Cyber Attacks:: The Electronic Battlefield

Author(s): Khalid Walid Mahmoud

Arab Center for Research & Policy Studies (2013)

Stable URL: http://www.jstor.com/stable/resrep12651

المركز العربي للأبحاث و دراسة السياسات
Arab Center for Research & Policy Studies

RESEARCH PAPER

Cyber Attacks: The Electronic Battlefield

Khalid Walid Mahmoud | December 2013

Cyber Attacks: The Electronic Battlefield

Series: Research Paper

Khalid Walid Mahmoud | December 2013

The Arab Center for Research and Policy Studies is an independent research institute and think tank for the study of history and social sciences, with particular emphasis on the applied social sciences.

The Center's paramount concern is the advancement of Arab societies and states, their cooperation with one another and issues concerning the Arab nation in general. To that end, it seeks to examine and diagnose the situation in the Arab world - states and communities- to analyze social, economic and cultural policies and to provide political analysis, from an Arab perspective.

The Center publishes in both Arabic and English in order to make its work accessible to both Arab and non-Arab researchers.

Arab Center for Research and Policy Studies

PO Box 10277

Street No. 826, Zone 66

Doha, Qatar

Tel.: +974 44199777 | Fax: +974 44831651

www.dohainstitute.org

Table of Contents

Introduction

In recent years, the notion of cyberspace as a battlefield has gone through a number of interesting developments, foremost of which is the devastating effect of cyber attacks devised by states, groups, and individuals. Hacking, a worrisome phenomenon for both governments and individuals, is the most prominent form of attack. At the root of this worry lies the different parties involved and the difficulty not only in tracking its sources, but also in locating its bases and assessing the cost of its effect. The World Wide Web has now become an arena for conflicts involving espionage, unauthorized entry, and control of databases that might impinge on some states national security. In light of these developments, most governments have prioritized the issue of cyberspace, and have focused on developing mechanisms of preventative action.

Most of the world's productive, intangible, and informational services have come to exclusively rely on the Internet. This process began in the 1990s with the shift of mass communication to the Internet and the ever-growing demands on it in the fields of production, distribution, communications, and finance. Such heavy reliance on the Internet makes the potential damage from cyberattacks even greater. These attacks have proliferated and take on a broader scope in a world where the Internet remains unsecure and easy to hack, particularly because of recent software and hardware developments. Savvy IT hackers, who take down highly critical websites to steal personal and private data from individuals and institutions—most seriously, of course, data from financial and military institutions have also become increasingly active. They hack institutions to deliver messages of political protest, amass documents and secrets, or sometimes make money. Beyond the inherent threats, the real danger lies in not knowing their capabilities and being unable to predict their actions.[1]

Cyberattacks have become a powerful, low-cost option of warfare. The world is facing forces armed with computer technology capable of hacking their way in and create virtual damage that materially hurts others with the click of a button. Recent incidents, virtual and real, have shed light on the new domain of cyberattacks, especially after those launched by *Anonymous*,[2] an international network of hackers. *Anonymous* has targeted

[1] Verwoerd, "Honours Report," p. 12.

[2] The Anonymous collective is considered the most influential group of hackers in the history of hacking. There is no information on their total number or the number of sub-groups. They have carried out well-

global and Middle Eastern targets, including Israel. On account of these attacks, it seems that the conflict between these players is taking the form of attack and counterattack against facilities and systems in various fields on both fronts of this conflict, creating intangible material damage. Estimates vary as to the extent of this damage and its effect on civil and military institutions' financial and technological activities and programs.

The phenomenon of cyberattacks has produced a host of challenges. This analysis attempts to comprehensively describe the "operational" element of cyberattacks and deal with the notion of cyberspace. It concentrates on hackers, especially those within Anonymous, as one of the main contenders within the conceptual cyber realm. The final section focuses on Israel and examines the attack against it on April 7, 2013, as well as the country's efforts to create strategic defenses in cyberspace.

This paper also aims to give a clear picture of the new cyber environment. The ability to deal with it successfully has become a pivotal matter for states who must use this knowledge to reformulate the lexicon of security and technological systems in the information age. Its importance stems from the fact that cyberattacks represent a guide that can aide them in understanding how to adequately deal with their implications in the physical world. Cyberattacks are to be added to the list of conventional threats facing states, groups, and individuals alike, and have the ability to affect individual countries or the world, "particularly in light of the growing role of cyberspace in various fields, and the greater reliance being placed upon it by individuals, political groups, and governmental bodies. This increases the strategic importance of these mechanisms [for cyberattacks] and their effectiveness in meeting the aims of users."[3]

known operations, including their support for the WikiLeaks site. These groups have caused many problems around the world. To date, they have attacked the websites of multinational corporations; intervened in the 2009 Iranian elections; attacked Australian government websites in demand of completely uncensored browsing; and leaked personal data on public figures in Bahrain, Morocco, Egypt, and Jordan. The Arab Spring was also an arena of intensive activity, as the group offered immediate help to the popular revolutions in Tunisia and Egypt by attacking government websites in the two countries. Some analysts have praised them as digital warriors, while others have condemned them as an army of computer anarchists. See Abu Talib, "Anonymous: Political Hacktivism," January 1, 2012.

[3] Ali, "Virtual Activists: E-clashes," June 10, 2013.

Definition and Implications of Cyberspace

Physically, cyberspace can be defined as the digital medium's extension across various lines of transmission—metallic, fiber optic, and wireless—and their channels on the network of networks, the Internet. In these terms, cyberspace is the technological expression of the information super-highway. In cyberspace, geographic locations have collapsed, and oceans of information now have to be charted and navigated spatially and temporally. This is what makes cyberspace the unrivalled key feature of the information age. Within its vast space, it houses the community of the global village in humanity's digital universe, along with its new structures, characteristics, and values.[4] "What is novel is the appearance of a virtual world as a spatio-temporal expanse that has become a literal 'new world'"—a world to which capital, contemporary arts and sciences, entertainment, and crime have flocked.[5]

There are numerous definitions of cyberspace. The International Telecommunication Union—the UN body responsible for Information and Communication Technology (ICT)—offers the following definition: "[It is] the material and immaterial space that develops or forms from one or more of the following: computers, smart devices, networks, computerized information, programs and content, traffic and control data, and those who use all of these."[6] In contrast to definitions that consider cyberspace a fifth dimension, some view it as one of seven: space, land, air, sea, electro-magnetic, and human.[7] There are also those who define cyberspace as the "fifth space of warfare after land, sea, air, and space".[8] In this definition, cyberspace is understood as being broader than the Internet, embracing other computer networks hooked into the Internet. In addition, there are Supervisory Control and Data Acquisition (SCADA) systems that only allow machines to speak to other machines, and control machines linked to critical junctures in the economy. This also leads to cyberspaces inclusion in the world of warfare. "Throughout human history, the world has known land and sea wars, aerial warfare, and, more

[4] Rahuma, *The Internet and the Socio-Technical System*, p. 33.

[5] Yunus, *The Information Society*, p.13.

[6] International Telecommunication's Union.

[7] "War in Cyberspace," p.3.

[8] Schreier, *On Cyberwarfare*.

recently, war in space. Now there is internet war."[9] This orientation also makes a distinction between cyberspace and electromagnetic space, viewing the human element as an independent arena.[10]

The clear common factor among all the definitions is cognition. Any differences and variations appear to reflect the level of attention states and organizations give to meeting the challenges of cyberspace. It seems, however, that differences in definition do not reflect different understandings of cyberspace. All assent to the aspects included in the UN's definition.[11]

The ICT revolution has provided a number of mechanisms and tools to overcome difficulties faced by those working in the information world and its networks extending through globalized cyberspace. There now exists a number of digital and physical tools with a growing number of specialist users to test the performance of networks or identify their vulnerabilities. Hackers have plenty of chances to use them in operations to hack into systems. Over the last decade, on the Internet and in the software field, many tools have emerged with potential to cause damage to IT systems. These have been built by amateurs or organizations that have harnessed their activities and made tools that contribute to the vandalizing of computer systems for the benefits of a third party or for other ends available.

The modern world experienced its first full-blown cyber storm after WikiLeaks revealed thousands of official classified documents between the US State Department and its missions around the world on its website. These leaks caused tense international relations among many world leaders, whose recorded words and statements conflicted with the positions they had declared to their peoples, causing unrest and protests in many countries. The use of the Internet to broadcast these leaks had an important effect in consolidating the concept, importance, and dangers of the Internet as one of the fruits

[9] Ghaneim, "Deadly virtual warfare," October 25, 2010.

[10] Schreier describes features of cyperspace as "reliant on the electromagnetic spectrum, requir[ing] man-made machines, constantly replicating, easy and inexpensive to enter, and that the offense is dominant rather than the defense." See Schreier, *On Cyberwarfare*.

[11] Ibid.

of the ICT revolution, and the varied and boundless technological abilities its users have, whether good or bad, locally, regionally, and globally.[12]

Hackers: Breaking into Cyberspace

The information revolution has given rise to cyberattacks and what has become known as cyber warfare fought through computers and the Internet. Hackers, pivotal players in the digital environment who use software and computers to breach systems, are at the core of this warfare.[13] The ever-growing amount of information on the net and its increasing value (as knowledge, economic, political, and military source, depending of the nature of the site hosting it) have led to a fundamental change to the aims of cyberattacks. Initially, these started as curious ventures by individuals in their pursuit to acquire knowledge or attempt to penetrate the firewalls set up by other parties to feel the thrill of victory. Now, attacks are effectuated for material or political gain, with the potential to partially or totally bring down targeted websites becoming an integral part of the hacker ethos.

Compromising a nation's cyberspace is undertaken by individuals or groups of hackers who have the ability to control and direct computer programs. These are typically skilled programmers capable of hacking into computers and discovering their contents. Most refuse to divulge their real identity for fear of prosecution by the state, and choose the name "Anonymous".

Hackers typically compromise and damage computer networks using the following tactics:

1. Virtual sit-ins and blockades aim to damage or disrupt ordinary operation by preventing users from having access to digital services and resources, which is done by overloading the server with requests.[14]

[12] al-Rashidi, *The Internet and Facebook*, p.16.

[13] These can be divided into two groups: hackers, or amateurs who are largely motivated by the desire to learn and have fun, and crackers, who are more professional and whose actions usually serve a particular goal.

[14] Slobbe and Verberkt, "Hacktivists: Cyberterrorists or Online Activists," July 22, 2012.

2. Email bombs involve sending thousands of emails to the target's address, causing the mail account to malfunction.[15]

3. Web hacks and computer break-ins occur when hackers gain unauthorized entry to a website and replace contents with contents of their own that changes the nature of the site.[16]

4. Viruses infect systems with computer viruses and internet worms, and spread them over national and global networks causing temporary or permanent disruption to files and operating systems.

5. Denial of Service (DoS) attacks flood sites with unnecessary data sent by programs dedicated to this task, which slows the service or causes excessive traffic to the site in question, making it difficult for users to access. Many important and sensitive websites (Amazon and Word Press, for example) have been attacked in this way despite the existence of products and programs that are meant to prevent such attacks.

In light of the digital and information revolution over the last 20 years, it is worth pointing out that the world has begun to witness the virtual damage of complex systems, not just for military objectives,[17] but also for economic,[18] media, political, and even criminal motivations. Experts predict a continued growth in the number of attacks over the next year, in addition to political hacking, cyberattacks, and governments' use of "legitimate" surveillance tools in cyberspace. They also suggest that attacks against computer-reliant infrastructure will take place, along with a decline in digital privacy, problems with

[15] al-Zaro, *Cyberspace*, p. 216.

[16] Slobbe and Verberkt, "Hacktivists."

[17] Over the past two decades, and as a result of the main developments in the international conflict arena, weapons systems and smart military hardware that rely upon accurate data for their operation and updating have proliferated. Such weapons systems and their peripherals depend on global information systems directly connected to computers controlled by other states (e.g., GPS, communications, and surveillance satellites) while having little control over the spread of the information. The technologically advanced nations (i.e., those whose infrastructures rely heavily on information systems) have become more anxious about their information systems being hacked and damaged.

[18] The best-known cyberattacks are those that target the economy of a state or steal from banks and bank accounts. In a 2012 report, *The Washington Post* reviewed a US intelligence assessment on cyber-espionage and hacking that targeted a number of states, including the US. The assessment affirmed that such operations were a threat to the economic interests of states.

Internet digital trust authorities, further attacks against mobile operating systems and devices, and the exploitation of software vulnerabilities.[19]

Following increasing hacker activity and heated competition between governments in this field, which has changed the form of modern warfare, states have come to realize the enormity of the threats they are facing. The matter is not just related to military affairs, but extends to the civilian arena[20] in terms of "damaging and totally paralyzing states at the touch of a keyboard. Those who do not hasten to comprehend this will not endure in any confrontation."[21]

Anonymous: An Army Stationed in Cyberspace

There are many factors that turn Anonymous into a usable weapon. Its unique features have made it a subject of prime interest to many unknown users of the Internet around the world, including the ability to penetrate information systems, cyberspace's absence of spatial borders, users' hazy digital identity in this open environment, and concerns extending beyond the boundaries of users' own state or society, all of which tangibly increase its capacity to have an impact. Hence, this group "is not presently composed of a set of professional hackers, but of groups with skills such as writing or video production, or street activism, or others with no particular skill, but who help spread and copy information and emails, especially over social media."[22] Low cost is also a factor since the availability of IT tools on the Internet, coupled with progress made in decryption ("cracking"), have provided a vast number of programs for such users to exploit their targets without large financial resources. Perhaps the most important feature of

[19] "Cyber Espionage and Hacking," December 10, 2012.

[20] Cyberspace is also a realm in which the military and civilians merge. In many cases, military communications are linked to civilian networks; therefore, the protection of civilian infrastructure and networks also becomes a vital military objective. At the same time, the military has capabilities in the virtual world that can help protect civilian networks.

[21] Shahboun, "Cyber Wars," June 4, 2011.

[22] Abu Talib, "Anonymous: Political Hacktivism."

Anonymous is that is does not have a shared ideology except for the insistence on and fight for absolute freedom on the Internet.[23]

Contrary to popular narrative, those who belong to the Anonymous network do not inhabit their own private universe inside darkened bedrooms as they are often portrayed in the media. Rather, they are young people well aware of what is happening in the world who hold Internet culture sacred as the embodiment of free expression. This non-hierarchical collection of anonymous individuals is being pursued by the authorities for compromising the US intelligence service, disseminating CIA documents, and directly backing WikiLeaks by hacking Master Card and Amazon in reaction to their refusal to allow the public to use their sites to send financial support to WikiLeaks.

Anonymous is a multinational operation. All it needs to launch an attack is a number of clever programmers, a few computers, and the accumulated IT knowledge of a broad spectrum of computer users, in addition to the ready availability of key Internet sites for large material storage that will assist in the development of the requisite skills. This has formed a critical factor in the increased interest in this field, particularly after "hacking turned into organized acts of espionage, vandalism, and cyber warfare against states or organizations. Vital sectors have been targeted, leading major states to acquiesce and admit the real danger being posed."[24]

Each of these factors create a fertile environment for the growth of a movement able to launch cyberattacks and compromise the infrastructural systems of states, and, if their techniques and cunning are perfected, perhaps take over air traffic control, traffic lights, and electronic warfare systems. "The sheer quantity and increasing value of the information spread over the Internet has affected the hackers' activity and produced a radical change in their goals. Once an expression of curiosity for new knowledge or an attempt to penetrate the firewalls set up by other parties, cyberattacks are now targeting material or political gains."[25]

There are multiple reasons members of Anonymous are driven to hack, such as accumulated resentment and grudges that lead to the desire to destroy or vandalize what belongs to others. There are even hackers who work with the actual target to undertake

[23] Slobbe and Verberkt, "Hacktivists."

[24] al-Zaydi, "Hackers: Pirates of the Cyber Age," January 31, 2012.

[25] al-Zaro, *Cyberspace*, p.218.

simulated attacks as a means to test the target's security systems. Others get involved for the technical challenge and the acquisition of status between users, simple enjoyment and pleasure in discovery, and the offer of material rewards. This motive may arise out of need, greed, or the desire to eliminate a rival as a result of conflicting interests. Similarly, curiosity and discovery of the unknown and forbidden or the existence of political objectives and motivations may unite individuals or groups with a particular political belief or ideas and who employ computer hacking to serve their political beliefs and positions. They might in this case, for example, resort to bringing down a web site, or extract data, from a database connected to states, groups, or companies they perceive as the enemy. Using groups of hackers to attack websites in support of popular struggles or to expose corrupt governments is a new development.

A prime example of this occurred during the Arab Spring, when Arab citizens used the Internet as a technological ally to help them exchange information, organize protests, and promote the movement as a whole. At the time, a debate opened over the morality of hacking, and prevalent Arab discourse depicted hackers as technologically obsessed youth who spent their time trying to compromise the security of states and large institutions for fun. Shortly after these accusations were thrown around, the popular uprisings demonstrated that many of these youth were using their expertise to help the revolutionaries and expose governments. One such example is when Egyptian citizens managed to find a solution that allowed them to carry on using social media sites even after the government of former president Hosni Mubarak ordered the Internet to be shut down. Members of Anonymous hacked official sites of the regime of former Tunisian president Zine el-Abideen Ben Ali in response to the government's blocking access to the Internet at the outset of the revolution. They left a message on these sites saying: "From Anonymous to the Tunisian government: We will never tolerate attacks on freedom of expression and your citizens' access to information. Any organization involved in censorship will be targeted." Hackers see governments as using the Internet to control citizens, so citizens have the right to use the internet to expose the secrets and workings of government.[26]

Anonymous carried out several attacks against websites and pages of Egyptian governmental bodies and ministries during the January 25 Revolution in response to the security forces' treatment of protestors and in revenge for cutting Egyptians' access to the internet and communications. This campaign was termed Operation Egypt, and

[26] al-Khouri, "We Are All Eye-Witnesses," p. 128.

elements from the Telecomix[27] group assisted in providing unconventional means for Egyptians to access the Internet once it had been cut off.[28]

It is worth noting that "since the eruption of protests in Tunisia, videos have started to appear on the Internet under the name Anonymous and entitled Operation Tunisia, which is a revenge operation against the Tunisian authorities for their violent practices against protestors and the campaign of arrests against bloggers. Sensitive websites were brought down, in particular those of the defense, interior, and foreign ministries. Similar actions—which mostly left a message of support for the people accompanied by threats against the government—were repeated in Egypt, Libya, Turkey, Spain, Greece, Italy, Portugal, Eastern European countries, Zimbabwe, China, Russia, Iran, Syria, and elsewhere in support of protest movements or movements demanding democracy and an end to corruption."[29] Things were somewhat different in the US in terms of support for the Occupy movement[30] when bloggers and news sites allied and sympathetic to Anonymous on Facebook covered events on the ground more than joining in hacking actions. Hence, "this group helped in one fashion or another to put the spotlight on the protests via alternative media networks when mainstream media deliberately ignored them, at least to begin with."[31]

It remains quite difficult to assess the number of members of Anonymous, which has become a symbol for hackers. A cyberspace army that meets and chats in private chat rooms, Anonymous members are operating in various regions of the world and have their own priorities. They have no leader and have sometimes used the motto, "We are Anonymous. We are Legion. We don't forgive. We don't forget. Expect Us."—a slogan used to end their written and video statements in reference to anyone who would violate freedom of expression and put limits on Internet freedom. Their goal is to expose corrupt governments, referring to all governments. They represent an intercontinental

[27] A hacker group interested in exposing those who block or censor the Internet.

[28] Abu Talib, "Anonymous: Political hacktivism."

[29] Ibid.

[30] Ibid.

[31] Ibid.

phenomenon and a form of 21st century protest movement. Their field of activity and response is cyberspace.

Cyberspace and the Frantic Race between States

Cyber warfare is a 21st century concept of international conflict, and refers to the "means of waging war that depend on IT and that target computers or websites. It includes covert entry into automated systems and the collection, export, corruption, alteration or encryption of data, as well as the planting of spyware and other such forms of compromise or hacking."[32] It follows that if the invention of gunpowder changed the map of international wars, then taking control of the modern technological state could paralyze major nations and bring them to their knees without firing a single bullet.[33] As Kheiri and Saeed note, this idea is an integral part of the fifth generation of asymmetrical warfare that may be undertaken by groups, individuals, or states using advanced technology. [34] Cyberattacks can have various objectives, although all of them pose a common threat to countries' economic interests. The best known forms of attack target the economy of a particular state, or attempt to rob banks or bank accounts. Similarly, cyberspace and its accelerating technological complexity have proved one of the most important means for future conflicts capable of being decisive in many aspects. The range of modern military strategies give weight to ideas of smart armies based on quality not size, or, to be more precise, based on advanced technology and the ability to achieve the highest gains with the fewest resources.

Over recent years, the world has been changing as a result of the extension of the public sphere in two main directions: the growth of the media space leading to greater competition between ideas and the masses' increasing reliance on media, and cyberspace

[32] Amal Kheiri, "Israel and Internet Piracy: A New Round of Cyber Warfare," *Alamat Online*, April 11, 2013, http://www.alamatonline.net/l3.php?id=56608.

[33] Anthony Jurji, "The First Successful Cyber Warfare Sortie against Israel," *Al-Khalij*, April 18, 2013. http://www.alkhaleej.ae/portal/e0c8722a-ca8c-4255-b0c2-27695b3b3a54.aspx. Also see Kheiri, "Israel and Internet Piracy."

[34] Saeed, "Cyber Wars," May 28, 2012.

as a new conflict zone. [35] This situation has prompted many countries to follow global developments in this field and better prepare themselves to confront this new challenge by improving their ways and means to defend cyberspace. Modern states and advanced armies are concentrating their efforts on cyberspace, which they have used to empower them, but they still remain vulnerable. For example, states' vital infrastructure (e.g., electricity, water, and transportation), military command, control networks, and modern advanced battlefield technology are all dependent on cyberspace.[36]

Along with the changes in lifestyle brought by the blooming of the internet, material objects have also changed. Warfare is no exception and with technological evolutions it has taken a new trajectory.[37] Some consider that if land, sea, and outer space were the conventional theaters of war throughout history, then cyberspace is the real space of electronic warfare. International parties struggle and compete to exploit this domain for their own interests. The arenas for cyberwar may extend from the computer screen to the bottom of the ocean and the far reaches of outer space, with the most advanced computer technologies used, such as surveillance and detection, command and control, blockage and deception, and target location and targeting.[38] The potential to cause partial or total destruction to websites targeted by cyberattacks is an integral part of the approach adopted by hackers against systems they target or spy on.[39]

Financially, cyberattacks cost the global economy an estimated one trillion dollars a year.[40] Many states are involved in this complex scene in which offensive and defensive capabilities have developed together in the context of a new form of arms race.[41] Other

[35] Ezzat, "Self, Space, and Time," p.31.

[36] "War in Cyberspace," 2012.

[37] Abu al-Hajjaj, *Infamous Computer and Internet Crimes*, p. 164.

[38] "Anonymous: Cyber Fun or a Cyber Army Upsets Theories of Physical Organized Armies," http://www.shofakhbar.com/articles/4661566/.

[39] al-Zaro, *Cyberspace*.

[40] Kanik, "Internet Governance in an Age of Cyber Insecurity," p. 13.

[41] At times, states are behind cyber-attacks, forming part of an alternative to direct military strikes and target IT systems of the enemy. An example of this happened in 2008 when Russia wanted to counter the cyberattacks that it claimed Georgia was launching against it. Russia did not turn to government IT experts, but to cyber militias that attacked Georgian IT systems. This meant Russia faced no legal liability. This is an example of how major states nurture cyber militias for use when needed. Penetrating

states have opened training camps for military personnel in preventative or strategic attacks using high tech tools.[42] It is, therefore, quite clear why the topic of the moment is cyberattacks when the cost of direct and indirect damage, in the short and long term, is commensurate with that caused by missile or aerial attacks.

The US Department of Defense (DOD) is particularly interested after its recognition of Chinese superiority in this field. Other states have made the same observation, notably South Korea and major European nations. On this basis, at the end of 2012, the US DOD decided to fund the Defense Advanced Research Projects Agency (DARPA) project, known as Plan X, to develop advanced and revolutionary internet technologies capable of understanding, planning, and directing battles over the Internet. Furthermore, in August 2012, the US Air Force announced that it was seeking new ideas on how to "destroy, prevent, corrupt, disable, deflect, stop, or muzzle the capacity of enemies to use the Internet to their advantage."[43] The United States Cyber Command was only formed in 2010, much later than its EU counterpart, the European Network and Information Security Agency, which was established in 2004, and whose military role was advanced in 2010. The UK developed its own independent capabilities in 2010.[44]

The ongoing race between countries to assemble virtual armies and confront this challenge is worth noting. A number of states have developed the capacity to mount advanced offensive cyber operations, while more than 100 countries have formed cyber warfare units.[45] With regard to the Arab states, analysis points to a range of efforts in this field, most of which are secret, with indications that Morocco is one of the most advanced in this respect. Gulf countries are also concerned about exploring this field given the challenge posed by accelerating Iranian capabilities and the Iranian readiness

systems with the aim of spying is usually linked to groups backed by the state. Chinese hackers attacked the networks of the Indian Ministry of Defence and obtained Indian army secrets. India discovered what was going on very belatedly and went on to create what it termed a defensive weapon against cyberattacks to protect its military secrets. See Kheiri, "Israel and Internet Piracy."

[42] Jurji, "The First Successful Cyber Warfare," April 18, 2013.

[43] Ibid.

[44] Ammar Bakkar, "Will World War III be Virtual," *Al-Sharq*, no. 37, January 10, 2012. https://www.alsharq.net.sa/lite-post?id=79506.

[45] McAfee, Inc. "Virtually Here," p.13.

to use these capabilities against any Arab state to further its expansionist, ideological agenda. Regional analysts note that this is likely to drive Arab developments.[46]

The race between countries is not limited to the manufacture of missiles and fighter jets. It includes the development of systems to protect sites from hacking. Despite this, even though the length of attacks have been successfully curtailed at times, and the restoration of the sites compromised had been quicker, the deflection or prevention of cyberattacks has not broken through in the virtual or real world.[47] There is no doubt that the cyber-attack experienced by the Iranian nuclear program in 2009 represents the enormous latent power of cyber weapons deployed across cyberspace; this should be seen as a key event in cyberspace's development into a battle zone. In this context, a number of cyberattacks, and the preparations some states have made, in cyberspace demonstrate that the cyber arms race has begun. Over recent years, various states have set up agencies and departments to deal with cyberspace as a battle zone. Security strategy has also been formulated for this space in the US, UK, France, Germany, and China, which has devoted a branch of the PLA to round-the-clock fighting on the Internet to obtain American intelligence information.[48]

Currently, many countries have started to launch offensive cyberattacks under the separate but related cover of espionage or battlefield preparation. Actions such as tampering with electricity networks to be able to disable them during time of war, cause instability and make it more likely that the conflict moves beyond cyberspace and into the real world. Such operations are not restricted to states alone. Rather, they can be carried out by individuals, groups, and organizations. Cyberattacks can become a form of protest, as is the case with Anonymous. This reflects the extent to which cyberspace has entered the heart of the strategic actions of states. It also reveals that such virtual attacks are a highly strategic affair and possibly at the heart of the national security of states.

[46] Bakkar, "Will World War III be Virtual."

[47] "Cyber-attacks against Israeli Websites," *Al-Jazeera Net*, April 8, 2013. http://www.aljazeera.net/programs/pages/dcf90ad4-7e85-4e4c-962e-7d6a2c063e31.

[48] For more detail see, "Hot Internet War between China and America: The Hackers of Unit 61398 as a Strategic Challenge to the Pentagon," *Al-Hayat*, May 12, 2013. http://alhayat.com/Details/512581.

Israel at the Heart of Cyber Conflict

Anonymous has carried out a succession of coordinated attacks against websites and pages belonging to Israeli government, security, and media bodies. However, the attack on April 7, 2013 was one of the most powerful and extensive. It looked like war had broken out in cyberspace as thousands of Arab and foreign hackers attempted to wipe Israel off the Internet in response to its policies toward the Palestinians.[49]

The challenge posed by the hacking of IT systems is not limited to specific states but applies to many of them, including Israel, causing tangible and intangible losses and leading Israel to amass an army of experts and technicians to confront them. It's sensitivity and fear of hackers lies in its understanding of the power hidden in such attacks on its cyberspace, and the fact that Israel carries out such warfare on a wide scale as part of its efforts to achieve tactical and strategic objectives. This has led to different readings of the methods in the Arab-Israeli struggle in the region, starting from the possibility of using technology and cyberspace effectively in wars where the mind is in charge.[50]

On April 7, 2013, a group of hackers launched their second largest attack, against official, business, and social websites in Israel. These groups, with the assistance and coordination of Anonymous—itself deemed an ally of WikiLeaks and included on *Time* Magazine's list of the most influential groups in the world[51]—sent a message to the world via a video clip on YouTube, stating that the most powerful hackers from across the world decided to unite in one body in solidarity with the Palestinian people and wipe Israel off the Internet.[52] The video clip featured a person wearing the mask of the group, who outlined the stages of the attack as removing Israel from the Internet and discovering its

[49] "Message from Anonymous to the Zionists," YouTube Video, April 7, 2013.

[50] Ali Badwan, "Israel and Cyber War," *Al-Bayan*, July 17, 2012, http://www.albayan.ae/opinions/articles/2012-07-17-1.1689715.

[51] Bassam al-Qantar, "Anonymous: Keeping the Keyboard Awake," *Al-Akhbar*, April 8, 2013, http://www.al-akhbar.com/node/180791.

[52] "Message from Anonymous to the Zionists," YouTube Video, April 7, 2013.

plans for future crimes. The third stage was not revealed but would be, “a present from Anonymous.”[53]

These cyberattacks, under the tag #OpIsrael, took the form of distributed attacks and delivered a digital blow to Israel. Such an advanced technique as the one employed by Anonymous worries those concerned about the Internet and digital networks. Hackers involved came from many countries, including Palestine, Lebanon, Algeria, Iran, South Africa, France, the US, Albania, Kosovo, Morocco, Turkey, Indonesia, Tunisia, Egypt, Saudi Arabia, and Jordan. The attack succeeded in disrupting or crashing dozens of Israeli websites. The date of the attack, April 7, also coincided with Holocaust Memorial Day. The attackers’ message to Israelis claimed that the Holocaust was fabricated by them and their partners and that they had made the world believe in the Jewish Holocaust.

The attack targeted important websites in Israel and succeeded in disrupting sites in the Israeli government, army, and military, such as the sites of the prime minister, the defense ministry, the intelligence service, the cabinet, the stock exchange, the courts, the Tel Aviv police, the Kadimah Party, the education ministry, the Jerusalem Bank, around 20,000 Facebook accounts, and 5,000 bank accounts.[54] Anonymous published the personal details of more than 5,000 Israeli officials, including their names, ID numbers, and personal email addresses. They also released data on more than 600,000 Israeli internet users. The hackers left messages in support of the Palestinians, songs, and criticisms of Israeli militaristic policy on the websites, sections from the Quran on occasion, and photographs of Palestinian prisoners, including one of Samir al-Eissawi, who was on hunger-strike at the time. In this way, the crimes of the Israeli occupation were placed before the world.[55]

Intense political, economic, military, and media debate within Israel followed the cyberattacks, with Israeli media reporting on security readiness and e-security against such attacks and the expected material losses. Despite Israeli readiness for such attacks,

[53] The text of the message from the attacking group to Israelis states is: “You have not stopped violating human rights and illegal settlement, you have not respected the cease-fire, nor do you respect international law.” See “hacker,” YouTube Video, April 7, 2013.

[54] For more detail on compromised sites see: http://www.israj.net/arabic/index.php/2011-05-14-07-15-55/2011-05-14-07-16-17/2011-05-14-23-52-51/7087-7-2013.

[55] “Anonymous Launches Most Violent Cyber-Attack against Israel,” April 7, 2013. For more on the extent of losses, see: Humaidan, “Anonymous disrupts Israel’s Internet,” April 8, 2013.

this was the most powerful attack of its kind—ten-times more powerful than a similar one Israel faced during its Pillar of Cloud military operation against the Gaza Strip in November 2012. In that attack, less than 150 websites, organizational or private, were damaged for up to a few hours, while only two or three sites suffered more prolonged damage.[56] The number of small business sites in Israel disrupted by hackers reached the hundreds and perhaps more.[57]

Another attack occurred on June 28, 2011, when Anonymous leaked a message onto a number of websites containing a cyber-attack against the official website of the Israeli Knesset, disrupting it for a few hours. Because Israel has launched cyber warfare against Iran and Lebanon (e.g., its launch of the Stuxnet virus against Iranian nuclear facilities and its disruption of a Lebanese communications company using its agents),[58] Anonymous took this as an attack against itself. The group sent a video message where it used voice distortion software to read the following message: "To the noble people of Palestine: for the past 65 years you have been forced to live under inhumane conditions by the illegal Zionist regime [...] Anonymous are your brothers and sisters, your sons and daughters, your parents and your friends, regardless of age, gender, race, religion, ethnicity or place of birth. Anonymous is you. United we are strong. Join us in this battle for freedom of information worldwide [...] We do not forgive. We do not forget."[59]

In 2011, a group from "Anonymous Egyptians" implemented Operation Netanyahu that attacked the website of Israeli Prime Minister Benjamin Netanyahu in revenge for the killing of Israeli soldiers on the border. The site and other Israeli sites were brought down.[60] In 2012, a nineteen-year-old Saudi citizen calling himself OXOMAR managed to hack websites of individuals and banks, thereby obtaining and publishing the credit card details of tens of thousands of Israelis, enabling anyone who wished to make purchases

[56] Humaidan, "Anonymous disrupts Israel's Internet," April 8, 2013.

[57] Madar Center, "Despite Assurances that the Attack Was Repelled," April 9, 2013.

[58] In April 2012, Iran accused both Israel and the US of compromising the computer systems at the Busheir nuclear reactor and infecting them with the Stuxnet virus that affected the Iranian nuclear reactors.

[59] "Anonymous—Operation Palestine," March 1, 2011.

[60] Abu Talib, "Anonymous."

on the internet using these cards.[61] On January 17, 2012, *Yedioth Ahronoth* revealed that this Saudi youth had tried to hack into sensitive Israeli websites, including those for infrastructure and government ministries and departments. The newspaper added that the young man confirmed he had acted to take revenge against Israel for its killing and mistreatment of Palestinians, and that the 2008-2009 Gaza war was the catalyst.[62]

After the Turkish Freedom Flotilla incident at the end of May 2010, around 1,000 Israeli sites were hacked by Turkish hackers.[63] On November 29, 2010, an Iranian nuclear scientist was assassinated in Tehran and another injured. Two days later, the network of the Israeli mobile phone company Cellcom went down for hours following a cyberattack.[64] On January 25, 2011 the Israeli Bezek telephone network also crashed for several hours, and though some in Israel spoke of a technical fault, others deemed it a cyberattack on the network.[65]

Israeli Capabilities in Cyberspace

Cyber warfare has become one of the main tools used by the Israeli army to realize its strategic objectives. The Israeli perception is that the next war will be cyber. Alex Fishman, an Israeli military correspondent, claimed that Tel Aviv is making serious preparations out of the concern that sensitive systems could be hit by viruses and paralyzed at the most critical moment. This seemed justified given that "enemies" had managed to take control of a number of systems over recent years and made technical leaps in terms of cyber warfare, which he termed "the shadow war" between armies at the heart of enemy information on a fluid front employing heavy weaponry akin to a global chessboard where the best minds are in combat.[66]

As a result there have been calls from the security establishment and the Knesset Foreign Affairs and Defense Committee for a reformulation of Israeli security policy laid down in

[61] Ghazi Hamed, "Cyber Jihad: the new war against Israel," *Filistine*, April 8, 2013.

[62] Shahboun, "Cyber wars."

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] Adnan Abu Amer, "Israel and Internet War," Al-Jazeera Net. http://www.aljazeera.net/opinions/pages/910f8b7d-b7d0-4ac1-b875-78cca8d77c8e.

the early 1950s so as to correspond to this new form of warfare over which Israel has started to obsess. A number of simulations in this field have been run, and the results confirmed the danger posed by the potential compromising of sensitive websites in Israel. For this reason, there have been efforts to mobilize human and material resources to support such programs.

General Amos Yadlin, former head of the Military Intelligence Directorate, dealt with the subject in a lecture he gave at the Institute for National Security Studies at Tel Aviv University in December 2009. He stated, "The Israeli Army is determined to provide good protection for networks and to launch cyberattacks." The cyber division of the army may help protect Israeli cyberspace, as does the US cyber command, but it is not the body dedicated to providing complete national protection to the state's cyberspace.[67]

The available literature for research on this subject remains scanty and does not deal openly with Israel's strategy and doctrine toward cyber security. In terms of the preparations undertaken by Israel to defend its cyberspace, a number of important markers can be indicated:

1. Israeli Army Unit 8200 focuses on three aspects of cyber warfare: intelligence gathering and electronic offense and defense.

2. The internal security service, Shin Bet, is charged with the defense of Israeli government computer systems, the state's electronic infrastructure, and information relating to the banking system. This has been the case since the end of the 1990s. Shin Bet is also active in internet and network warfare. It is considered an attractive place to work for Israel's best technological minds. It is also ranked in the top six units world-wide for launching internet attacks.[68]

3. The Israeli Army has around 300 young computer experts working on the Internet. Thirty staff have been seconded to various branches of the Internet to monitor networks. It is thought that Unit 8200, which grew out of the structure of the monitoring apparatus, is at the heart of this force.[69]

[67] Even and Siman-Tov, "Cyber Warfare: Concepts And Strategic Trends".

[68] Jurji, "The First Successful Cyber Warfare," April 18, 2013.

[69] Yusuf Bughanemi, "Anonymous: Toying with the Internet or a cyber army that has overturned the doctrine of the regular standing army," *Marrakech Press*, April 10, 2013. http://www.marrakechpress.com/?p=6279.

4. The C4I Corps is responsible for communications and the organization and coordination of Israeli cyber defense capabilities.[70] A senior intelligence officer was assigned to the Centre for Encryption and Information Security (known by the Hebrew acronym MATZOV) with responsibility for providing intelligence on technological advances among Israel's adversaries in the field of computer hacking. MATZOV is responsible for writing the codes that encrypt the Israel Defense Forces, Shin Bet, and Mossad networks. The C4I Corps has teams that test firewalls and encryption.[71]

5. In 2012, the Israeli National Security Institute established a training program in cyber security. The Institute issued a detailed report on cyber warfare in May 2012 in which it recommended that the Israeli administration develop offensive and defensive capabilities, undertake national and international training, raise the state of alert, and incorporate IT security into Israel's strategic defenses.[72]

6. In March 2011, the government approved the creation of the IT Systems Directorate (MINMAR). This is a cross-ministry body tasked with coordinating electronic communications within government. Under the general director of the Ministry of Finance, it is supposed to guide electronic communications units within government ministries, and is directly responsible for all government computerization programs.[73]

7. On March 27, 2011, the Israeli government approved the creation of the Information Management Unit under the director general of the Ministry of Finance. It is directly responsible for all government computer communications systems, including the program for Government Infrastructure for the Internet Age.[74]

8. Israel created a new government agency, the National Cybernetic Taskforce, on May 18, 2011 to secure the country against the hacking of critical networks, as well as to protect private industry from espionage. It will be an 80-member team and operate in a defensive capacity. The taskforce will also devote resources to

[70] Lewis and Timlin, *Cyber Security and Cyber Warfare*, 2011.

[71] Ibid.

[72] Kheiri, "Israel and Internet Piracy."

[73] Madar Center, "Paragraphs from a Memorandum p. 7.

[74] Ibid.

improving university research on cyber security and increasing the number of students in such programs.[75]

9. In 2002, the Information Protection Authority of the General Security Service (Shabak) was set up, and is responsible for providing professional guidance to relevant bodies regarding the protection of vital computer networks from terrorist threats and damage in the area of classified information and threats of espionage and disclosure.[76]

10. In 2009, Israel launched the new Digital Iron Dome under the aegis of the National Cyber Bureau. According to Netanyahu, the program exists to support Israel's cyber capabilities by dealing with cyberattacks, and is recruiting outstanding high school students and asking them to repel the cyberattacks against Israel.[77]

11. The Israeli Army's Cyber Division was formed in 2009 after General Gabi Ashkenazi described cyberspace as a strategic battleground to coordinate and guide activities in cyberspace.[78]

12. In 1997, the Government Infrastructure for the Internet Age (TEHILA) project was set up. Under the public comptroller of the Ministry of Finance, the project aims to provide secure browsing services for government ministries and departments. TEHILA uses a range of mechanisms to secure government networks, starting with a team of IT security experts and ending with products and technologies from leading international companies. Within the scope of TEHILA, there is also the Centre for the Security of Israeli Government Information whose tasks include the monitoring of incidents concerning information security world-wide, observing attacks within networks linked to Israel, coordinating between government agencies to solve problems of information security, coordinating relations with agencies and outside bodies, and undertaking research and development in this field. The Centre issues

[75] Lewis and Timlin, *Cyber Security and Cyber Warfare*.

[76] Ibid.

[77] "Netanyahu: We're Building a Digital Iron Dome," *The Jerusalem Post*, January 1, 2013. http://www.jpost.com/DiplomacyAndPolitics/Article.aspx?id=298023.

[78] Muhareb, "Israel and Cyber Warfare, September 22, 2011.

> information security warnings to organizations working in the IT field that are linked to TEHILA or to non-classified government agencies.[79]

The Economic Importance of IT and Cyberspace to Israel

Israel is considered among the world's most advanced nations in the field of ICT. Israel tried to use the recent cyber-attack against it "to encourage companies to strengthen precision industries, develop information security systems, and attract foreign investors to open additional companies to manufacture, innovate and market IT systems, which will help boost the stagnant Israeli economy."[80] According to a study conducted by the international consultancy firm McKinsey, the internet economy in Israel is divided into two areas. The greater part is focused on the ICT industry and comprises the production and sale of equipment, software, and services. The smaller part, which is experiencing rapid growth, concerns e-commerce.[81] According to the study, the direct contribution (to production) made by the internet economy in Israel reached around 50 billion shekels in 2009, around 6.5 percent of GDP.[82] This places Israel in the leading ranks of the world's internet economies.[83]

Cyberspace, undoubtedly, forms a major concern inseparable from Israel's security strategy. This space has been incorporated into operational security and military efforts.[84] The aim meets several goals: lessening its geographical isolation in the Middle East, forming good relations with the world, and strengthening the links between Israel's center

[79] "Cyber Warfare: Concepts And Strategic Trends."

[80] "Cyber Warfare boosts the Israeli IT industry," *Palestine Today Agency*, April 15, 2013, http://paltoday.ps/ar/post/165435.

[81] "Cyber Warfare: Concepts And Strategic Trends."

[82] Ibid.

[83] Ibid.

[84] It is worth pointing out that in 2009, Israel, in cooperation with the US, used the Stuxnet virus to cause damage to the centrifuges relied on by Iran for uranium enrichment. Then in June 2012, it launched a cyberattack against sensitive Iranian computer systems using the Flame virus. Israel also hacked into the command systems of the Syrian Air Defenses on the eve Israeli jets raided the Syrian nuclear facility near Deir Zor in northeast Syria in September 2006. These systems were disabled, thus minimizing the chances of the raiding planes having to face Syrian Air Defense fire.

and periphery. This last forms a key element in social policy and is a main factor in strengthening the link between the authorities and citizens.[85]

The Significance of Cyber Attacks on Websites in Israel

Anonymous carried out its threat on April 7, 2013, and despite the limited nature of the strike and its impact, which Israel downplayed,[86] it was able to significantly impair the prestige of one of the most technologically and informationally advanced nations. Despite their limited nature, these attacks sent out multiple messages. The first message is political. The Palestine question lives on among Arab youth, who were able to add a new form of resistance to the Arab-Israeli conflict by harnessing the Internet to that end. The issue lives on in their hearts and minds, virtually and on the ground. The second is technological. Israel can be damaged by virtual means, and its capabilities were exposed. The Digital Iron Dome has shortcomings. There are other parties, be they states or individuals, capable of causing it damage.

The third message was for the military. Israel and its "invincible" army are not the only party able to carry out cyberattacks of this kind against the countries of the Arab and Islamic world. The increase in cyberattacks and their proliferation over the Internet, and the systematic targeting of Israeli infrastructure—such as the water and electricity supply, traffic lights, energy and banks—and the theft of sensitive security information all represent a threat to be added to the list of theoretical threats to Israeli security. Israel may be able to defend its geographic borders, but things are different when it comes to cyberattacks because they go beyond geography, need little time, and do not cross borders. Israel is thus preparing itself to repel such attacks. Such attacks could be repeated again and again in light of the global growth in cyberattacks anticipated in future.

The question posed in Israel today is: What will we do if there is coordination and expansion of cyberattacks with the participation of a very large number of hackers all over the globe, who could potentially flood its systems by crashing the network, along with its production and services?

[85] "War in Cyberspace."

[86] Anonymous estimated the damage caused by the attack against Israeli institutions and websites at around 3 billion US dollars. Israel stated, however, that the impact of the attack was limited. "Anonymous: We cost Israel 3 billion dollars," April 8, 2013.

Conclusion

Cyberspace has become a new battlefield forming an additional threat on the list of conventional threats faced by our world today. The extent of its impact transcends geographical and political borders, and the ramifications for the future vital national security of countries is significant. Hackers can now flood servers with requests from various systems, thereby paralyzing their operations and stopping production systems. Many of the world's advanced armies have increased their activities and intensified efforts in this field, and have revealed a number of vulnerabilities—electricity, water, transportation, command and control systems, military command and advanced battlefield technologies; these are all reliant on cyberspace. On today's Internet, systems crash, institutions are hacked, and presidents fall. This is not surprising when confronted with a war not controlled by states and their security apparatuses, a war that does not recognize conventions or treaties, and whose virtual heroes are individuals and groups similar to "sleeper cells" that activate when desired and return to dormancy when desired.

Bibliography

Abu al-Hajjaj, Yusuf. 2010. *Infamous Computer and Internet Crimes*. Cairo: Arab Book Publishers.

Abu Talib, Ahmed. January 1, 2012. "Anonymous: Political Hacktivism in Cyberspace." *Digital Ahram*. http://digital.ahram.org.eg/Policy.aspx?Serial=780539.

al-Khouri, Tanya. Autumn 2011. "We Are All Eye-Witnesses: The Arab Spring in Pictures and Cyber Warfare." *Journal of Palestine Studies* 88.

al-Rashidi, Mahmoud. 2012. *The Internet and Facebook: The January 25 Revolution as a Model*. Cairo: Egyptian-Lebanese Publishers.

al-Zaro, Hassan Muzzafar. 2007. *Cyberspace*. Beirut: Centre for Arab Unity Studies.

al-Zaydi, Bassem Hussein. January 31, 2012. "Hackers: Pirates of the Cyber Age." *Annabaa Information Network*. http://www.annabaa.org/nbanews/2012/01/313.htm.

Ali, Nouran Shafiq. June 10, 2013. "Virtual Activists: E-clashes between political forces after the Arab revolutions." *Al-Siyasa Al-Dawliya*. http://www.siyassa.org.eg/NewsQ/3137.aspx.

"Anonymous Launches Most Violent Cyber-Attack against Israel." April 7, 2013. http://www.tech-wd.com/wd/2013/04/07/opisrael.

"Anonymous—Operation Palestine—Short Press Release." YouTube Video. Posted by Anonymousworldwar3. 1:32. March 1, 2011. http://www.youtube.com/watch?v=2-zXF1DVNDY.

"Cyber Espionage and Hacking Directed against Countries: 2013's Main Challenges." December 10, 2012. *Al-Iqtisadiya* (Saudi Arabia). http://www.aleqt.com/2012/12/10/article_715862.html.

Even, Shmuel and David Siman-Tov. "Cyber Warfare: Concepts And Strategic Trends." http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=152953.

Ezzat, Hiba Raouf. January 2012. "Self, Space, and Time: From the Public Sphere to the Political Street." Trends Supplement to *Al-Siyasa Al-Dawliya*.

Ghaneim, Emad. October 25, 2010. "Deadly virtual warfare." *Digital Ahram*. http://digital.ahram.org.eg/articles.aspx?Serial=340346&eid=601.

"hacker." YouTube Video. Posted by Infoprogramme, 2:38, April 7, 2013, http://www.youtube.com/watch?v=0_rEQKUpsUc.

Humaidan, Mashal. April 8, 2013. "Anonymous disrupts Israel's Internet with 44 million attacks." *Al-Iqtisadiya*. http://www.aleqt.com/2013/04/08/article_745515.html.

International Telecommunication's Union. 2013. "Cybersecurity." http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

Kanik, Robert. 2011. "Internet Governance in an Age of Cyber Insecurity." *International Studies Series* 95. Abu Dhabi: Emirates Center for Strategic Studies and Research.

Lewis, James A. and Katrina Timlin. 2011. *Cyber Security and Cyber Warfare, Preliminary Assessment of National Doctrine and Organization*. Center for Strategic and International Studies (CSIS). http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

Madar Center. April 9, 2013. "Despite Assurances that the Attack Was Repelled, Israel Declares the Recent Cyber-Attack Was Strongest to Date." *Al-Mashad Al-Isra'ili* (special issue). http://www.madarcenter.org/pub-details.php?id=441.

——. October 23, 2012. "Paragraphs from a Memorandum on Israel's Preparations to Confront the Age of Cyber Warfare." *Al-Mashad Al-Isra'ili* 292. http://www.madarcenter.org/mash_had_pdf/.

McAfee, Inc. 2009. "Virtually Here: The Age of Cyber Warfare." *McAfee Virtual Criminology Report*. http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf.

"Message from Anonymous to the Zionists-2013." YouTube Video. Posted by Anonymous Arab. 2:38. April 7, 2013. https://www.youtube.com/watch?v=FPbjIS-GDHU&feature=player_embedded.

Muhareb, Mahmoud. September 22, 2011. "Israel and Cyber Warfare: A Review of *Cyber Warfare: Concepts, Trends, and Implications*." *ACRPS*.

http://english.dohainstitute.com/release/c82f6a5e-6ba7-40c0-ba42-819b34167108.

Rahuma, Ali Muhammad. 2005. *The Internet and the Socio-Technical System: An Analysis of the Technology of the Internet and the Model of Its Social System*. Beirut: Centre for Arab Unity Studies.

Saeed, Fahd. May 28, 2012. "Cyber Wars." *White Hats Community*. http://www.whit3hats.com/?p=2775.

Schreier, Fred. 2012. *On Cyberwarfare*. The Geneva Centre for the Democratic Control of Armed Forces (DCAF). http://www.dcaf.ch/Publications/On-Cyberwarfare.

Shahboun, Adil. June 4, 2011. "Cyber Wars: The New International Battleground." *Digital Ahram*. http://digital.ahram.org.eg/articles.aspx?Serial=528342&eid=1103.

Slobbe, J. and S.L.C. Verberkt. July 22, 2012. "Hacktivists: Cyberterrorists or Online Activists?: An Exploration of the Digital Right to Assembly". http://arxiv.org/pdf/1208.4568.pdf.

Verwoerd, Theuns. November 5, 1999. "Honours Report: Active Network Security". Ray Hunt (Supervisor). Canterbury University. http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/1999/hons_9909.pdf.

"War in Cyberspace". Winter 2012. Translated by Saeed Ayash. *Israeli Affairs Journal* (*Qadaya Isra'iliya*) 43-44.

Yunus, Omar bin. 2010. *The Information Society*. Beirut: Arab Encyclopedia House.