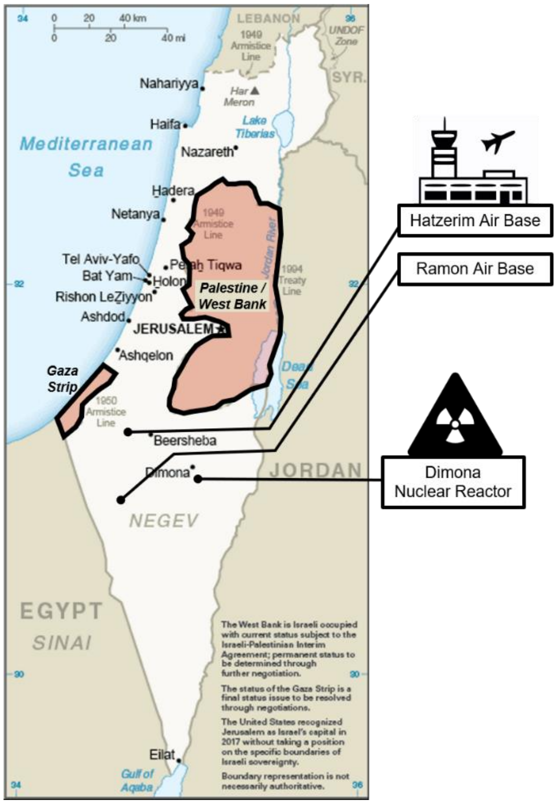
Using a Kidon team, Mossad gained access to the Syrian's laptop by braking into the Syrian official's hotel room. Once they had physical access to the laptop, a Mossad computer expert collected data from the laptop and installed software that allowed remote activity monitoring. From the laptop, Israel gained photographs and blueprints for a plutonium reactor at al-Kibar near Deir el-Zor, a remote desert town eighty miles from Syria's border with Iraq (see

[108] Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," *OpenNet Initiative*, accessed December 10, 2019, https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army.

[109] Gabriella Coleman, "Anonymous: From the Lulz to Collective Action," *The New Everyday: A MediaCommons Project*, last modified April 6, 2011, accessed January 20, 2020, https://web.archive.org/web/20130517212228/http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action.

[110] Klieger, "A Strike in the Desert."

Figure 8).[111] The physical and logical layers of cyberspace enabled Israel to remotely collect information from the Syrian's laptop. The stream of information eventually supported Israel's decision to attack the nuclear site in the physical domain.



The West Bank is Israeli occupied with current status subject to the Israeli-Palestinian Interim Agreement; permanent status to be determined through further negotiation.

The status of the Gaza Strip is a final status issue to be resolved through negotiations.

The United States recognized Jerusalem as Israel's capital in 2017 without taking a position on the specific boundaries of Israeli sovereignty.

Boundary representation is not necessarily authoritative.

Figure 9. Israel and Palestine. Created by the author. Data for base map from United States Central Intelligence Agency, Israel Map, (Washington, DC: Central Intelligence Agency, 1988), accessed February 17, 2020. Created using image from https://en.wikipedia.org/wiki/File:Airport_symbol.svg, 2020, distributed under CC-BY 2.0 license 2020.

The intelligence gained from the laptop helped Israel develop a strike package to destroy the al-Kibar nuclear facility. On September 5, 2007, Israel began Operation Outside the Box with eight F-15s and F-16s departing from the Hatzerim and Ramon air bases in the southern Israel (see Figure 9). The fighter jets struck the Syrian nuclear facility on the morning of September 6,

[111] Duncan Gardham, "Mossad Carries out Daring London Raid on Syrian Official," *The Telegraph*, last modified May 15, 2011, accessed December 5, 2019, https://web.archive.org/web/20110518025425/http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8514919/Mossad-carries-out-daring-London-raid-on-Syrian-official.html.

2007.[112] To support the airstrike, Israel utilized the BAE Systems Suter airborne network attack system to manipulate Syrian surface-to-air missile (SAM) systems.[113] The Suter technology allowed Israel to penetrate into the Syrian SAM communication network and manipulate the data in the SAM system.[114] The air delivered cyberattack allowed Israeli air force fighter jets to fly into Syrian airspace undetected. Israel did not completely disable the Syrian air defenses, but instead manipulated system data to hide the presence of the Israeli fighters. Israel conducted an attack in the virtual-cyber domain to affect a system in the physical domain which enabled Israeli to destroy the al-Kibar nuclear facility.[115]

Before Operation Pillar of Defense began, Israeli military forces identified and intercepted an unmanned aerial vehicle (UAV) that entered Israeli airspace on October 6, 2012. The Israeli military assessed that the UAV was an Iranian made helicopter that departed from Lebanon flying a reconnaissance mission. Before Israel destroyed the UAV, an Israeli cyber unit gained control of the drone.[116] While Israeli cyber forces immobilized the UAV an Israeli F-16 fighter jet shot down the UAV.[117] Using cyberspace, Israel controlled enemy reconnaissance aircraft to enable its destruction by air forces and disabled SAMS systems to allow air forces to penetrate enemy air defenses. Israel coordinated both actions to ensure that effects in the virtual-cyber domain supported operations in the physical domain.

[112] Melman, "OUTSIDE THE BOX."

[113] David A. Fulghum and Douglas Barrie, "Israel Used Electronic Attack in Air Strike against Syrian Mystery Target," *ABC News*, last modified October 8, 2007, accessed October 8, 2019, https://web.archive.org/web/20140207061332/http://abcnews.go.com/Technology/story?id=3702807.

[114] John Leyden, "Israel Suspected of 'hacking' Syrian Air Defences," *The Register*, October 4, 2007, accessed August 15, 2019, https://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

[115] Matthew S. Cohen, Charles D. Freilich, and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17, no. 3 (August 1, 2016): 9.

[116] Daniel Dieterle, "Did Israel Hack Unmanned Helicopter That Entered Their Airspace?," *CYBER ARMS - Computer Security*, October 7, 2012, accessed August 15, 2019, https://cyberarms.wordpress.com/2012/10/07/did-israel-hack-unmanned-helicopter-that-entered-its-airspace/.

[117] David Cenciotti, "Israeli Air Force Releases Video of Mysterious Drone Shot down by an F-16 over Israeli Airspace," *The Aviationist*, October 6, 2012, accessed November 10, 2019, https://theaviationist.com/2012/10/06/iaf-uav-shotdown/.

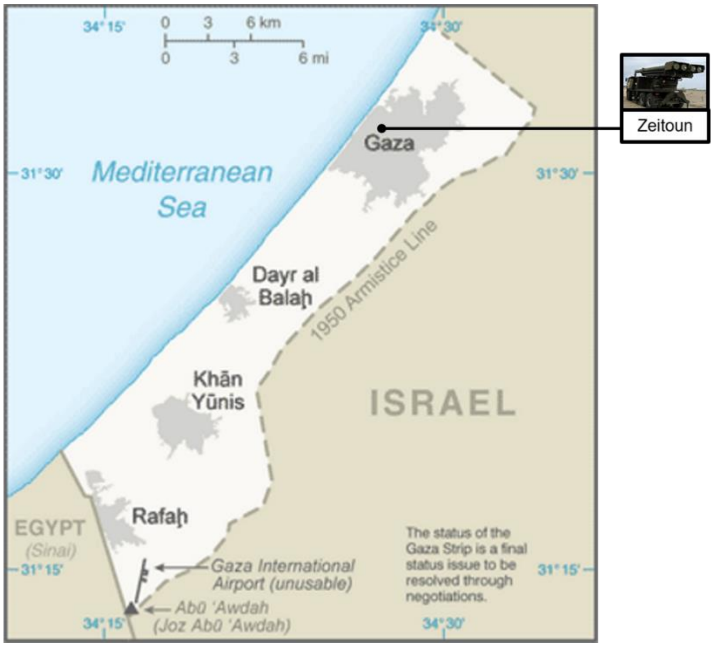


Figure 10. Hamas Rocket Launcher Location in the Gaza Strip. Created by the author. Data for base map from United States Central Intelligence Agency, Gaza Strip, (Washington, DC: Central Intelligence Agency, 1988), accessed February 17, 2020. Created using image from https://en.wikipedia.org/wiki/Fajr-5, 2020, distributed under CC-BY 2.0 license 2020.

During Operation Pillar of Defense, Israeli defense forces aggressively liveblogged, tweeted, and followed military operations with posts on social media websites boasting their success (see appendix 1). Israel also used official Facebook, Flickr, and Twitter accounts to disseminate information to a worldwide audience. For example, Israel spotted a Fajr-5 rocket launcher in Zeitoun, Gaza and uploaded surveillance footage and tweeted a map of the location of the launcher (see Figure 10).[118] One of the most viewed posts concerned the killing of the Hamas military leader, Ahmed al-Jabari.[119] IDF posted a video of the strike that killed Ahmed al-Jabari to its blog and a list of Jabari's offenses including his connection to kidnapping Israeli soldiers.[120] The post included a warning to all of Jabari's comrades: "We recommend that no Hamas

[118] Noah Shachtman, "Israel Kills Hamas Leader, Instantly Posts It to YouTube," *Wired*, November 14, 2012, accessed December 5, 2019, https://www.wired.com/2012/11/idf-hamas-youtube/.

[119] Robert Beckhusen and Noah Shachtman, "Hamas Shoots Rockets at Tel Aviv, Tweeting Every Barrage," *Wired*, November 15, 2012, accessed December 5, 2019, https://www.wired.com/2012/11/gaza-social-media-war/.

[120] Shachtman, "Israel Kills Hamas Leader, Instantly Posts It to YouTube."

operatives, whether low level or senior leaders, show their faces above ground in the days ahead."[121]

To enable their information operations the Israeli defense forces applied the hashtag *#IsraelUnderFire* to their social media posts to draw viewers to their online content. IDF contested Hamas over control of *#Gaza* on Twitter.[122] The hashtag struggle led Palestinians to create *#GazaUnderAttack* to draw viewers away from the content tagged with *#Gaza*.[123] Hamas also used social media websites to publicize their rocket and mortar attacks against Israel. Hamas also used *#FreeGaza*, *#Resistance*, and *#ShaleStones* to tag its social media posts and draw users to its content.[124] Israel and Hamas both used the virtual-cyber domain to support operations in the virtual-information domain. Both parties used the information dimension, logical, and cyber-persona layer of cyberspace to deliver their messages to a worldwide audience.

Israeli defense forces planned military information disclosure using social media with the intent to control the global perception of their military actions.[125] IDF established an interactive media branch two months before Operation Pillar of Defense began. The IDF staffed the branch with thirty soldiers trained in writing and graphic-design skills.[126] The Israeli military's media office Twitter account gained more than 50,000 followers twenty-four hours after Operation Pillar of Defense began. The IDF relayed near real-time information through its official public channels before it released information to public reporters.[127]

[121] Ibid.

[122] Beckhusen and Shachtman, "Hamas Shoots Rockets at Tel Aviv, Tweeting Every Barrage."

[123] Lauren E. Bohn, "Israel and Hamas Battle on Social Media as Well," *Boston.Com*, last modified November 15, 2012, accessed December 5, 2019, https://web.archive.org/web/20121116194700/http://www.boston.com/news/world/middle-east/2012/11/15/israel-and-hamas-battle-social-media-well/O2zOPWK7t3FG4QeMBhxVpL/story.html.

[124] Beckhusen and Shachtman, "Hamas Shoots Rockets at Tel Aviv, Tweeting Every Barrage."

[125] Ibid.

[126] Bohn, "Israel and Hamas Battle on Social Media as Well."

[127] Beckhusen and Shachtman, "Hamas Shoots Rockets at Tel Aviv, Tweeting Every Barrage."

During Operation Pillar of Defense Israel identified the importance of controlling and projecting their narrative in the virtual-information domain. An Israeli military spokeswoman stated that an "additional war zone" developed on the internet between Hamas an Israel during Operation Pillar of Defense.[128] To keep pace with physical domain operations Israel used the virtual-cyber domain to quickly conduct operations in the virtual-information domain.

During Operation Pillar of Defense Israel faced millions of cyberattacks originating from IP addresses in Europe and the United States.[129] Israel assessed that the attacks intended to disrupt Israeli websites and networks using a denial of service attack (see appendix 1).[130] Anonymous also took part in cyber efforts against Israel and attacked over seven hundred Israeli websites during Operation Pillar of Defense under the campaign hashtag *#OpIsrael*. Anonymous took down the Israeli president's official website and the blog of the Israeli Defense Forces, *www.idfblog.com*.[131] Anonymous attacked the websites of the Israeli Foreign Ministry, Kadima party, Bank of Jerusalem, and Tel Aviv municipality. The Tel Aviv municipal website provided residents with directions to bomb shelters. The attacks left the websites blank or posted pro-Palestinian propaganda.[132] After a successful cyberattack Anonymous posted on Twitter using the hashtags *#TANGO #DOWN* and posting the message, "This attack is in response to the injustice against the Palestinian people."[133] Anonymous also helped the Palestinians by using Twitter to

[128] Bohn, "Israel and Hamas Battle on Social Media as Well."

[129] Daniel Cohen and Danielle Levin, "Cyber Infiltration During Operation Protective Edge," *Forbes*, August 12, 2014, accessed August 19, 2019, https://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/.

[130] David Shamah, "Hackers Threaten 'Israhell' Cyber-Attack over Gaza," *The Times of Israel*, July 9, 2014, accessed August 19, 2019, http://www.timesofisrael.com/hackers-threaten-israhell-cyber-attack-over-gaza/.

[131] "Israel Faces 44 Million Attacks on Websites in Response to Gaza Offensive," *RT International*, 44, last modified November 18, 2012, accessed December 5, 2019, https://www.rt.com/news/israel-cyber-hackers-gaza-000/.

[132] "Anonymous Hack Hundreds of Israeli Websites, Delete Foreign Ministry Database in Support of Gaza," *RT International*, last modified November 17, 2012, accessed December 5, 2019, https://www.rt.com/news/anonymous-gaza-israel-website-938/.

[133] "Israel Faces 44 Million Attacks on Websites in Response to Gaza Offensive."

provide information to Gaza residents which contained instructions on how to evade Israeli cyber surveillance, how to reconnect to the internet during a shutdown, and first aid information.[134]

Operation Pillar of Defense thrusted Israel into information and cyber warfare. Cyberspace became the battleground where Israel and its adversaries attempted to influence each other and the world. Israel received attacks in the virtual-cyber domain to its logical network layer of cyberspace which affected Israel's ability to conduct operations in the virtual-information domain.

The Israeli-Hamas conflict continued during Operation Protective Edge. Before military operations began, both sides prepared for a repeat of the cyberwar experienced during Operation Pillar of Defense. On July 25, 2014, Anonymous implored hackers to fight against Israel.[135] They created and used the hashtags *#OpIsrael* and *#OpSaveGaza* to coordinate cyber-protests of Israeli.[136]

Israel planned to receive cyberattacks during Operation Protective Edge and prepared a cyber defensive strategy that included the use of advanced defensive measures. The Israeli Security Agency (ISA), coordinated with Israeli companies, the Israeli Ministry of Communications, and Israeli media to pre-organize measures against cyberattacks. Israeli Defense Forces created a private communications network between the military intelligence and non-military Israeli cyber companies to assist with detecting and neutralizing cyber threats. Israel also blocked all foreign IPs from its networks before Operation Protective Edge began.[137] Both belligerents began preparing for conflict in the virtual-cyber and information domain. Anonymous used the virtual-cyber domain to organize forces to conduct operations in the virtual-

[134] "Anonymous Hack Hundreds of Israeli Websites, Delete Foreign Ministry Database in Support of Gaza."

[135] Cohen and Levin, "Cyber Infiltration During Operation Protective Edge."

[136] Anat Kurz and Shlomo Brom, eds., *The Lessons of Operation Protective Edge* (Tel Aviv: Institute for National Security Studies, 2014), 60, accessed December 5, 2019, https://www.inss.org.il/publication/the-lessons-of-operation-protective-edge/.

[137] Ibid., 61.

information domain. Israel opened lines of communication in the logical network layer of cyberspace to enable counter-actions to enemy attacks in the virtual-cyber domain.

Hackers attacked Israeli government websites and media outlets using denial of service attacks and domain name system (DNS) attacks which exposed the personal data of Israeli citizens (see appendix 1).[138] Anti-Israeli hackers used *#OpSaveGaza* to rally pro-Palestinian hackers for the execution of a DDoS against Israel—Israel detected a million attacks per day during the attack. Attackers exploited successful website attacks by replacing website content with anti-Israeli messages.[139] Cyberattacks against Israel breached over one-thousand Israeli websites, diverted Israeli internet traffic, blocked foreign IPs, and publicly exposed the IP and email addresses of Israeli ministry workers. However, most Israeli websites recovered within hours after the attacks.[140] Some of the attacks assessed by Israeli C4I were zero-day attacks imbedded in malware specifically designed to target Israeli network defenses (see appendix 1).[141] Israel assessed that seventy percent of cyberattacks originated from Qatar.[142]

Hacker groups from Hezbollah, Hamas, Palestine, and Iran also conducted cyberattacks against Israel during Operation Protective Edge. Israel noticed that cyberattacks were more sophisticated compared to those during Operation Pillar of Defense.[143] Israel assessed that Iran and the Syrian Electronic Army participated or supported Hamas in cyberattacks during Operation Protective Edge. Cyberattacks on Israel caused the collapse of over one-thousand non-critical Israeli websites, defaced Israeli websites, and exposed personal information and login

[138] Cohen and Levin, "Cyber Infiltration During Operation Protective Edge."

[139] Shamah, "Hackers Threaten 'Israhell' Cyber-Attack over Gaza."

[140] Cohen and Levin, "Cyber Infiltration During Operation Protective Edge."

[141] David Shamah, "Iran, Hamas Conduct Cyber-Attacks against Israel," *The Times of Israel*, accessed August 13, 2015, http://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

[142] Cohen and Levin, "Cyber Infiltration During Operation Protective Edge."

[143] Shamah, "Iran, Hamas Conduct Cyber-Attacks against Israel."

credentials of Israelis.[144] Adversaries posted false messages on the Israeli defense forces official Twitter account stating the Dimona nuclear reactor was hit by a rocket and was leaking radiation.[145] Hamas also sent mass text messages with misinformation to Israelis claiming to be either from the Israeli Security Agency, the Israeli news service Haaretz, or Hamas. Hamas also attacked private television satellite signals and placed pro-Hamas propaganda on Israeli television channels.[146] Hamas and Israel leveraged the virtual-cyber domain to execute operations in the virtual-information domain and deny their adversaries the same. Both sides used the logical and cyber-persona layers of cyberspace to counter and disrupt their adversary's information operations.

The Israeli Defense Forces provided near real-time information concerning military operations by posting multiple operational updates each day to its Twitter account. Information included alerts of incoming rocket fire into Israel and the interception of Hamas rockets by Israel's Iron Dome anti-rocket system. Hamas also provided operational updates using an English language Twitter account.[147] The IDF also dropped leaflets, made personalized phone calls, and sent text messages to civilians in the Gaza Strip before they conducted a strike into Gaza to minimize civilian casualties.[148] When Israeli ground operations against Hamas concluded cyberattacks from both sides significantly declined.[149] Israeli activities in cyberspace and the virtual-information domain benefited from control of information outlets, coordination between agencies, and pre-planning. As a result, Israel combatted enemy information operations,

[144] Kurz and Brom, The Lessons of Operation Protective Edge, 60.

[145] Gabi Siboni and Sami Kronenfeld, "The Iranian Cyber Offensive during Operation Protective Edge," INSS Insight, no. 598 (August 26, 2014): 1.

[146] Kurz and Brom, The Lessons of Operation Protective Edge, 60.

[147] Bohn, "Israel and Hamas Battle on Social Media as Well."

[148] Sarah Fowler, "Hamas and Israel Step up Cyber Battle for Hearts and Minds," BBC News, July 15, 2014, sec. Middle East, accessed December 5, 2019, https://www.bbc.com/news/world-middle-east-28292908.

[149] Kurz and Brom, The Lessons of Operation Protective Edge, 59.

cyberattacks, and opened avenues in the virtual-cyber domain to conduct information operations against Hamas.

On May 5, 2019 Israel foiled a Hamas cyberattack against Israel.[150] The cyberattacks came in conjunction with Hamas rocket and mortar attacks into Israel. After detecting the cyberattack, the IDF identified the physical location of the Hamas cyber-attackers.[151] After locating the attackers, the IDF executed an airstrike to destroy the building where the cyberattack originated.[152] After the air strike concluded, Israel posted a Twitter message with a picture of the destroyed building and a message "HamasCyberHQ.exe has been removed."[153] Israel assessed that the Hamas cyber unit was located in the headquarters of the Hamas military intelligence.[154] This event is the apogee of multi-domain operations. Israel countered Hamas attacks in the virtual-cyber domain, provided information to enable an air strike in the physical domain, and then exploited success with a message in the virtual-information domain—all events occurred within the same day.

[150] Israel Defense Forces, "CLEARED FOR RELEASE: We Thwarted an Attempted Hamas Cyber Offensive against Israeli Targets. Following Our Successful Cyber Defensive Operation, We Targeted a Building Where the Hamas Cyber Operatives Work. HamasCyberHQ.Exe Has Been Removed.Pic.Twitter.Com/AhgKjiOqS7," Tweet, *@IDF*, May 5, 2019, accessed August 13, 2019, https://twitter.com/IDF/status/1125066395010699264.

[151] Judah Ari Gross, "IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle," *The Times of Israel*, May 5, 2019, accessed August 13, 2019, https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/.

[152] Elias Groll, *The Future Is Here, and It Features Hackers Getting Bombed* (The Foreign Policy Group, May 6, 2019), accessed August 13, 2019, https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

[153] Lily Hay Newman, "What Israel's Strike on Hamas Hackers Means for Cyberwar," *Wired*, May 6, 2019, accessed August 15, 2019, https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

[154] Mohit Kumar, "Israel Neutralizes Cyber Attack by Blowing up a Building with Hackers," *The Hacker News*, last modified May 6, 2019, accessed September 25, 2019, https://thehackernews.com/2019/05/israel-hamas-hacker-airstrikes.html.

How the Cyberspace Actions during the Israel-Hamas Conflict Supported Operations in other Domains

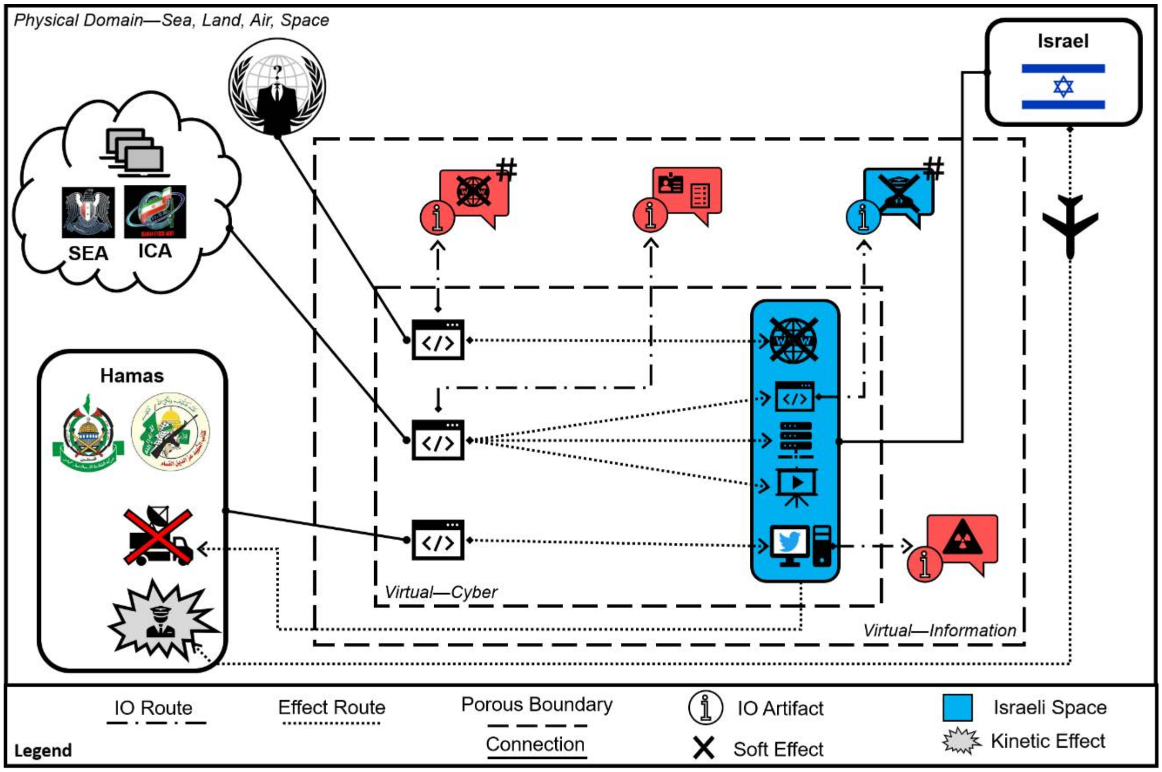


Figure 11. Cyberspace Operations During the Israeli-Hamas Conflict. Created by the author using images from https://en.wikipedia.org/, https://fabiusmaximus.com, and https://www.mtctutorials.com, distributed under CC-BY 2.0 license.

Intelligence gained from the virtual-cyber domain supported Israeli's kinetic strikes of targets in the physical domain. Using cyberspace as an avenue to deliver information, Israel was able to build targets quickly and over a long term. During Operation Outside the Box Israel used cyberspace to collect information from a laptop over a long period until enough information supported a strike in the physical domain. In 2019, Israel quickly detected a cyberattack and provided information to rapidly execute a strike in the physical domain (see Figure 11).[155]

Israel also used the virtual-cyber domain to deliver effects to the physical domain. Israel used cyberspace to manipulate Syrian radar feeds allowing Israeli air fighters to pass undetected

[155] Cohen, Freilich, and Siboni, "Israel and Cyberspace," 9.

through Syrian air defenses.[156] Israel used a cyberspace attack to control an Iranian drone enabling fighter jets to destroy the drone.[157]

Israel, Hamas, and Anonymous used the virtual-cyber domain to conduct operations in the virtual-information domain and deny their adversaries the same. All sides contested for control of outlets within virtual-cyber domain to gain access to avenues to conduct information operations. Hamas and Israel used events in the physical domain as material to develop messages to deliver during information operations. The execution of information operations and delivery of messages was enabled by the logical network and cyber-persona layers of cyberspace. Both sides used overt Twitter accounts and websites to relay messages to multiple audiences. Israel used cyberspace defense to defend its logical network and cyber-persona positions allowing retention of avenues to conduct operations in the virtual-information domain.[158] Hamas and Anonymous used cyberspace to rally individuals to conduct mass cyberattacks on Israeli positions in the logical and cyber-persona layers of cyberspace. The success of cyberattacks provided Hamas access to avenues to execute information operations against Israeli citizens. All parties used their positions in the cyber-persona layer to contest control of influential hashtags to gain wider avenues to conduct operations in the virtual-information domain.[159]

[156] Ibid.

[157] David Cenciotti, "Israeli Air Force Releases Video of Mysterious Drone Shot down by an F-16 over Israeli Airspace," *The Aviationist*, October 6, 2012, accessed November 10, 2019, https://theaviationist.com/2012/10/06/iaf-uav-shotdown/.

[158] Daniel Cohen and Danielle Levin, "Cyber Infiltration During Operation Protective Edge," *Forbes*, August 12, 2014, accessed August 19, 2019, https://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/.

[159] Anat Kurz and Shlomo Brom, eds., *The Lessons of Operation Protective Edge* (Tel Aviv: Institute for National Security Studies, 2014), 60, accessed October 19, 2019, https://www.inss.org.il/publication/the-lessons-of-operation-protective-edge/.

Analysis

Cyberspace operations that support the operational level of war synchronize with physical domain and virtual-information operations. Each case study has examples of cyberspace operations that preceded or followed an action in another domain. During Operation Allied Force, NATO bombed Serbian military targets after neutralizing Serbian air defenses through cyberspace. To suppress the Green Movement, Iran identified Greens in cyberspace and delivered influential messages to them or physically located and arrested them. The Iranian Cyber Army propagated pro-government messages after completing a cyberattack on opposition websites. During the Israel-Hamas conflict, the Israeli Defense Forces used cyberspace to physically locate a Hamas cyber unit and then conducted an air strikes on the location. Following the strike, Israel posted messages on their official Twitter account touting the success and warning against future attacks.

Cyberspace operations that support the operational level of war gather intelligence on adversaries to support future operations in other domains. During Operation Matrix, US Central Intelligence Agency surveilled Serbian leaders through the virtual-cyber domain which supporting building a link diagram and helped information operations target Slobodan Milošević. Iran used their control of the physical and logical layers of cyberspace to surveille Greens and then provided information to target Greens during information and physical domain operations. Israel bugged a Syrian official's laptop and collected information that eventually supported the targeting and destruction of a Syrian al-Kibar nuclear reactor. Cyberspace connects to all domains and people interact with all layers of cyberspace. As a result, opportunities exist to collect information from human interactions with the layers of cyberspace.

Cyberspace operations that support the operational level of war deny or disrupt delivery avenues within the virtual-information domain. During Operation Allied Force, the Modern Black Hand attacked NATO's websites and networks to affect their use as delivery avenues for information operations. Iran used their control of the cyberspace layers to deny the Iranian civilians use of avenues to disseminate anti-government information. Using the logical and cyber-persona layers of cyberspace, Israel and Hamas struggled over control of popular hashtags to disrupt each other's ability to influence a worldwide audience. Successful disruption of delivery avenues in cyberspace follows with delivery of messages that support the attacker's cause.

Cyberspace operations that support the operational level of war affect entities residing in the physical domain. During Operation Allied Force, NATO used the virtual-cyber domain as an avenue to manipulate Serbian air defenses in the physical domain. Iran used their control of the virtual-cyber domain to message Iranian civilians to deter them from attending protests. During Operation Outside the Box, Israel used the virtual-cyber domain to obscure Syrian air defenses and enable an air strike on a Syrian nuclear reactor.

Conclusion

After the defeat of the Prussian Army at the battle of Jena-Auerstädt, Clausewitz identified an urgent need to modernize the Prussian Army. To understand the change in warfare Clausewitz studied battles and applied the results to modernize the Prussian Army. The US Army faces a similar problem when trying to plan and execute operations to support activities at the operational level of war. It is not enough for a military to use existing principles when operating in a new domain. Observation, experimentation, and testing help derive and confirm existing and new principles for planning and execution of military operations. The problem this monograph addresses is how to integrate cyberspace operations to support other domain operations at the operational level of war.

Through analysis of Operation Allied Force, Iranian suppression of civil dissidence, and the Israel-Hamas conflict, this monograph found that cyberspace operations supported other domain operations by gathering intelligence on adversaries to support future operations; denying or disrupting delivery avenues within the virtual-information domain; and affecting entities residing in the physical domain.

Though the results of the analysis may seem obvious, this study aligned principles to factual evidence from actions on the battlefield. Moreover, the exercise of research and analysis spawned a framework for analyzing operational level cyberspace activities. The military practitioner can conduct the same analysis by considering the strategic context, cyberspace actors, cyberspace actions, and how cyberspace actions supported other domains.

The results of analysis are useful for planning cyber operations at the operational level. In addition, the framework of analysis is useful to commanders and planners at the tactical and operational level because it provides a modest method to study past cyber operations. Finally, the derived points link to tactical cyberspace actions that the planner and commander can consider for employment of tactical cyber operations.

Just as Clausewitz and US Army understood the changing conduct of war, so to must the modern military observe the changing landscape to modernize their tactics and operations. Nations, individuals, and groups are executing operations in cyberspace and the US Army should take note of their successes and failures. Study of cyberspace operations and how they support other domain operations helps prepare the US Army for future employment of cyber forces. If the US Army ignores the cyberspace events unfolding around them then they face a possible future akin to Prussia's fate at the battle of Jena-Auerstädt.

Appendix 1: Definitions

Black hat hackers—A black hat hacker is a person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons**.** Black hat hackers can inflict major damage on both individual computer users and large organizations by stealing personal financial information, compromising the security of major systems, or shutting down or altering the function of websites and networks.[160]

Blue cyberspace—denotes areas in cyberspace protected by the United States, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare, on order, and when requested by other authorities, to defend or secure other United States Government (USG) or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the United States and Partnered Nations.[161]

Denial of Service Attack—occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts, or other services that rely on the affected computer or network. A denial-of-service (DoS) condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.[162]

Deny action—To prevent access to, operation of, or availability of a target function by a specified level for a specified time.[163]

Degrade action—To deny access to, or operation of, a target to a level represented as a percentage of capacity.[164]

Destroy action—To deny access completely and irreparably to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted.[165]

Disrupt action—To completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent.[166]

[160] "What Is a Black Hat Hacker? - Definition from Techopedia," *Techopedia.Com*, accessed February 18, 2020, https://www.techopedia.com/definition/26342/black-hat-hacker.

[161] US Department of Defense, *Joint Publication (JP) 3-12*, I–5.

[162] CISA, "Understanding Denial-of-Service Attacks," *Security Tip (ST04-015)*, last modified November 20, 2019, accessed March 18, 2020, https://www.us-cert.gov/ncas/tips/ST04-015.

[163] US Department of Defense, *Joint Publication (JP) 3-12*, II–7.

[164] Ibid.

[165] Ibid.

[166] Ibid.

Domain name service cache spoofing—is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones. A DNS cache can become poisoned if it contains an incorrect entry. There is no real way of determining whether DNS responses you receive are actually legitimate or whether they have been manipulated.[167]

Grey hat hacker—performs illegal hacking activities to show off their skills, rather than to achieve personal gain.[168]

Grey cyberspace—is all cyberspace that does not meet the description of either "blue" or "red." cyberspace[169]

Hacker—any individual or group that circumvents security to access unauthorized data. Most hackers are highly skilled computer programmers that locate security gaps and access secure systems via unique computing and analytical skills.[170]

Hacktivist—someone who uses hacking to bring about political and social change.[171]

Hashtag—is a number symbol (#) used to label keywords in a tweet. The name "hashtag" was coined by Twitter and combines the word "hash" and "tag," since it is used to tag certain words. Hashtags are used to categorize tweets, since all tweets with the same hashtag are related. Therefore, searching for hashtags is a good way to monitor hot topics or trends. A hashtag can be any word or combination or words and can also include numbers.[172]

Internet Protocol—A set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place.[173]

Liveblog— a blog containing entries about an event that are written and posted while the event is taking place.[174]

Manipulate—a form of cyberspace attack, controls or changes information, information systems, and/or networks in gray or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. It uses an

[167] Chris Hoffman, "What Is DNS Cache Poisoning?," *How-To Geek*, accessed February 24, 2020, https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/.

[168] "What Is a Hacker? - Definition from Techopedia," *Techopedia.Com*, accessed February 18, 2020, https://www.techopedia.com/definition/3805/hacker.

[169] US Department of Defense, *Joint Publication (JP) 3-12*, I–5.

[170] "What Is a Hacker?"

[171] "What Is a Hacktivist?," *United States Cybersecurity Magazine*, last modified December 11, 2018, accessed February 18, 2020, https://www.uscybersecurity.net/hacktivist/.

[172] "Hashtag Definition," accessed February 18, 2020, https://techterms.com/definition/hashtag.

[173] "What Is the Internet Protocol?," *Cloudflare*, accessed February 18, 2020, https://www.cloudflare.com/learning/ddos/glossary/internet-protocol/.

[174] "Definition of Liveblog," *Www.Dictionary.Com*, accessed February 18, 2020, https://www.dictionary.com/browse/liveblog.

adversary’s information resources for friendly purposes, to create denial effects not immediately apparent in cyberspace. The targeted network may appear to operate normally until secondary or tertiary effects, including physical effects, reveal evidence of the logical first-order effect.[175]

Nation-State Threat—involve traditional adversaries; enemies; and potentially, in the case of espionage, even traditional allies. Nation-states may conduct operations directly or may outsource them to third parties, including front companies, patriotic hackers, or other surrogates, to achieve their objectives.[176]

Network layer filters—operate at the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set defined by the administrator or applied by default. Modern firewalls can filter traffic based on many packet attributes such as source IP address, source port, destination IP address or port, or destination service like WWW or FTP.[177]

Non-State Threats—are formal and informal organizations not bound by national borders, including legitimate nongovernmental organizations (NGOs), and illegitimate organizations such as criminal organizations, violent extremist organizations, or other enemies and adversaries. Non-state threats use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, undermine confidence in governments, conduct espionage, and conduct direct terrorist actions within cyberspace.[178]

Ping-saturation attack, ICMP (ping) Flood—overwhelms the target resource with ICMP Echo Request (ping) packets, sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim’s servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.[179]

Ping bombardment—one computer automatically and repeatedly communicates with another using the Internet Control Message Protocol.[180]

Proxy Server—a computer system or router that functions as a relay between client and server. It helps prevent an attacker from invading a private network.[181]

URL redirection—A URL redirect is a webserver function that sends a user from one URL to another. Redirects commonly take the form of an automated redirect that uses one of a series of

[175] US Department of Defense, *Joint Publication (JP) 3-12*, II–7.

[176] Ibid., I–11.

[177] “Common IP Filtering Techniques,” accessed February 18, 2020, https://www.apnic.net/manage-ip/apnic-services/registration-services/resource-quality-assurance/filtering/.

[178] US Department of Defense, *Joint Publication (JP) 3-12*, I–11.

[179] “DDoS Attack Types & Mitigation Methods,” *Learning Center*, n.d., accessed February 18, 2020, https://www.imperva.com/learn/application-security/ddos-attacks/.

[180] “News Briefs,” *InfoWorld*, April 5, 1999, 5.

[181] “Definition of Proxy Server,” *PCMAG*, accessed February 18, 2020, https://www.pcmag.com/encyclopedia/term/proxy-server.

status codes defined within the HTTP protocol.[182]

Red cyberspace—refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, "controlled" means more than simply "having a presence on," since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others.[183]

Social media—computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. By design, social media is internet-based and gives users quick electronic communication of content. Content includes personal information, documents, videos, and photos. Users engage with social media via computer, tablet or smartphone via web-based software or web application, often utilizing it for messaging.[184]

Spamming—unsolicited usually commercial messages such as e-mails, text messages, or Internet postings sent to a large number of recipients or posted in a large number of places.[185]

Tweet—a post made on the Twitter online message service.[186]

White Hat Hackers—use their skills to help enterprises create robust computer systems.[187]

Zero day—A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability.[188]

[182] "What Is a URL Redirect? - Definition from Techopedia," *Techopedia.Com*, accessed February 18, 2020, https://www.techopedia.com/definition/1708/url-redirect.

[183] US Department of Defense, *Joint Publication (JP) 3-12*, I–5.

[184] Maya E. Dollarhide, "Social Media," *Investopedia*, accessed February 18, 2020, https://www.investopedia.com/terms/s/social-media.asp.

[185] "Definition of SPAM," accessed February 18, 2020, https://www.merriam-webster.com/dictionary/spam.

[186] "Definition of TWEET," accessed February 18, 2020, https://www.merriam-webster.com/dictionary/tweet.

[187] "What Is a Hacker?"

[188] "What Is a Zero-Day Exploit?," *FireEye*, accessed February 18, 2020, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

Bibliography

Arkin, William M. “Ask Not for Whom the Phone Rings.” *Http://Www.Washingtonpost.Com*. Last modified October 11, 1999. Accessed September 25, 2019. http://www.washingtonpost.com/wp-srv/national/dotmil/arkin101199.htm.

———. “The Cyber Bomb in Yugoslavia.” *The Washington Post*, October 25, 1999. Accessed August 28, 2019. https://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

Arkin, William M., and Robert Windrem. “The Other Kosovo War.” *InfoSec News*. Last modified August 29, 2001. Accessed November 6, 2019. http://lists.jammed.com/ISN/2001/08/0196.html.

Bacevich, Andrew J., and Eliot A. Cohen, eds. *War over Kosovo: Politics and Strategy in a Global Age*. New York: Columbia University Press, 2001.

Bassford, Christopher. “Clausewitz and His Works.” *Clausewitz and His Works*. Last modified March 8, 2016. Accessed February 26, 2020. https://www.clausewitz.com/readings/Bassford/Cworks/Works.htm.

Beckhusen, Robert, and Noah Shachtman. “Hamas Shoots Rockets at Tel Aviv, Tweeting Every Barrage.” *Wired*, November 15, 2012. Accessed December 5, 2019. https://www.wired.com/2012/11/gaza-social-media-war/.

Bohn, Lauren E. “Israel and Hamas Battle on Social Media as Well.” *Boston.Com*. Last modified November 15, 2012. Accessed December 5, 2019. https://web.archive.org/web/20121116194700/http://www.boston.com/news/world/middle-east/2012/11/15/israel-and-hamas-battle-social-media-well/O2zOPWK7t3FG4QeMBhxVpL/story.html.

Campen, Alan D., and Douglas H. Dearth, eds. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*. Fairfax, VA: AFCEA International Press, 2000.

Carlisle, Rodney P. *Encyclopedia of Intelligence and Counterintelligence*. New York, NY: M.E. Sharpe, 2015.

Cenciotti, David. “Israeli Air Force Releases Video of Mysterious Drone Shot down by an F-16 over Israeli Airspace.” *The Aviationist*, October 6, 2012. Accessed November 10, 2019. https://theaviationist.com/2012/10/06/iaf-uav-shotdown/.

CISA. “Understanding Denial-of-Service Attacks.” *Security Tip (ST04-015)*. Last modified November 20, 2019. Accessed March 18, 2020. https://www.us-cert.gov/ncas/tips/ST04-015.

Cohen, Daniel, and Danielle Levin. “Cyber Infiltration During Operation Protective Edge.” *Forbes*, August 12, 2014. Accessed August 19, 2019. https://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/.

Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. “Israel and Cyberspace: Unique Threat and Response.” *International Studies Perspectives* 17, no. 3 (August 1, 2016): 307–321.

Coleman, Gabriella. “Anonymous: From the Lulz to Collective Action.” *The New Everyday: A MediaCommons Project*. Last modified April 6, 2011. Accessed January 20, 2020. https://web.archive.org/web/20130517212228/http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action.

Conti, Greg, and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press, 2017.

Dieterle, Daniel. “Did Israel Hack Unmanned Helicopter That Entered Their Airspace?” *CYBER ARMS - Computer Security*, October 7, 2012. Accessed August 15, 2019. https://cyberarms.wordpress.com/2012/10/07/did-israel-hack-unmanned-helicopter-that-entered-its-airspace/.

Dollarhide, Maya E. “Social Media.” *Investopedia*. Accessed February 18, 2020. https://www.investopedia.com/terms/s/social-media.asp.

Forces, Israel Defense. “CLEARED FOR RELEASE: We Thwarted an Attempted Hamas Cyber Offensive against Israeli Targets. Following Our Successful Cyber Defensive Operation, We Targeted a Building Where the Hamas Cyber Operatives Work. HamasCyberHQ.Exe Has Been Removed.Pic.Twitter.Com/AhgKjiOqS7.” Tweet. *@IDF*, May 5, 2019. Accessed August 13, 2019. https://twitter.com/IDF/status/1125066395010699264.

Fowler, Sarah. “Hamas and Israel Step up Cyber Battle for Hearts and Minds.” *BBC News*, July 15, 2014, sec. Middle East. Accessed December 5, 2019. https://www.bbc.com/news/world-middle-east-28292908.

Fulghum, David A. “Telecom Links Provide Cyber-Attack Route.” *Aviation Week & Space Technology*, November 8, 1999.

———. “Yugoslavia Successfully Attacked by Computers.” *Aviation Week & Space Technology*, August 23, 1999.

Fulghum, David A., and Douglas Barrie. “Israel Used Electronic Attack in Air Strike against Syrian Mystery Target.” *ABC News*. Last modified October 8, 2007. Accessed October 8, 2019. https://web.archive.org/web/20140207061332/http://abcnews.go.com/Technology/story?id=3702807.

Gardham, Duncan. “Mossad Carries out Daring London Raid on Syrian Official.” *The Telegraph*. Last modified May 15, 2011. Accessed December 5, 2019. https://web.archive.org/web/20110518025425/http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8514919/Mossad-carries-out-daring-London-raid-on-Syrian-official.html.

Gast, Phil, Dakin Andone, and Kara Fox. “Here’s Why the Iran Protests Are Significant.” *CNN*. Last modified January 2, 2018. Accessed November 21, 2019. https://www.cnn.com/2017/12/30/world/iran-protests-issues/index.html.

Geers, Kenneth. *Cyberspace and the Changing Nature of Warfare*. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008. https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfW arfare.pdf.

Groll, Elias. *The Future Is Here, and It Features Hackers Getting Bombed*. The Foreign Policy Group, May 6, 2019. Accessed August 13, 2019. https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Gross, Judah Ari. "IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle." *The Times of Israel*, May 5, 2019. Accessed August 13, 2019. https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/.

Hoffman, Chris. "What Is DNS Cache Poisoning?" *How-To Geek*. Accessed February 24, 2020. https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/.

Issacharoff, Avi. "Hamas Establishes New Intelligence Service in Gaza." *Haaretz*, January 8, 2007. Accessed December 10, 2019. https://www.haaretz.com/1.4957530.

Janczewski, Lech, and Andrew M. Colarik, eds. *Cyber Warfare and Cyber Terrorism*. Hershey, PA: Information Science Reference, 2008.

Klieger, Noah. "A Strike in the Desert." *Ynetnews.Com*. Last modified November 2, 2009. Accessed December 5, 2019. https://web.archive.org/web/20121025090109/http://www.ynetnews.com/articles/0%2C7340%2CL-3799227%2C00.html.

Kumar, Mohit. "Israel Neutralizes Cyber Attack by Blowing up a Building with Hackers." *The Hacker News*. Last modified May 6, 2019. Accessed September 25, 2019. https://thehackernews.com/2019/05/israel-hamas-hacker-airstrikes.html.

Kurz, Anat, and Shlomo Brom, eds. *The Lessons of Operation Protective Edge*. Tel Aviv: Institute for National Security Studies, 2014. https://www.inss.org.il/publication/the-lessons-of-operation-protective-edge/.

Lappin, Yaakov. "IAF Strike Kills Hamas Military Chief Jabari." *The Jerusalem Post*. Last modified November 14, 2012. Accessed December 5, 2019. https://www.jpost.com/Defense/IAF-strike-kills-Hamas-military-chief-Jabari.

Levin, Daniel. "Iran, Hamas and Palestinian Islamic Jihad." *Wilson Center*. Last modified July 9, 2018. Accessed November 13, 2019. https://www.wilsoncenter.org/article/iran-hamas-and-palestinian-islamic-jihad.

Leyden, John. "Israel Suspected of 'hacking' Syrian Air Defences." *The Register*, October 4, 2007. Accessed August 15, 2019. https://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

McCoy, Kelly. "The Road to Multi-Domain Battle: An Origin Story." *Modern War Institute*, October 27, 2017. Accessed February 22, 2020. https://mwi.usma.edu/road-multi-domain-battle-origin-story/.

Melman, Yossi. "OUTSIDE THE BOX: Israel's Strike on Syria's Nuclear Plant." *The Jerusalem Post*. Last modified April 6, 2018. Accessed December 5, 2019.

https://www.jpost.com/Arab-Israeli-Conflict/OUTSIDE-THE-BOX-Israels-strike-on-Syrias-nuclear-plant-547870.

Merrin, William. *Digital War: A Critical Introduction*. New York, NY: Routledge Taylor & Francis Group, 2019.

Messmer, Ellen. "Serb Supporters Sock It to NATO, U.S. Web Sites." Last modified April 6, 1999. Accessed September 24, 2019. http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html.

Milosevic, Nikola. "Case of the Cyber War: Kosovo Conflict." *Inspiratron*, July 1, 2014. Accessed August 25, 2019. http://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/.

Moghanizadeh, Somayeh. "The Role of Social Media in Iran's Green Movement." Master of Communication, University of Gothenburg, 2013.

Newman, Lily Hay. "What Israel's Strike on Hamas Hackers Means for Cyberwar." *Wired*, May 6, 2019. Accessed August 15, 2019. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

Noman, Helmi. "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army." *OpenNet Initiative*. Accessed December 10, 2019. https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army.

Parkinson, Roger. *Clausewitz A Biography*. New York: Stein and Day, 1971.

Rathmell, Andrew. "Information Operations--Coming of Age?" *Jane's Intelligence Review* 12, no. 5 (May 2000).

Ravid, Barak. "Netanyahu: Cease-Fire with Hamas Is the Right Thing for Israel." *Haaretz*, November 21, 2012. Accessed December 5, 2019. https://www.haaretz.com/netanyahu-cease-fire-right-thing-1.5199481.

Rezvaniyeh, Farvartish. "Pulling the Strings of the Net: Iran's Cyber Army." *FRONTLINE - Tehran Bureau*. Last modified February 26, 2010. Accessed October 31, 2019. http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html.

Sadjadpour, Karim, and Collin Anderson. *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. Washington, DC: Carnegie Endowment for International Peace, 2018. https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. First edition. New York: Crown Publishers, an imprint of the Crown Publishing Group, 2018.

Shachtman, Noah. "Israel Kills Hamas Leader, Instantly Posts It to YouTube." *Wired*, November 14, 2012. Accessed December 5, 2019. https://www.wired.com/2012/11/idf-hamas-youtube/.

Shamah, David. "Hackers Threaten 'Israhell' Cyber-Attack over Gaza." *The Times of Israel*, July

9, 2014. Accessed August 19, 2019. http://www.timesofisrael.com/hackers-threaten-israhell-cyber-attack-over-gaza/.

———. “Iran, Hamas Conduct Cyber-Attacks against Israel.” *The Times of Israel*. Accessed August 13, 2015. http://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

Siboni, Gabi, and Sami Kronenfeld. “The Iranian Cyber Offensive during Operation Protective Edge.” *INSS Insight*, no. 598 (August 26, 2014).

Slackman, Michael. “On Anniversary, Ahmadinejad Boasts of Iran’s Nuclear Prowess.” *The New York Times*, February 11, 2010, sec. Middle East. Accessed November 19, 2019. https://www.nytimes.com/2010/02/12/world/middleeast/12iran.html.

Smith-Spark, Laura. “UN Experts Urge Iran to Respect Rights, End Internet Crackdown.” *CNN*. Last modified January 5, 2018. Accessed October 31, 2019. https://www.cnn.com/2018/01/05/middleeast/iran-protests-united-nations-intl/index.html.

Somfalvi, Attila. “Gaza Truce Deal: Crossings to Open under Israeli Supervision.” *Ynetnews*. Last modified August 26, 2014. Accessed December 5, 2019. https://www.ynetnews.com/articles/0,7340,L-4564456,00.html.

Thomas, Douglas, and Brian Loader, eds. *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. New York, NY: Routledge, 2000.

Torbati, Yeganeh, and Joseph Menn. “Hackers Accessed Telegram Messaging Accounts in Iran.” *Reuters*, August 2, 2016. Accessed October 31, 2019. https://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM.

US Air Force. *Basic Doctrine*. Vol. I. Maxwell AFB, AL: United States Air Force, 2015.

US Department of Defense, Joint Staff. *Capstone Concept for Joint Operations*. 2nd ed. Washington, DC: Government Printing Office, 2005.

———. Joint Publication (JP) 3-0, *Joint Operations*. Washington, DC: Government Printing Office, 2017.

———. Joint Publication (JP) 3-12, *Cyberspace Operations*. Washington, DC: Government Printing Office, 2018.

US Department of the Army. Field Manual (FM) 3-0, *Operations*. Washington, DC: Government Printing Office, 2008.

———. Field Manual (FM) 3-13, *Information Operations*. Washington, DC: Government Printing Office, 2016.

———. TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*. Washington, DC: Government Printing Office, 2018.

Woodford, Shawn. “The Russian Artillery Strike That Spooked The U.S. Army.” *Mystics & Statistics*, March 29, 2017. Accessed October 1, 2019. http://www.dupuyinstitute.org/blog/2017/03/29/the-russian-artillery-strike-that-spooked-the-u-s-army/.

“Anonymous Hack Hundreds of Israeli Websites, Delete Foreign Ministry Database in Support of Gaza.” *RT International*. Last modified November 17, 2012. Accessed December 5, 2019. https://www.rt.com/news/anonymous-gaza-israel-website-938/.

“Common IP Filtering Techniques.” Accessed February 18, 2020. https://www.apnic.net/manage-ip/apnic-services/registration-services/resource-quality-assurance/filtering/.

“DDoS Attack Types & Mitigation Methods.” *Learning Center*, n.d. Accessed February 18, 2020. https://www.imperva.com/learn/application-security/ddos-attacks/.

“Definition of Liveblog.” *Www.Dictionary.Com*. Accessed February 18, 2020. https://www.dictionary.com/browse/liveblog.

“Definition of Proxy Server.” *PCMAG*. Accessed February 18, 2020. https://www.pcmag.com/encyclopedia/term/proxy-server.

“Definition of SPAM.” Accessed February 18, 2020. https://www.merriam-webster.com/dictionary/spam.

“Definition of TWEET.” Accessed February 18, 2020. https://www.merriam-webster.com/dictionary/tweet.

“Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries.” *Mi2g Cyber Warfare Advisory*, April 19, 1999. Accessed October 24, 2019. http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/170499.php.

“Hamas - Conflict with Israel.” *Encyclopedia Britannica*. Last modified January 17, 2019. Accessed November 13, 2019. https://www.britannica.com/topic/Hamas.

“Hamas’ Izz al-Din al-Qassam Brigades.” *Australian National Security*. Accessed December 10, 2019. https://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/HamassIzzal-Dinal-QassamBrigades.aspx.

“Hashtag Definition.” Accessed February 18, 2020. https://techterms.com/definition/hashtag.

“In Response to Protests, Iran Cuts off Internet Access, Blocks Apps.” *NPR.Org*. Last modified January 3, 2018. Accessed October 31, 2019. https://www.npr.org/2018/01/03/575252552/in-response-to-protests-iran-cuts-off-internet-access-blocks-apps.

“Iran: State of the Green Movement.” *Foreign Policy Initiative*. Last modified April 6, 2010. Accessed November 19, 2019. https://web.archive.org/web/20160827141650/http:/www.foreignpolicyi.org/event/iran/greenmovement.

“Israel Faces 44 Million Attacks on Websites in Response to Gaza Offensive.” *RT International*. Last modified November 18, 2012. Accessed December 5, 2019. https://www.rt.com/news/israel-cyber-hackers-gaza-000/.

“Net Warfare over Kosovo.” *BBC News*, October 23, 1998. Accessed August 25, 2019. http://news.bbc.co.uk/2/hi/science/nature/200069.stm.

"News Briefs." *InfoWorld*, April 5, 1999. https://books.google.com/books?id=ElAEAAAAMBAJ&pg=PA1&lpg=PA1&dq=inforworld+volume+21+edition+14&source=bl&ots=5IiejwqPRV&sig=ACfU3U2ofjc2VQr-jGUkb7CyrHNzx-UotA&hl=en&ppis=_e&sa=X&ved=2ahUKEwiH6MP2-6foAhV1IDQIHcNgARcQ6AEwAHoECAkQAQ#v=onepage&q&f=false.

"Operation Pillar of Defense." *Israel Defense Forces*. Last modified October 30, 2017. Accessed December 5, 2019. https://www.idf.il/en/minisites/wars-and-operations/operation-pillar-of-defense-2012/.

"Operation Protective Edge." *Israel Defense Forces*. Last modified October 30, 2017. Accessed December 5, 2019. https://www.idf.il/en/minisites/wars-and-operations/operation-protective-edge-julyaugust-2014/.

Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election. Santa Monica, CA: RAND, 2012.

"War of Words on the Internet." *BBC Monitoring*. Last modified October 25, 1998. Accessed September 24, 2019. http://news.bbc.co.uk/2/hi/world/monitoring/200708.stm.

"What Is a Black Hat Hacker? - Definition from Techopedia." *Techopedia.Com*. Accessed February 18, 2020. https://www.techopedia.com/definition/26342/black-hat-hacker.

"What Is a Hacker? - Definition from Techopedia." *Techopedia.Com*. Accessed February 18, 2020. https://www.techopedia.com/definition/3805/hacker.

"What Is a Hacktivist?" *United States Cybersecurity Magazine*. Last modified December 11, 2018. Accessed February 18, 2020. https://www.uscybersecurity.net/hacktivist/.

"What Is a URL Redirect? - Definition from Techopedia." *Techopedia.Com*. Accessed February 18, 2020. https://www.techopedia.com/definition/1708/url-redirect.

"What Is a Zero-Day Exploit?" *FireEye*. Accessed February 18, 2020. https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

"What Is the Internet Protocol?" *Cloudflare*. Accessed February 18, 2020. https://www.cloudflare.com/learning/ddos/glossary/internet-protocol/.