Cyberspace and National Security

Selected Articles III

Edited by Gabi Siboni

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Cyberspace and National Security

Selected Articles III

Edited by Gabi Siboni

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Graphic design: Michal Semo-Kovetz
Printing: Elinir

Institute for National Security Studies
(a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556

Tel. +972-3-640-0400
Fax. +972-3-744-7590

E-mail: info@inss.org.il
http://www.inss.org.il

April 2015

ISBN: 978-965-7425-76-3

INSS Institute for National Security Studies

The Institute for National Security Studies (INSS), incorporating the Jaffee Center for Strategic Studies, was founded in 2006.

The purpose of the Institute for National Security Studies is first, to conduct basic research that meets the highest academic standards on matters related to Israel's national security as well as Middle East regional and international security affairs. Second, the Institute aims to contribute to the public debate and governmental deliberation of issues that are – or should be – at the top of Israel's national security agenda.

INSS seeks to address Israeli decision makers and policymakers, the defense establishment, public opinion makers, the academic community in Israel and abroad, and the general public.

INSS publishes research that it deems worthy of public attention, while it maintains a strict policy of non-partisanship. The opinions expressed in this publication are the authors' alone, and do not necessarily reflect the views of the Institute, its trustees, boards, research staff, or the organization and individuals that support its research.

Contents

Foreword

Israel's rapid development as a leader in cyberspace places it in a unique position to advance cyberspace research in Israel in general and at the Institute for National Security Studies in particular. In order to expand research and the scope of cyberspace activity, and given the fact that cyberspace does not recognize national or institutional boundaries and borders, we at the INSS have decided to extend the program and hold the annual cyberspace security conference in the United States. The Defensive Cyberspace Operations & Intelligence (DCOI) conference highlights core issues of security and defense in cyberspace and its related intelligence aspects. The conference, held this year in Washington D.C., is the product of collaboration between several institutions in Israel, the United States, and other countries.

The conference's focus on defensive operations and intelligence allows the INSS to showcase its own activity in this field and complement the range of operations carried out in Israel and around the world. The objectives of this year's conference are manifold: developing the discourse of defense in cyberspace, the corporate and financial fields as well as in the field of critical infrastructures; enhancing cooperation among government bodies and institutions working in the field of cyberspace in Israel and the United States; exposing the Israeli cyberspace and technology market to foreign technological companies seeking to develop business with Israel and/or seeking to expose Israeli capabilities and technologies abroad; enhancing international cyberspace cooperation with friendly nations, etc.

As is our custom every year, we offer those interested in cyberspace this unique publication, which brings together some of the products of cyberspace research and essays published by the INSS Cyber Security Program. The essays in this journal have been published in *Military and Strategic Affairs* and represent the efforts of INSS researchers and outside researchers working in tandem with its cyberspace program.

Gabi Siboni
Editor

The Islamic State's Strategy in Cyberspace

Gabi Siboni, Daniel Cohen, Tal Koren

The success of the Islamic State (henceforth: ISIS) includes the integration of interrelated elements in a way that helps the organization consolidate its control of extensive regions, serve as the current spearhead in the global Jihad effort, and threaten the world with terrorist attacks carried out by its agents holding citizenship in a Western country. These agents are liable to return to their homeland and along with "lone wolves" they are liable to carry out terrorist attacks against targets in the West. The aim of this article is to examine ISIS's model, as it is an organization that has successfully conquered many geographic areas while attracting public attention on an unprecedented global scale. The article will attempt to assess the organization's unique strategy, which combines two key interrelated elements: extensive use of the social media on the one hand and extreme and savage cruelty on the other.

Keywords: Islamic state, ISIS, social media, Iraq, Syria, terrorism

Introduction

In May 2004, an Islamic website published a video clip showing the execution of Nick Berg, a U.S. citizen, in Baghdad. The clip showed Berg in an orange prisoner's uniform (the same worn by prisoners at Guantanamo Prison), beheaded by Abu Musab al-Zarqawi, the leader of al-Qaeda in Iraq. Ten years later, this video assumed horrifying historical significance with the publication of a video clip showing the beheading of American James Foley by agents of ISIS, carrying on the actions of Abu Musab al-Zarqawi.

Dr. Gabi Siboni is a senior research fellow and the head of the INSS Cyber Security Program. Dr. Tal Korn is a research fellow in the Cyber Security Program. Daniel Cohen is a Research Fellow and coordinator of the Cyber Security Program.

This article was first published in *Military and Strategic Affairs* 7, no. 1 (2015).

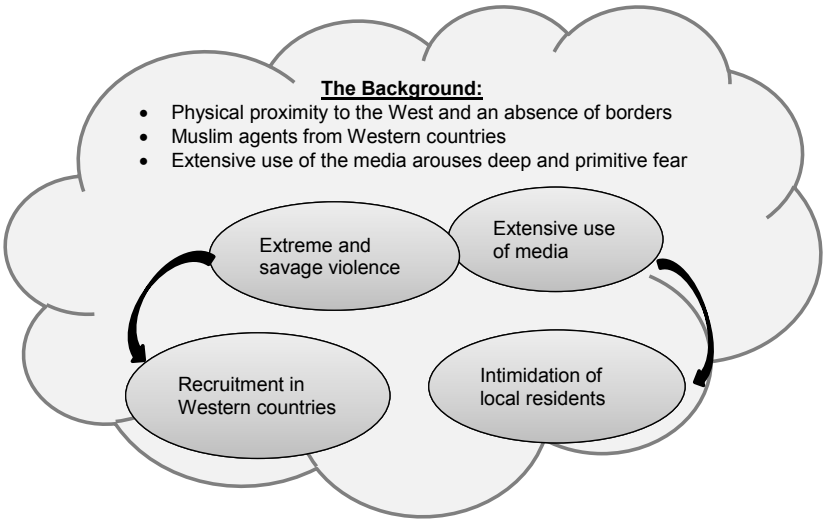
The main difference between the two video clips is that the man who beheaded Foley spoke fluent English, and the professionally edited clip was spread virally throughout the entire world. Viewers in Western countries experienced a feeling of horror at the sight of a prisoner being led to the slaughter, not only because the victim seemed like their next-door neighbor, but because the slaughterer also represented the image of a neighbor. ISIS uses the global village of the information era, in which the boundaries between reality and imagination have been blurred using technological means available to everyone, in its call to its supporters in the West to make the hegira (immigration to the Islamic state) or join the jihad - "pack your suitcases or prepare explosive devices."

Psychological warfare in the service of terrorist organizations is not a new phenomenon. Carlos Marighella, one of the fathers of modern revolutionary terrorism, published The Mini-Manual of the Urban Guerilla in the 1960s, in which he referred to a war of "nerves" and psychological warfare. He asserted that governments will always be in a position of inferiority in combating psychological warfare used by a terrorist organization, as a result of the many resources used in counter efforts and censorship. According to Marighella, this investment is doomed to fail. In the digital and new media era, the challenges and threats have changed as a result of the new spheres in which a terrorist organization can operate to promote its political objectives. ISIS operates on a large scale in virtual space by using new media platforms that make censorship difficult. The position of inferiority in defending against this phenomenon is therefore significant, and requires observation and a solution to this threat that makes use of up-to-date tools.

The wave of spontaneous terrorist attacks ("lone wolves") in the U.S., Canada, Australia, Europe, and Israel highlights the emerging symbiotic connection between ISIS's recruitment calls, propaganda, and terrorism against Western civilians and the various communications platforms made possible by virtual space. It incorporates terrorism executed by veterans who fought within ISIS ranks in Syria and Iraq and returned to the west, such as the murder of Israeli couple Mira and Emanuel Riva at the Jewish Museum in Brussels in May 2014 by Mehdi Nemmouche, a French citizen of Algerian origin who returned to Europe after fighting with jihad forces in Syria. These local unorganized terrorist actions, carried out "under the influence of ISIS" and inspired by it, include attacks by shooting

and running over pedestrians in Canada, and attempted beheadings in Australia and the U.S. ISIS employs public relations, recruitment, and propaganda apparatuses in virtual space, including the publication of magazines and high-quality video clips that can be viewed by the international media with restrictions, and sells merchandise with the organization's symbol online. The organization's agents even document and share their comments on social networks. This mode of operation, which includes transparency and ruthlessness, is perfectly suited to the organization's current strategic policy: preparation for global terrorist activity by recruiting foreign agents and establishing new terrorist cells throughout the world. In "The Violent Image: Insurgent Propaganda and the New Revolutionaries," Neville Bolt says that the Islamic State has adopted the idea of "propaganda of the deed," similar to the old tactics used by revolutionary groups, in which violence and communications were merged in order to achieve the maximum effect in delivering a political message. He claims that what is unique about ISIS is its combination of distribution platforms in the media and the new media to display extreme and savage cruelty. This constitutes a new spectrum of "network warfare" involving exploitation of the information revolution. The organization uses reciprocal propaganda, and includes horrific pictures immortalizing terrorism, designed to generate fear and anxiety (such as video clips featuring beheadings), and as means for influencing decision-makers in the West.

The success of ISIS, which has consolidated itself over the past year in Iraq and Syria, and has established organizational infrastructure in North Africa and the Sinai peninsula, includes the integration of interrelated elements in a way that helps the organization consolidate its control of extensive regions and serve as the current spearhead in the global Jihad effort. In addition to posing a threat to the stability of Arab regimes in the Middle East such Saudi Arabia, Jordan, and Lebanon, there is also the threat of terrorist attacks carried out throughout the west by western citizens who have joined ISIS in Syria and Iraq and then returned home, and encouragement of spontaneous terrorist attacks against Western targets. The media and violence are used in tandem to both intimidate nearby enemies and to recruit agents and supporters. These actions, which are being conducted in places geographically proximate to democratic countries (the West), include extensive use of media on the one hand, and extreme and savage cruelty on a previously unseen scale on the other.



These elements are intertwined; aiming at a Western target group and the physical proximity to this target along with the appeal for recruitment of supporters from those countries generates a feeling of deep primitive dread among the general public, combined with a strong attraction among the audience of potential supporters.

This article asserts that ISIS's internet success is due to the connection between its use of extreme ruthless cruelty and the use of cyberspace to spread messages internally and externally for purposes of recruitment and intimidation. The background to this policy is physical proximity to the West and the creation of a deep feeling of dread in Western countries of being inundated with terrorists and supporters of Islamic-motivated violence.

ISIS makes intelligent use of social networks for delivering focused messages to specific target audiences, namely Muslim communities in Western and Asian countries. Up until now, ISIS's media strategy has succeeded in positioning the organization as the main enemy of the West, branding it as the spearhead in the global jihad struggle, winning support among Muslim audiences and jihad organizations.[5]

ISIS Propaganda and Recruitment System

ISIS, like al-Qaeda in its early days, recognizes the fact that it must operate simultaneously on a number of fronts in its war against infidels. The organization therefore regards its media strategy as representing "two thirds

of the battle,"[6] and regards the struggle over popular opinion as essential and complementary to its activity.[7] The importance of the media in it various forms as means of gaining influence, support, and sympathy from millions of Muslims around the world is evident in the organization's activities and the many resources invested for the purpose. The Internet and social networks are the chief means of disseminating its ideology and political messages, as well as means of recruiting foreign volunteers and financing, while being careful to control the flow of information from the battle areas. ISIS uses a number of online platforms,[8] such as the al-Furqan Institute for Public Relations Production,[9] which serves as the official media arm of ISIS and its leaders, and the "al-Athzam Agency for Media Production." This agency has been operating for the past two years, producing ISIS video clips and distributing them on the social networks. Another ISIS media arm is the Islamic State organization website, called the al-Hayat (Life) Media Center, which is aimed mainly at a Western target audience.

The al-Hayat media center contains a great deal of material about ISIS, including speeches and video clips translated into more than 10 languages. The website, which is aimed at the West and a non-Arabic speaking audience, combines content and diverse material with new video clips and subtitles for earlier video clips, in addition to articles, news reports, and translation of jihad material. The website is of high quality, and was probably designed by a team with experience in producing material for a Western audience. ISIS distributes bloody propaganda clips on the Internet, in which the organization showcases the cruel tactics used in its conquests in Syria and Iraq, while boasting the helplessness of its enemies. One of the propaganda films issued in September by the Islamic State, which was professionally edited as a documentary film, is entitled, "Flames of War: The Struggle Has Only Begun."[10] Its purpose is to deliver a clear message against U.S. intervention targeting the organization. The 55-minute film uses carefully designed romantic images, combined with special elements of explosions, battles, wounded American soldiers and those about to be killed, anti-American rhetoric, edited slow-motion segments of executions, and archive segments of Western leaders. The film includes sophisticated illusory elements (size, distorted pictures, enhancement of speakers, a speech lit by torches) resembling the 1934 propaganda film produced in Nazi Germany as a propaganda documentary move by Leni Riefenstahl, "Triumph of the Will."[11]

This movie joins a long series of professionally edited films documenting bombings, terrorist attacks, and assassinations of officials, military, and security forces personnel in Iraq. One example is the popular four-part series entitled "The Clanging of the Swords," the first part of which was distributed as early as June 2012. The series has gained widespread exposure on platforms such as Twitter and Facebook.[12] A comprehensive analysis of the fourth part of the Clanging of the Swords, aired on May 17, 2014, was published by Nico Prucha and Ali Fisher on the Jihadica website. It describes the level of sophistication demonstrated in the use of the social media and in the use of information distribution technology on various platforms, including cellular telephones (the preferred platform, especially the use of the "Twitter for Android" application), various web technologies, and file sharing websites (justpaste.it, archive.com), with the use of a different size and format, variable quality, and different languages (Arabic, Indonesian, English, German, and Japanese). It is no surprise that the video was released on Saturday as a deliberate strategy to prevent blocking by web companies, as their employees are on their day off. In the first 24 hours after the video was released, there were nearly 60,000 hits (the average viewing time was 17 minutes).[13]

In November 2014, a short film showing the beheading of 22 Syrian prisoners was published. The film was analyzed by the Terrorism Research and Analysis Consortium (TRAC), and the Quilliam Foundation think tank pointed out that the film was professionally produced, including many hours of filming, the use of HD cameras, and professional editing. The analysis concluded that the cost of producing this film was about $200,000.[14] The production of this film reflects the level of savagery as well as the level of sophistication. This film does not document an execution; it is a "reality" film of a mass execution carried out solely by "outside" soldiers recruited to the organization. The "extras" in the film are executed. This method shows the importance attributed by the organization to the use of media, and its profound understanding of the effect that such a film has on viewers; generating a feeling of "romantic" attraction for potential recruits on the one hand, and the creation of a feeling of terror and dread among Western citizens on the other.

In addition to violent material and content, some of its publications are designed to recruit new volunteers from Western and non-Arab countries. The al- Hayat Media Center, for example, published a number of original

video clips under the "Mujatweets" headline aimed at showing that life under the Islamic State was peaceful and normal, pointing to a positive aspect that would soften the brutal image of a murderous organization, and in order to attract new recruits.[15] In addition, a series of high-quality articles published as PDF documents, similar to al-Qaeda's "Inspire" online magazine, can be found on the website aimed at showing and emphasizing the organization's success on the battlefield and portraying prominent soldiers in its ranks. Some of the video clips were designed for the purpose of influencing public opinion by showing scenes of food distribution, medical treatment, and charity. The films have English subtitles, and are designed to convince Western professionals to come and help in the building of the Islamic state. The organization publishes something called the IS Report, which contain articles in English describing the founding of offices for the training of Imams, religious legal rulings, pictures of executions, and victories on the battlefield.[16]

In addition to the ISIS media apparatus distributing the organization's publications on the Internet, ISIS publishes a number of Internet magazines; the most important is the Dabiq periodical.[17] The first issue was published in July 2014 in a large number of languages, and resembled the al-Qaeda "Inspire" magazine in its design. The main emphasis in the first issue, which filled 50 pages and was entitled "The Return of the Calilafah," was to convince its readers of the legitimacy of the caliphate declared by ISIS leader Abu-Bakr al-Baghdadi, and to call upon Muslims from all over the world to come to "their natural country" under its leadership. The other three issues came out in September-October, and included quotations and remarks by senior officials in the organization, hadiths legitimizing slavery as "the spoils of war," information about building the Islamic State, calls for the killing of "Crusaders," justification of executions, etc. Another public relations activity designed to appeal to Muslim communities outside the war zones in Syria and Iraq was the English language "Islamic State News" Internet news magazine, which contained both regular reports about the organization and reflections with an Islamic Salafı-jihadist orientation.[18] ISIS conducts additional forums and official news sites in Arabic on the Internet, such as al- Minbar al- Ilami al- Jihadi[19] (Jihad Forum) and others with diverse propaganda content about ISIS.

For ISIS, the use of social networks is a platform constituting a significant lever enabling the organization to recruit broad support among the young

radical Muslim public in their countries of origin and in the West, while delivering focused messages. On the other hand, communications and messages between the global jihad organizations and their supporters, such as al-Qaeda, are usually deployed over the "dark web" that is not accessible to everyone, in mosques, and through distribution of leaflets and designated websites.[20] ISIS has therefore chosen to operate openly on the social media channels, including YouTube, Twitter, Facebook, and other less well-known social networks that appeal to a Western target audience and in Muslim communities in the West. ISIS is flooding social networks with especially savage and graphic materials of torture, mass execution, beheading, and crucifixion. As noted, however, this is only part of the broader picture. The use of social networks serves a number of purposes, such as psychological warfare and creating a deterrent effect on both a specific target audience in the battle zones and on Western public opinion, creating a presence and image of size in order to give the impression that the organization is larger than it actually is, disseminating ideology, obtaining financing, and calling for volunteers to join jihad, while distributing videos and interviews with Australian, European, and American Muslim citizens.

The organization's use of these networks is highly sophisticated, mainly in transmitting vicious propaganda messages that overshadow the media efforts of competing organizations, such as al-Qaeda and its affiliates. The efforts by Western countries to close accounts affiliated with ISIS and its supporters and censor their content almost never succeed. For example, the Islamic State organization used an application working on the Twitter network called "Dawn of Glad Tidings." Until not long ago, this application, which could be downloaded from the Google Play Store, facilitated automatic posts to the accounts of the organization's supporters. Another method is the use of Hashtag, which is used on social networks (such as Twitter, and Facebook).[21] ISIS uses "Hashtag Hijacking," which is a relatively simple method of implanting popular words, thereby gaining the attention of people looking for certain content. ISIS also uses advanced technologies, as noted in a recent special report published by the ZeroFox Company. This involves taking advantage of computers by inserting malware in order to promote specific campaigns. ISIS also distributes computer games in order to recruit volunteers and supporters, while training and preparing them for the battlefield. One example is a trailer distributed with a computer game called "Jihad Simulator," in which the games simulate abductions, military

vehicles' detonation, and shooting at schools.[22] The games facilitate a high level of communications (managing conversations through texts, network cameras, earphones, and microphones), and constitute a convenient way of maintaining an extensive recruitment and training infrastructure.[23]

As part of its well-financed and well-timed media activity, ISIS is initiating major media campaigns designed to encourage joining its ranks, including the issuing of threats against the U.S. and its allies in order to deter them from intervening in events in Iraq. One such campaign took place on July 19, 2014, and was distributed on various media outlets under the headline "A Billion Muslims Support the Islamic State." The campaign was successful in gaining support when messages were published all over the world following photographs of various sites: the Temple Mount in Jerusalem, the Eiffel Tower in Paris, Big Ben in London, and other landmarks in North America, Europe, and Asia. ISIS also sells souvenirs (shirts, key chains, toy soldiers, and personal items) for propaganda purposes and as an additional source of income. Several months ago, CNN reported that Facebook was taking steps to stop this, so far unsuccessfully.[24]

Psychological Warfare

The savage terrorist theater used by ISIS, the result of a dangerous symbiosis between the terrorist hungry for recognition and exposure, and the media in pursuit of ratings and eager for violent and riveting scripts created by terrorist events,[25] is not a new phenomenon. It is part of a rational strategy aimed at delivering a message that is mainly psychological in nature. In this sense, the use of terrorism by ISIS and similar organizations against British and American civilians is "mainly symbolic and part of propaganda."[26] Given the great cruelty and inhumanity used by the organization and its comprehensive use of cyberspace to distribute this content, ISIS introduces a new method of operation. By its nature, savagery creates an atmosphere of prolonged international interest and awareness. It also shapes its cruel image, sometimes creating the impression of being more powerful than it actually is.

The use of media by ISIS for terrorist purposes is substantially different from previous terrorist attack that won broad international media coverage, such as the 1979-1981 hostage crisis in Iran, the attack on the Twin Towers (2001) and the hostage crisis in a Moscow theater (2002).[27] While the subject of the use of the communications media by terrorists has been extensively

researched[28] in an attempt to understand it in the context of symbolic communications theory,[29] ISIS does not regard the victim as "unimportant." The victims (children, journalists, aid workers, and women) are very important, and their selection is designed to target the "soft underbelly" while the organization invests many resources in using kidnapped journalists for propaganda purposes.

A Strategic Change in the Targets of Terrorism

During 2014, ISIS made a number of strategic changes in its targets and modus operandi in the battle zone. In the first stage, the organization focused on creating infrastructure that would enable consolidation of its control of various areas in Syria and Iraq. The organization therefore committed savage terrorist acts against hostile local Sunni populations, symbols of the regime, and religious-based ethnic cleansing. These included the massacre of the Yazidi minority in the Erbil region, the Sinjar Mountains, and the area of the Mosul Dam. This process was accompanied mainly by media threats against the West, and continued until late summer 2014. A document was recently published by the Syrian Observatory for Human Rights documenting the execution of 1,429 people since last June in Syria. Half of the victims were civilians, and half were members of the al-Shaitat Shi'ite tribe in the eastern Deir a-Zor region in eastern Syria.[30]

The second stage began in August 2014, during the formation of the coalition to fight ISIS, the main significance of which was marking the West, particularly the U.S., as a key target for terrorist operations. As part of this change, ISIS brutally beheaded a number of foreigners it had kidnapped (Americans, British, and French), while making manipulative use of the media with the intention of generating horror in the West and the moderate Arab world. At the media level, the well-timed executions by an ISIS soldier of British origin dressed in black, referred to as "Jihadi John" was done under the heading of "A message to America," according to a prepared script, using advanced photography equipment. The messages placed responsibility on the U.S. and Canada, with the threat that any intervention by Western governments would lead to attacks on innocent civilians. According to a November 17 report in *The New York Times*, at least 23 people from 12 countries were kidnapped by ISIS in November 2012-January 2014, some of whom were released for ransom.[31]

In the third stage, beginning in mid-September, ISIS called for attacks on civilians in various Western countries taking part in the coalition formed against the organization. This was expressed in a speech by ISIS leader Abu Mohammad al-Adnani al-Shami under the title: "Indeed, your Lord is ever watchful," in which he called for the killing of "disbelievers" in Western countries.[32] The calls were issued in audio recordings calling for attacks on Western civilians and security forces.[33] The call also appeared in the fourth issue of Dabiq in October. Initial signs of the results of ISIS's call to kill Western civilians can be seen in the thwarted plan to kill civilians in Australia, the shooting and vehicular attacks in Canada, the axe attack against policemen in Queens in New York, the laying of explosives in Vienna, etc.[34]

The main purpose of the widely publicized beheadings is twofold; on the one hand, it is designed to generate pressure on public opinion, mainly against the governments of the U.K., U.S., and France, and to differentiate ISIS from the other organizations by its ultra-national savagery. On the other hand, it is a source of attraction for potential recruits by appealing to senses of basic Islamic morality in the framework of a return to the fundamentals of early Islam and a rejection of modern Western morality. The beheading of journalist James Foley on August 19 was designed to deliver a threatening message ("a message to America"), while attributing responsibility for his murder to the U.S., stating that any decision or action taken against the Islamic State will lead to attacks on American civilians. The murder of journalist Steven Sotloff on September 2 was also designed to deliver a sharp message to the U.S. ("a second message to America") against the continued aerial attacks by U.S. forces: "as long as your missiles continue to attack our people, our knife will continue to attack your people's throats."[35]

The beheadings are aimed at two target audiences: local and global. The first is not organized; it is part of the desire to wage psychological warfare against opponents from within. This includes propaganda videos, which are usually not well edited. The second and more significant audience, however, consists of the Western world, especially the U.S., the U.K., and Australia, with the purpose of gaining achievements and propaganda, terrorizing public opinion, and recruiting potential operatives. In September-October 2014, ISIS published a number of videos featuring British journalist John Cantlie from the battlefields in Ayn al-Arab (Kobani) designed for propaganda purposes, in which he announces that he will present the "manipulation

of the Western media," and that "the West is being dragged into a war it cannot win against thousands of armed men."[36] Syrian Observatory for Human Rights director Rami Abdul Rahman claimed that a large number of soldiers were murdered by beheading, and by placing the head in a public place ISIS wishes to generate terror and dread.[37] It should be noted that the phenomenon of murdering hostages by beheading is not new. Examples can be found, such as the execution of Daniel Pearl in 2002 by the National Movement for the Restoration of Pakistani Sovereignty, beheadings of ethnic Russians and foreigners by Chechen terrorists, and other groups, including Abu Sayyaf in the Philippines, Algerian groups, and the Taliban.

Summary and Insights

In recent months, the Islamic State has exhibited its mastery of social media, which it regards as a legitimate weapon in its war against its opponents in the organization's countries of origin and against the West (the U.S., U.K., and Australia). ISIS uses simple content that makes its objectives and message very clear, with one ultimate purpose: to induce terror through the calculated management of savagery and the complete absence of mercy.[38] The viral campaigns featuring beheading, crucifixions, burnings, and mass executions distributed through the various media are conducted with unprecedented brutality and cruelty. Terrorism is a type of propaganda, and the more cruel elements it includes, the greater its effect and the bigger the impression it leaves. The horrifying graphic description of beheadings, with its focus on a lone defenseless individual, has a greater effect than propaganda achieved through different means, such as car bombs and terrorism, even if the latter's death toll is higher.[39] ISIS is exploiting the inherent potential of global networking and the ability to simultaneously operate various and diverse means of mass influence, based on computer games, the Internet, and social networking.[40] These measures have created a sophisticated and well-timed online propaganda campaign.

ISIS's propaganda machine and the use of the social and communications media fulfill two important functions that are very distinguishable from each other in their purpose, relying on a media platform that did not exist a decade ago. The first is psychological warfare, targeting the morale of the enemy's soldiers. This is not a new strategy. Chinese general and philosopher Sun Tzu (Master Sun) asserted that victory is usually achieved by "selective, instant decapitation of military or societal targets to achieve

shock and awe" through the use of cruel and merciless means, such as beheading.[41] The Blitzkrieg in WWII brought a similar concept of intimidating the enemy through psychological warfare by distributing leaflets from the air, messages from very powerful loudspeakers, etc. The second involves gaining support from Western Islamic groups, while unifying the Islamic State's soldiers behind one goal and under one leadership through an appeal for a return to Islamic roots and sanctioning violence by recruits with no need for any further justification.

The combination of cruelty and the use of social networks by ISIS have been very successful so far, and are being used as a very powerful tool in combination with the Islamic State's military arsenal. In an unusual step, the Iraqi government banned the use of social media during the fighting in June in order to disrupt communications between ISIS members, a ban that continued for 17 days. More than 20 news websites were blocked, including al-Arabiya.[42]

ISIS operates differently than al-Qaeda, which has so far refrained from harming innocent Muslim civilians in order to avoid losing the population's support. Al-Qaeda leader Ayman al-Zawahiri advised that it was better to kill hostages by shooting, and to focus on attacks against the American and Iraqi forces. "You shouldn't be deceived by the praise of some of the zealous young men and their description of you as the sheikh of the slaughterers," he said, adding, "we are in a battle, and more than half of this battle is taking place in the battlefield of the media. And this media battle is a race for the hearts and minds of our people."[43]

In contrast, ISIS has no scruples about means; it also conducts deadly attacks against the local Muslim population, while implementing a murderous ideology in which the Islamic State's vision is realized through provocations, such as pitiless attacks against strategic sites and national infrastructures.[44] ISIS regards the use of rough violence as essential. The use of media, on the other hand, is also essential for effective propaganda.

The success of ISIS in adopting this strategy is reflected in a number of principal characteristics that distinguish its activity from that of other terrorist organizations and constitute criteria for the organization's success: conquering large territories in Syria and Iraq within a relatively short time span, consolidation of its rule, and the establishment of an Islamic Caliphate. The organization, which was founded as a branch of al-Qaeda in Iraq, has spread to eastern Syria and to the north, while exploiting the weakness of

the Iraqi regime. It now controls a population of 10-12 million people, one third of Iraq's territory, and one third of Syria, a territory almost equal in size to the entire U.K.

In the context of combating the organization, coalition military operations should be supplemented by action in other spheres. One is locating and disrupting the "money trail" through which the organization successfully operates a widespread financial system to supply its needs. This task requires an intelligence and global economic warfare effort in order to identify and neutralize the parties involved in financing the organization and trading with it. In addition, a supplementary political effort should be made, particularly with Turkey and Qatar, which in their support for radical Islam, ignoring the movement of volunteers to ISIS by way of the border between Turkey and Syria, are maintaining support in both camps. Finally, there should be an intelligence struggle and operations in cyberspace should be employed as well.

The second element involves reining in the organization's Internet exposure by blocking sites and content. These are used to recruit operatives, generate attacks, raise money, and exert psychological warfare. Legal infrastructure should be created for this purpose, and agreements should be reached with the large Internet companies having commercial interests. The technological ability to take practical measures exists, but without assembling an international task force that will take immediate effective action to remove malware from the Internet, it will be difficult to cope with this phenomenon. This team can also take action to undermine the organization's narrative through counter campaigns on the social networks: "fighting fire with fire."

The third element is designed to deal with spontaneous terrorist attacks in Western countries. Due to the absence of hierarchies in these attacks and the fact that most of the attacks do not require an existing organizational infrastructure in the country in which the attack takes place, it will be necessary to devise suitable tools for dealing with the attacks. One of these tools would be the ability to generate a profile of potential attacks. This profile will be derived from a variety of sources, the chief of which will be an analysis of the characteristics of the Internet activity by the populations likely to produce attackers. It is usually possible to retrospectively find signs indicating a wish to carry out an attack. It is therefore necessary to assemble an international task force that will be able to create the methodology for

constructing such a profile and devise the tools to identify potential hazards on the basis of an analysis of regularly collected big data. The main challenge in this approach concerns the assembling of the characteristics in the profile, rather than the technological aspects of the analysis systems. The defense organizations in the Western countries have a common interest, and will therefore be able to cooperate in devising this capability, thereby pooling their capabilities and expediting the implementation of this concept.

The Western countries require a combined effort to cope with the phenomenon before it is too late. ISIS is acting systematically in cyberspace, and creating a successful model for itself. The West, led by the U.S., needs political, legal, economic, operational, and technological action. Only a long-term combination of these aspects can facilitate an effective struggle against the organization and its jihad effort in the West.

Notes

1 As expressed by a soldier in the organization of Canadian origin in a recruitment video clip distributed by ISI in November: https://www.youtube.com/watch?v=Hzg2WMQB3ZA.
2 Carlos Marighella, "Minimanual of the Urban Guerrilla," *Survival 13*, no. 3 (1969): 95-100.
3 Daniel Cohen, "Fighting Islamic State in Cyberspace," *Haaretz* (September 5, 2014), http://www.haaretz.com/opinion/.premium-1.614320.
4 Neville Bolt, *The Violent Image: Insurgent Propaganda and the New Revolutionaries (*London: Hurst & Company, 2012).
5 *ISIS: Portrait of an Organization*, Meir Amit Intelligence and Information Center, document no. 182, November 28, 2014, http://www.terrorism-info.org.il/he/article/20733.
6 "Antiterrorism Seminar Discusses Media Role," *a-Sharq al-Awsat* (November 25, 2005), http://www.aawsat.net/2005/11/article55268813.
7 Angela Gendron, "al-Qaeda : propaganda and media strategy," ITAC Trends in Terrorism Series 2 (2007).
8 For further discussion of the ISIS public relations apparatuses, see the comprehensive analytic study of ISIS, *ISIS: Portrait of an Organization.*
9 The literal translation of al-Furqan is "separation," i.e., separation of truth from lies.
10 Ryan Mauro, "ISIS Releases 'Flames of War' Feature Film to Intimidate West," *The Clarion Project* (September 21, 2014), http://www.clarionproject.org/analysis/isis-releases-flames-war-feature-film-intimidate-west.
11 Brad Conley, "Leni Riefenstahl – Triumph Des Willens [1935] [HD]," February 25, 2014, https://www.youtube.com/watch?v=rclIE-_VZ5g.

12 "Al-Furqan Media Production Presents a New Film of the Islamic State of Iraq and the Levant," Online Jihad Exposed (May 18, 2014), http://www.onlinejihadexposed.com/2014/05/4.html.
13 Nico Prucha, "Is this the Most Successful Release of the Jihadist Video Ever?" Ideological trends, Iraq, social media (May 19, 2014), http://www.jihadica.com/is-this-the-most-successful-release-of-a-jihadist-video-ever. And: http://www.jihadica.com/is-this-the-most-successful-release-of-a-jihadist-video-ever-part-2-the-release-of-صليل-الصوارم-الرابع/.
14 See Terrorism Research & Analysis Consortium (TRAC) Press Room, http://www.trackingterrorism.org/content/trac-press-room.
15 "New ISIS Media Company Addresses English, German and French-Speaking Westerners," *MEMRI: Jihad & Terrorism Threat Monitor* (June 23, 2014), http://www.memrijttm.org/new-isis-media-company-targets-english-german-and-french-speaking-westerners.html.
16 For example, see https://azelin.fıles.wordpress.com/2014/06/islamic-state-of-iraq-and-al-shc481m-22islamic-state-report-122.pdf.
17 According to Muslim tradition, Dabiq is named after the place in northern Syria mentioned in the hadith about the end of days, when a great battle is expected to take place between Islam and the infıdels, which the Muslims will win.
18 It is worth noting that in October 2014, al-Qaeda issued *Resurgence*, a new magazine. The newspaper contains 117 pages, including English pages, and focuses on general jihad topics and current content focusing on the organization's activity in the Indian subcontinent. It can be found at http://www.longwarjournal.org/archives/2014/10/al_qaedas_resurgence.php.
19 See al-Platform Media: alplatformmedia.com/vb.
20 "ICT Jihadi Monitoring Group Periodic Review: Bimonthly Report Summary of Information on Jihadist Websites," International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center at Herzliya (February 2014), http://i-hls.com/wp-content/uploads/2014/06/JWMG122014.pdf.
21 Hashtag is used on social networks to label a given post as part of a given subject by adding a hash mark before the subject, after which content on a specific subject can be found effectively.
22 David Shamah, "Video Games, Twitter Tricks: How ISIS Pulls in the Kids," *Times of Israel* (September 21, 2014), http://www.timesofisrael.com/video-games-twitter-tricks-how-isis-pulls-in-the-kids-2.
23 More discussion about the use of the various media platforms, specifically the use of computer games can be found in an in-depth study published by the Dado Center for Interdisciplinary Military Studies: Daniel Baran and Yossi Levi, "What Does the West Not Understand?" *Between the Poles* 3 (January 2015).

24 Samuel Burke, "Facebook Looks to Block ISIS Clothing Sales," *CNN* (June 25, 2014), http://edition.cnn.com/2014/06/24/world/isis-facebook-merchandise.
25 Gabriel Weinmann and Conrad Winn, *The Theater of Terror: The Mass Media and International Terroris*m (New York: Longman Group, 1993).
26 Stephen L. Carter, "Boston and the Terrible Theater of Terrorism," *Bloomberg* (April 18, 2013), http://www.bloombergview.com/articles/2013-04-18/boston-and-the-terrible-theater-of-terrorism.
27 Gabriel Weinmann, "The Role of the Media in Propagating Terrorism," in *Countering Terrorism: Psychological Strategies*, U. Kumar and M.K. Mandal, eds. (London: SAGE publications, 2012), pp. 182-203.
28 Boaz Ganor, "The News Media in Terrorists' Strategy," *Ma'arachoth* 340 (1995), 41; Boaz Ganor, "the counter-terrorism puzzle: a guide for decision makers," Transaction Publishers, 2011.
29 Communications or symbolic interpretation is exchanges of symbols between various objects that alter the advance expectation of events.
30 "In Five Months, ISIS Executed 1,500 People in Syria," *Maariv- NRG Online* (November 17, 2014), http://www.nrg.co.il/online/1/ART2/646/773.html.
31 Karen Yourish, "The Fates of 23 ISIS Hostages in Syria," *New York Times* (November 17, 2014), http://www.nytimes.com/interactive/2014/10/24/world/middleeast/the-fate-of-23-hostages-in-syria.html?_r=0.
32 Robert Spencer, "Islamic State: 'We Will Conquer Your Rome, Break Your Crosses, and Enslave Your Women, by the Permission of Allah," *Jihad Watch* (September 21, 2014), http://www.jihadwatch.org/2014/09/islamic-state-we-will-conquer-your-rome-break-your-crosses-and-enslave-your-women-by-the-permission-of-allah.
33 The recording can be heard through the following link: http://ent.siteintelgroup.com/Statements/is-spokesman-had-called-for-lone-wolf-attacks-in-australia-in-september-2014-speech.html.
34 For example, Perry Chiaramonte, "Citizen Jihadists: ISIS Uses 'Lone wolves' to Mount Cheap, Effective Attacks on US Soil," *FOX News* (October 25, 2014), http://www.foxnews.com/world/2014/10/25/citizen-jihadists-isis-uses-lone-wolves-to-mount-cheap-effective-attacks-on-us/.
35 (GRAPHIC VIDEO) Islamic State Beheads American Journalist Steven Sotloff, http://leaksource.info/2014/09/02/graphic-video-islamic-state-beheads-american-journalist-steven-sotloff/.
36 "ISIS Publishes Video of Kidnapped Journalist 'I'm Going to Show You the Truth,'" *Ynet* (August 18, 2014), http://www.ynet.co.il/articles/0,7340,L-4572689,00.html.
37 The exact quote: "In order to strike terror into civilians and into any group that might decide to fight it," taken from: "Over 1,400 People

Executed in Syria by Isis in 5 Months: Monitor" (November 19, 2014), http://khabarsoutheastasia.com/en_GB/articles/apwi/articles/newsbriefs/2014/11/19/newsbrief-01.

38 Alastair Cooke, "The ISIS's 'Management of Savagery' in Iraq," *World Post,* updated August 30, 2014, http://www.huffingtonpost.com/alastair-crooke/iraq-isis-alqaeda_b_5542575.html.

39 Shashank Joshi, "Where Does the Islamic State's Fetish with Beheading People Come From?" *Telegraph* (September 14, 2014), http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11071276/Where-does-the-Islamic-States-fetish-with-beheading-people-come-from.html.

40 Baran and Levi, "What Does the West Not Understand?"

41 Harlan K. Ullman and James P. Wade, "Shock and Awe, Architecting Rapid Dominance," Chapter 2, NDU Press Book (December 1996), http://www.globalsecurity.org/military/library/report/1996/shock-n-awe_ch2.html.

42 Matt Smith, "Iraq Lifts Social Media Ban, Some Websites Still Blocked," *al-Arabiya News* (July 1, 2014), http://english.alarabiya.net/en/media/2014/07/01/Iraq-lifts-social-media-ban-some-websites-still-blocked.html

43 Craig Whitlock, "Keeping al-Qaeda in His Grip," *Washington Post* (April 16, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/04/15/AR2006041501130.html.

44 Abu Bakr Naji, *The Management of Savagery: the Most Critical Stage through which the Umma Will Pass. Translated by William McCants* (Cambridge: The John M. Olin Institute for Strategic Studies at Harvard University, 2006).

Commercial and Industrial Cyber Espionage in Israel

Shahar Argaman and Gabi Siboni

Cyberspace is especially suited to the theft of business information and to espionage. The accessibility of information, along with the ability to remain anonymous and cover one's tracks, allows various entities to engage in the theft of valuable information, an act that can cause major damage. Israel, rich in advanced technology and a leader in innovation-based industries that rely on unique intellectual property, is a prime target for cyber theft and commercial cyber attacks. This article examines the scope of cyber theft and cyber industrial espionage globally, and attempts to estimate how much financial damage they cause in countries around the world and in Israel. It seeks to raise awareness of the extent of the phenomena among the relevant authorities in Israel and provide recommendations on how to grapple with it.

Keywords: Cyber, espionage, industrial espionage, intellectual property, cyber crime, cyber theft, technology

> *"There are two types of companies: companies that have been breached and companies that don't know they've been breached.... The vast majority of companies have been breached."*[1]
> Shawn Henry

> *The director of the National Security Agency, Gen. Keith Alexander, called cybercrime "the greatest transfer of wealth in history." The price tag for intellectual property theft from U.S. companies is at least $250 billion a year.*[2]

Shahar Argaman is the director of the National Cyber Staff. Col. (ret.) Dr. Gabi Siboni is the head of the Military and Strategic Affairs Program and Cyber Security Program at INSS.

This article was first published in *Military and Strategic Affairs* 6, no. 1 (2014): 43-58.

Background

Cyberspace is a product of the accelerated pace of technological developments in the last few decades. Initially, communications and computerized systems were linked together to function as local networks. These networks were later linked together to form a global medium of existence and activity. At present, cyberspace continues to develop on numerous levels: in the wealth of interconnected computerized tools, in the number and variety of networks, in the volume of information traffic, in the level of connectivity, in the variety of applications, and in the degree to which economic and social activity depends on cyber functions.

While cyberspace brings with it much positive potential and broadens horizons on every level of human activity, it also entails new threats and in effect presents a new arena for hostile activity, from the sabotage of information in cyberspace to damage to the physical world through cyberspace functions.[3] As the overall use of cyberspace increases, so too does the hostile activity within the arena,[4] which already includes a vast range of threats: denial of service, destruction of websites, exposure of personal information for the purpose of wielding influence or instilling fear, various types of crime, industrial and security espionage, and damage to national strategic infrastructures, databases, command and control systems, and even weapon systems.

By its very nature, cyberspace is a medium particularly well suited to espionage in general and commercial and industrial espionage in particular. Industrial espionage among commercial rivals is hardly a new phenomenon, but cyberspace allows simpler access than in the past to a great deal of information while allowing a high level of invisibility. The damage that can result from commercial espionage today is of unprecedented scope precisely because cyberspace is optimally suited to such activity. Another reason cyberspace has become a key means of espionage is that state-sponsored intelligence organizations use it in the pursuit of state-sponsored goals – political, security, technological, and economic – as do criminal outfits pursuing purely economic gain. Much information has emerged about cyberspace espionage between states, especially cyber skirmishes between the United States and China, indicating that commercial espionage has become a primary tool of states in general and the powerful ones in particular, serving as a weapon in their economic wars and pursuit of global dominance.

As a state rich in advanced technology, Israel is very much at risk. The vast amounts of information created by financial, scientific, and other institutions within the state are stored, moved, and managed in cyberspace, and are therefore accessible to a variety of attackers. In addition, the part played by innovation-based industries and unique intellectual property in the Israeli economy is highly significant. Israel is a global leader in startup industries, which by their very nature generate additional motivation for commercial espionage against Israel. Given that advanced persistent threats (APTs) are rarely discovered by standard security measures of commercial companies, Israeli companies, especially those developing unique knowledge, presumably constitute targets for commercial espionage and the theft of intellectual property, as is the case in other technologically advanced countries.

The purpose of this article is to examine the use of cyberspace for commercial espionage and theft of intellectual property. The article seeks to underscore the complexity in assessing the extent of these phenomena and the economic damage they cause. Finally, the essay seeks to analyze the scope of commercial espionage in Israel in order to raise awareness of the phenomenon in the public discourse and thereby promote action to curtail it and as a result contain the damage it incurs.

Cyberspace as a Medium for Commercial Espionage

While commercial espionage has existed since the dawn of history, the transition of much of the business world to the cyber realm has propelled commercial espionage to this arena as well. Indeed, cyberspace is ideally suited to espionage, particularly commercial espionage. It allows relatively anonymous activity, including convenient and safe transmission of vast amounts of information regardless of distance and national borders. At the same time, it is very difficult for the victims of espionage – be they commercial or government bodies – to detect its occurrence. Even if the victims are aware of the attack and identify the spyware used to effect it, it is hard for them to attribute the malicious action to a particular culprit and credibly establish the responsibility and identity of the attacker.

Commercial espionage in cyberspace costs very little compared to other means of intelligence gathering, and entails a low level of risk of exposure. Cyberspace espionage greatly reduces the need for agents to infiltrate the target, and thus intelligence entities throughout the world can amplify

their capabilities, in terms of intelligence gathering within cyberspace[5] and the integration of traditional forms of espionage with new capabilities in this sphere. As such, espionage becomes simpler for the attacker and more dangerous for the attacked. For example, espionage involving a mole working for the organization under attack becomes simpler in the cyberspace era: transmitting stolen information is easier and identifying its source is harder. Furthermore, law enforcement has a lenient approach to cybercrime, thus reducing the risk taken by those engaged in commercial espionage. A burglar caught breaking and entering a physical place of business to steal information will probably have to pay a much higher price than someone stealing the same information using a keyboard.

Commercial espionage may be defined as the unauthorized possession of confidential commercial information not revealed to the public at large, for the purpose of attaining a technological advantage or economic gain. Such information may include data on strategy, planning, technological innovation, product development processes, manufacturing and marketing processes, advertising campaigns, financial status, legal issues, key personnel, salary information, tenders and bids data, and more. Targets might include not only competing organizations but also academic research institutes and other entities possessing valuable information. Unlike information gathering from open sources, obtaining the information often entails criminal offenses. This activity is only one branch of a larger group of economic crimes, such as embezzlement, fraud, theft, disruption of business activity, and more. Commercial espionage by a state is usually intended to strengthen the state's own economy, to create an economic advantage for that state or a sector of its economy in relation to competing sectors around the world.

The rise in the scope of commercial espionage in cyberspace reflects the technological, economic, and social changes that have occurred in recent years and the corresponding manner in which information is created, moved, stored, and managed in economic and scientific organizations, including sensitive bodies. Throughout the world, almost all commercial and scientific records, even the most sensitive, are digitally stored and accessible to computer networks. Given this pattern and given the advantages currently available to hi-tech attackers such as state-sponsored intelligence organizations or sophisticated criminal syndicates, these groups can use cyberspace to carry out theft of commercial and business information. Such thefts are on a scale that far outstrips any past commercial espionage,

both in terms of the importance and sensitivity of the stolen information to its owners and in terms of sheer quantity.

Experience has shown that only a few companies can identify hi-tech attacks carried out by state-sponsored espionage organizations or sophisticated crime syndicates. Even fewer are capable of effective defense.[6] There are many examples indicating that even the most sensitive companies in the defense industry in the United States were relatively easy targets for commercial (or security) espionage through the internet by state-sponsored organizations, apparently out of commercial motives.[7]

A report by ONCIX (the Office of the National Counterintelligence Executive) to the US Senate[8] addressed the threat of theft of commercial information and key rivals carrying out such activity in the United States. China and Russia were described as having the highest capabilities in the field and being "the most aggressive collectors of US economic information and technology."[9] A July 2012 report to the Congress by the same agency[10] cites Congressional testimony by Director of National Intelligence (DNI) General James R. Clapper regarding the US intelligence community's national threat assessment. Clapper testified that intelligence agencies of enemy nations are systematically developing methodologies and technologies to challenge the capabilities of the administration and private sector in the United States that protect national and commercial secrets.[11] Indeed, the 2013 US threat assessment put cyber threats at the top of the list of threats facing the United States,[12] ahead of terrorism and the proliferation of weapons of mass destruction.

The Complexity in Assessing the Damage of Commercial Espionage

Given the very nature of commercial espionage, assessment of the damage it causes is difficult for various reasons, including first and foremost the methodological problem of quantifying the scope of damage resulting from the loss of intellectual property and the fact that only a tiny fraction of all advanced espionage activity ever comes to light. In testimony before a US government committee, Richard Bejtlich, Chief Security Officer at Mandiant,[13] a company specializing in incident response and computer forensics solutions and services for government, defense, and enterprise organizations, said that of the total number of sophisticated espionage attacks originating in China investigated by his company, only 6 percent of the attacks

were discovered by the targets. This indicates that a tremendous gap exists between the prevalence of the phenomenon and an accurate appreciation of the cost to the economy resulting from commercial espionage.[14] Furthermore, sophisticated organizations engaged in commercial espionage in cyberspace use specific spyware that are incapable of being identified, blocked, or neutralized by the standard defensive tools of most commercial enterprises. Today, cyberspace favors the attacker by a wide margin.

Many espionage agencies use cyberspace as a key information-gathering arena. The capabilities developed by security agencies for this purpose far outstrip current defensive responses to these threats. Furthermore, focused, dedicated attackers also enjoy the advantage of being able to learn about and even obtain the defenders' security tools,[15] enabling them to run simulations in order to identify the conditions under which they will not be exposed by the very security tools the defenders are using.[16] In addition, state-sponsored espionage is carried out by intelligence groups designed for this purpose, whereas effective defense requires comprehensive, state-sponsored activity that involves security outfits and non-security organizations from both the government and the private sectors – an effort that is, by nature, slow and cumbersome.

The FBI has estimated that for every incident of penetration into computer networks identified by a US company, one hundred similar incidents have occurred that the computer networks failed to identify.[17] A report by Mandiant published in February 2013[18] stated that the goal of the Chinese attack formation was commercial espionage and that in that year it had attacked 141 Western companies, primarily in the United States. This is an example of commercial espionage activity carried out by a state-sponsored body that had been operating for years and eluding public awareness until the publication of the report.[19] On the basis of this example, one may infer that other companies coming under attack by sophisticated formations almost always fail to identify the attack. Even on the rare occasion when they realize they have been attacked, the attack is not made known to the public and the economic and security implications are not studied in the overall national context.

In the few cases in which companies and other organizations realize they are targeted and even manage to identify the spyware installed on their computers, they are hard pressed to assess the scope and type of information that has already leaked through their networks. Failure to

protect the company's or organization's assets often means that those in charge of security in these outfits tend to downplay the damage caused by the espionage. When unknown software – that is, malware – is discovered on the company's computers, the natural inclination is to remove it and make sure that the system continues to work. Only rarely will a company carry out a comprehensive forensic investigation aimed at uncovering the true nature of the attack and identifying the tools used to carry it out, as such an investigation is very costly – both in financial terms and in terms of the time needed to carry out a forensic investigation, during which the company's computer communications are severely compromised. Even when a full, professional forensic investigation is successfully conducted and the company's management receives a full, reliable picture of the theft of commercial data, often the organization will prefer not to make the theft publicly known or will at least seek to minimize the damage assessment, in the hopes of reducing the damage to the company's reputation that would result from a complete description of the theft. Damage to the company's reputation would, of course, endanger the company's relationship with its shareholders, investors, suppliers, customers, and all other stakeholders.

Finally, there is an inherent difficulty in assessing the financial worth of intellectual property. Clearly it is not necessarily reflected in the value of the investment that went into creating it, and this is probably the most precise statement one can make on the subject. The value of future income denied to a company as the result of information theft through cyberspace is entirely subjective and grounds for wild speculation.

For these and other reasons, it is extremely difficult to assess the cumulative damage caused to an organization as a result of commercial espionage in cyberspace. This difficulty is intensified when one tries to assess the financial damage the phenomenon causes the state, and thus assessments of damage to the state from commercial espionage in cyberspace vary wildly.

Methods of Assessing Commercial Damage

Various studies of the costs of commercial espionage have attempted to propose methodologies for damage assessment. The vast gaps in knowledge stemming from the above mentioned reasons as well as the inherent difficulty in closing those gaps pose an obstacle to any attempt to assess the scope of the phenomenon.

It is customary to divide the cost of cyberspace crime into three main categories:[20] *defense cost*, such as security, compliance with standards, and insurance; *direct cost*, such as damage to functionality, repair of the damage, loss of work time, resolution of the breaches, reconstruction of information, direct losses to the business, compensation to customers, fines, and legal issues; and *indirect cost*, such as loss of customer trust, loss of future business and income, or damage to the company brand.

The various approaches to damage assessment are based on surveys and theoretical analyses. In the studies based on surveys, sample groups of executives and IT specialists in commercial ventures are asked to provide damage assessments, from which overall assessments are extrapolated. The problem with this approach is the profound gap between the respondents' understanding of the issue and the scope of the phenomenon in practice. This gap is even more pronounced given that the sample group is liable to be biased. Those who have suffered painful attacks tend not to share their experiences and are therefore likely not to participate in surveys of this type. Accordingly, the studies must correct for these factors, which in itself has a dramatic effect on understanding the scope of the phenomenon.

The theoretical approach uses a model based on calculations drawing on open data, hypotheses, and assessments by information security experts, businesspeople, economists, and law enforcement agencies. This model too suffers from a gap between the quality of available information and true data; it also relies heavily on assessments. One example of such research is a study of the cost of cybercrime conducted by Detica in England.[21]

Threat assessment and measurement are critical for understanding the phenomenon of theft in cyberspace and for the optimal allocation of resources to defend against it. Therefore it is in the best interests of both commercial enterprises and states to assess the damage they face from information theft. Gen. Keith Alexander, Commander of the US Cyber Command and the Director of the NSA, has claimed that US companies lose some $250 billion annually as a result of cyber theft of intellectual property.[22] Citing a report published by Symantec, he said, "Symantec placed the cost of IP theft to the United States companies [at] $250 billion a year, global cybercrime at $114 billion annually ($388 billion when you factor in downtime)."[23] A report by the Commission on the Theft of American Intellectual Property estimates that the damage caused by cyber theft exceeds $300 billion a year.[24]

Countries other than the United States are also trying to assess the scope of the phenomenon. The Federal Office for the Protection of the Constitution in Germany assesses that German companies annually lose $28-71 billion and 30,000-70,000 jobs because of foreign economic espionage. South Korea has reported that the costs of economic espionage carried out by foreign entities in 2008 totaled $82 billion, compared to $26 billion in 2004. According to this report, 60 percent of the victims were small to medium-sized companies, and half of the cases of commercial espionage could be traced to China. In 2007, the Japanese Ministry of Economy, Trade, and Industry undertook a survey among 625 exporting companies and found that more than 35 percent of them reported the loss of some technology, and that more than 60 percent of the reported incidents were linked to China. Official sources in Great Britain have assessed that attacks on computer systems, including industrial espionage and theft of commercial information, cost the British private sector some $34 billion a year. More than 40 percent of this sum stems from the theft of intellectual property, such as specifications, formulas, and proprietary company information.[25]

Table 1: Assessments of Damage Resulting from Economic Espionage in Select Countries

Country	Assessment of annual damage (in $ billion) caused by theft of commercial information and intellectual property	Scope of damage in terms of percent of GNP
United States	250-300	1.67-2
South Korea	82	7.3
Germany	28-71	0.8-2
Great Britain	34	1.4

At the same time, those offering the estimates did not explain how they had arrived at their damage assessments, probably because of the difficulty in estimating the direct, not to mention the indirect costs of cybercrime. One must also take into account that those undertaking damage assessment studies, particularly certain information security companies, are liable to have a vested interest in inflating the scope of the phenomenon.

A study published by McAfee in July 2013[26] attempted to address the complexity of assessing the cost of cybercrime. The study questions published cost assessments and offers lower assessments than the official

estimates of damage to the US economy. The study does not include definitive assessments of the cost of such damage, but points out, for example, that the upper limit of damage to the US economy claimed by one method of assessment is anywhere between 1/2 to 2 percent of the GNP,[27] whereas another method of assessment places it at lower than 1 percent of the GNP.[28]

Commercial Espionage in Israel

As a state rich in advanced technology, Israel is particularly vulnerable to threats in cyberspace in general and commercial espionage in particular. A great deal of Israeli export relies on companies highly dependent on intellectual property, thereby making Israel a target for the theft of this sort. Furthermore, the role of industries based on innovation and unique intellectual property in the Israeli economy is very significant. Israel is a global leader in startups, which invites further motivation for commercial espionage against Israel. In addition, the commercial sector in Israel has little awareness of the risks of cyberspace espionage and prefers convenience, functionality and exploitation of business opportunities rather than security. Presumably, therefore, as in other developed countries, commercial enterprises in Israel – especially those developing unique knowledge – are targets for commercial espionage and the theft of intellectual property. Of the 141 companies attacked by the Chinese attack formation APT1, as described by Mandiant, three were Israeli.[29]

Israel was a world leader when it came to understanding cyberspace-based threats to critical infrastructures, but not when it came to grasping cyber threats to the business world. As early as 2003, the state established the National Information Security Authority,[30] charged with securing Israel's critical infrastructures against cyberspace attacks and preventing the theft of state secrets. The Israeli business sector and the public at large did not benefit from similar attention, and currently no organization has the responsibility of protecting these entities against commercial espionage in cyberspace. As a result, Israel today lags behind many other countries in the world, including the United States, when it comes to protecting the business sector. Other countries reached the conclusion that state-sponsored protection of national commercial assets is a high priority and that they are responsible for providing the scaffolding for responding to cyberspace threats to the economy in general and the private sector in particular. This realization has led to the establishment of one or several state agencies

charged with leading state-sponsored defensive activity in cyberspace in order to strengthen overall protection in the field.[31]

It is hard to assess the damage caused to the Israeli economy by commercial espionage. There is no obligation to report the discovery of information-gathering tools in company computers, other than minimal guidelines for the population registry and regulation for special sectors, such as banks and bodies within the purview of the National Information Security Authority, and with respect to the authority overseeing security in the defense establishment. Furthermore, in Israel, companies are under no legal obligation to report the loss of sensitive business information,[32] and there is no organization charged with defending the business sector in cyberspace, whose job it would be to collect such information and use it in order to draw conclusions and strengthen overall defensive responsiveness. Consequently, the likelihood of identifying commercial espionage in cyberspace in Israel and accurately assessing its scope is very slim. This state of affairs presumably also accounts for the dearth of reports on theft of commercial information and intellectual property from Israeli companies.

Despite the difficulty of assessing the damage caused by attacks in cyberspace, Israeli businesses and organizations are presumably just as exposed to commercial theft as those of other developed nations, both because of Israel's image as a global leader in the development of innovative knowledge and because of the lacunae in defense and protections noted above. Even using conservative estimates – namely, that commercial theft in cyberspace accounts for one percent of the GNP – the annual damage of such crime in Israel reaches roughly $2.5 billion. Preliminary research on the damage of commercial espionage in Israel, undertaken for the National Cyber Command by Meidata, a market research company, assesses the annual damage to the Israeli market from commercial espionage to be in the $1-3 billion range. There is no doubt that damage on this scale, which increases from one year to the next, requires a national response and justifies significant investment in the defense of companies and organizations under attack, which currently bear the lion's share of the cost of commercial espionage.

Conclusion

The State of Israel, with its high level of security awareness, was a pioneer in understanding the security risk developing in cyberspace, even before any

damage to its critical infrastructures was actually identified. Nonetheless, to date the danger posed by the theft of trade secrets and intellectual property from commercial companies in Israel has not been recognized as a significant threat to the country's stability, even after clear evidence has emerged proving that nations and criminal syndicates, equipped with the most sophisticated tools in existence, use cyberspace to commit commercial espionage and that this state of affairs has far reaching economic ramifications for commercial companies and countries.

The economic threat to commercial companies from commercial espionage has been defined by the head of the US intelligence community as a concrete threat against the United States of the highest order, ranked ahead of terrorism and the proliferation of WMDs. The cost of damage incurred from commercial espionage in cyberspace is high and on the rise, and it is borne primarily by the business community. According to various studies, the component represented by the cost of commercial espionage is the most dominant in the total of all types of cyberspace crime.[33] Israel, whose economy is to a large extent driven by innovative knowledge, is also vulnerable to the threat of cybercrime, including commercial espionage.

It is very difficult to assess the damage incurred by commercial espionage in cyberspace. Therefore we see a very broad range of assessments generated by a variety of reports. The difficulty in assessing damage empirically and the extensive reliance on assessments by experts seeking to address major gaps in the quality of collected data constitute obstacles to all methods of assessing the damage caused by commercial espionage and account for the vast discrepancies among various damage assessments. Nonetheless, these assessments are necessary in order to understand the impact of commercial espionage, and they provide the basis for states' comprehension of the phenomenon and their attempts to thwart it.

A strong methodology that would provide the tools for reliable assessments of the damage discussed by this essay is highly necessary. Development of this methodology would increase awareness of the need to improve protection against the threat and the ensuing damage. Toward this end, first and foremost it is necessary to improve the ability to gather reliable information about the phenomenon by means of mechanisms for reporting cyberspace incidents. Furthermore, it is necessary to develop better assessment tools that address existing gaps between reports and assessments surveying the number of incidents and resulting damage on

the one hand, and reality on the other. This is an inherent gap in knowledge, because in most cases the attacked parties are not aware that they have been attacked and that information about their business has been stolen; they are therefore incapable, even after the fact, of linking damage to their business to information theft about which they knew nothing in the first place. In addition, improving the overall civilian responses in cyberspace in Israel, while also establishing an agency charged with responsibility for the matter, could allow for the development of a comprehensive doctrine for addressing commercial theft in cyberspace based on a broad view of national needs.

The goal of this essay is to shed light on the phenomenon of commercial espionage in cyberspace and the damage it causes to the Israeli economy. In the absence of in-depth studies of the phenomenon, its precise scope remains elusive, but it is reasonable to conclude that it has a significant impact on the Israeli economy and is steadily increasing. The response to the phenomenon must include a range of efforts, including but not limited to the following: focused research on the scope of the phenomenon and a breakdown by sector; improved security for the business sector; the development of a cyberspace security industry; and state-sponsored measures providing a response to commercial espionage throughout cyberspace, including cooperation and arrangement with other states suffering similarly from the phenomenon.

Commercial espionage in cyberspace demands a complex response and requires tremendous resources. Raising the level of awareness regarding the phenomenon, both in the business world and among the decision makers in Israel, appears to be a necessary precondition for engaging in efforts to reduce the damage caused by cybercrime in general and by commercial espionage in particular. It will then be possible to bring Israel's defensive cyberspace capabilities to bear against the entire gamut of threats.

Notes

1 Nicole Perlroth, "Nissan is Latest Company to Get Hacked," *New York Times*, April 24, 2012, http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/?_r=0.

2 Carrie Lukas, "It's Time for the U.S. to Deal with Cyber-Espionage," *US News*, June 4, 2013, http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy.

3 For example, by making changes to computerized command and control systems of industrial processes so that damage is caused to the industrial process or to the industrial systems themselves.
4 Francois Paget, "2014 Threats Predictions: Cybercrime and Hacktivism Will Continue to Grow," McAfee Labs, January 8, 2014, http://blogs.mcafee.com/mcafee-labs/2014-threats-predictions-cybercrime-and-hacktivism-will-continue-to-grow.
5 The most prominent example of surveillance carried out entirely in cyberspace is the global PRISM system of the NSA, whose existence came to light thanks to Edward Snowden's revelations. The NSA's surveillance was allegedly carried out for the sake of the security and safety of US citizens. However, there are reports charging that industries of interest to the United States, especially in the field of advanced security capabilities, were also placed under surveillance. See Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; and Scott Shane, "No Morsel Too Minuscule for All-Consuming N.S.A.," *New York Times*, November 2, 2013, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=1&_r=0.
6 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units," February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
7 See, for example, the successful cyber attack in 2011 on Lockheed Martin with the aim of stealing plans for the advanced F-35 stealth aircraft.
8 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, Annex B – West and East Accuse China and Russia of Economic Espionage*, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.
9 Ibid., p. 4.
10 *Foreign and Economic Espionage Penalty Enhancement Act of 2012*, House of Representatives Report 112-610, 2012, http://www.fas.org/irp/congress/2012_rpt/ecoesp.pdf.
11 James R. Clapper, Director of National Intelligence, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," January 31, 2012, p. 8, http://www.intelligence.senate.gov/120131/clapper.pdf.
12 James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence," March 12, 2013, http://www.intelligence.senate.gov/130312/clapper.pdf.
13 In January 2014 Mandiant was bought by FireEye.

14 Devlin Barrett, "U.S. Outgunned in Hacker War," *Wall Street Journal*, March 28, 2012, http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html.
15 In most cases, the security tools are standard commercial tools.
16 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."
17 "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year," *International Business Times*, July 13, 2012, http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559.
18 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."
19 In the report, the company notes that it investigated dozens of advanced attack formations, of which more than 20 had similar characteristics and all originated in China. For reasons of its own, the company chose to relate to only one such formation in its report.
20 R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the Cost of Cybercrime," in *Workshop on the Economics of Information Security*, WEIS, 2012, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.
21 Detica, *The Cost of Cyber Crime*, A Detica Report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, UK, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf.
22 "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year."
23 Emil Protalinski, "NSA: Cybercrime is the Greatest Transfer of Wealth in History," *ZDnet*, July 10, 2012, http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/.
24 The IP Commission Report, *The Report of the Commission on the Theft of American Intellectual Property*, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
25 Office of the Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*.
26 McAfee, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.
27 Ibid., p. 14.
28 Ibid., p. 15.
29 Mandiant Report, "APT1 Exposing One of China's Cyber Espionage Units."
30 The National Information Security Authority, established in accordance with a December 2002 government decision, is subordinate to Israel's General Security Services.
31 Overall responsibility for national defense in the United States falls on the Department of Homeland Security, which works in very close cooperation with the Department of Defense (which includes intelligence agencies, such as the National Security Agency and the Office of the

National Counterintelligence Executive, that are very active in defending cyberspace against attacks and commercial espionage), the Federal Bureau of Investigation, and the Department of Justice.

32 Cyberspace theft from publicly held companies in Israel, which is liable to affect their activities or assets, might give rise to an obligation to inform the stock exchange, as such information could potentially affect the considerations of reasonable investors in deciding whether to buy or sell their company shares.

33 Detica, *The Cost of Cyber Crime*, p. 3.

A Multidisciplinary Analysis of Cyber Information Sharing

Aviram Zrahia

The emergence of the cyber threat phenomenon is forcing organizations to change the way they think about security. One of these changes relates to organizations' policy on sharing cyber information with outside parties. This means shifting away from the view of the organization as an isolated, compartmentalized entity towards a view of the organization as a sharing one. Sharing generates a complex, multifaceted challenge to technology, law, organizational culture and even politics. Establishing a system of sharing serves many parties, including regulatory bodies, governments, legal authorities, intelligence agencies, the manufacturers of solutions and services, as well as the organizations themselves, but it also arouses opposition among elements within the organization, and organizations defending the right for privacy. The purpose of this essay is to present the various challenges posed by cyber information sharing, expose the reader to its conceptual world, and present some insights and forecasts for its future development.

Key words: cyber, information sharing, privacy, regulation, information security, trust

Introduction

One of the most difficult challenges faced by organizations is confronting the cyber threat phenomenon. The increased use of technology in organizations of any kind–government, public, and private–turns them into targets of attacks aimed at gathering or damaging information, or suspending services. Attacks on commercial organizations are liable to harm the organizations'

Aviram Zrahia is a cyber security expert at Juniper Networks and a lecturer on cyberspace, and is an intern at INSS.

This article was first published in *Military and Strategic Affairs* 6, no. 3 (2014): 59-77.

reputation, endanger physical assets and intellectual property, and cause serious financial damage. Attacks on governments, public bodies, and infrastructures may also disrupt the routines of entire nations and jeopardize the health and safety of their citizens.

Over the last decade, traditional crime has crossed into cyberspace; the growing sophistication of cracking tools and attack vectors has led to the creation of a new, developed and sophisticated cyberspace crime economy. A similar process has also occurred in the sphere of warfare between nations, as many now view cyberspace as the fifth dimension of the modern battlefield, in addition to sea, land, air, and space.

Confronting the cyberspace threat requires an investment in human and technological infrastructures based on an organizational or national risk management policy. The quality of an organization's information security system is affected by different factors, among them the ability to gather and analyze information on legitimate user traffic as well as attacks, regardless of their success. This allows one to identify vulnerabilities in the security system and prevent their exploitation, while identifying and responding to attacks and breaches quickly and effectively, thereby preventing or at least minimizing the damage.

Sharing organizational cyber information is the act of communicating information regarding an organization's security to an external party. While such sharing results in gains for both parties, it does, however, create a complex, multifaceted challenge and represents a shift in the traditional information technology paradigm. The sharing model may exist within the same sector, across different sectors, between commercial enterprises and government bodies, and between different governments. The last two years have seen an increase in the sharing trend; regulatory and law enforcement bodies, both local and international, are promoting it by means of incentives, guidelines and legislation. Concurrently, a security solutions industry based on information sharing among bodies is developing rapidly.

The purpose of this essay is to present the multifaceted nature of the challenge posed by sharing. It begins by presenting the current state of affairs and related problems, followed by an analysis of the practical aspects of sharing implementation, including reference to the theoretical background of trust among bodies. The following section lists the organizational gains and challenges, describing the business opportunities, aspects of the law, regulation and privacy. The paper concludes by offering several insights.

Most of the examples in the essay are from the United States, where sharing initiatives, standardization efforts, government and intelligence agencies actions, and legislative processes are open and at the heart of public debate.

From Compartmentalization to Sharing

The cyber threat is a sophisticated, complex dimension of crime and warfare that has developed in recent years in scope and severity. In terms of the scope of the threat, organizations must now defend not only their computer networks and information systems but also the range of endpoints available to users, such as smartphones and tablets, as well as infrastructure systems, including electricity and air conditioning. They must do so continuously while also making sure they can provide service anywhere, anytime, as expected of an organization of this era.

In terms of the severity of the threat, attacks are becoming harder to identify and locate, as they also include undocumented attack vectors that are unknown to the manufacturers of security solutions. This is true of zero day attacks;[1] the fact that hackers share information continuously and in real time creates a situation in which any weak point exposed in the system or malware can be replicated and used as means to perpetrate an attack almost instantaneously, regardless of location. A recent study of the topic conducted by the RAND Corporation[2] provides an analysis of the way in which cyberspace black markets are built, functioning like ecosystems with clear infrastructure and modules.

These developments create a paradigm shift towards joint efforts at fighting cybercrime, and as a result, many organizations are changing their approach to security; in most organizations, except for those subordinate to regulation and military and/or government systems, the approach to information security management was characterized by total separation from other organizations, both in terms of the technology of their information and security systems and in terms of sharing information about cyber events and security. Information about an attack or an attempted attack and the results of its analysis were kept within the organization, classified and distributed to a very limited intra-organizational list. Revealing information to a third party was perceived as a risk, a move liable to result in damage to its reputation, legal exposure and other complications.

Recently, this trend has reversed. Many organizations and authorities have abandoned the compartmentalization strategy[3] in favor of information

sharing. Through sharing cyber information among organizations, the way hackers do on the attacking side, security measures created in a certain organization to deal with a particular threat can be used by other organizations as an inoculation or at least as information that will heighten their alertness to that particular threat.

The high costs incurred by organizations–in terms of time, manpower and technology–required to provide an effective security protection generate an organizational interest in sharing information and passing some of the costs on to a third party. A study carried out in the United States[4] analyzed the connection between sharing cyber information and the costs of organizational cyber security. It found that companies sharing information spent less on security systems to reach the same level of protection attained by companies that did not share information, meaning that companies can save on direct costs as a result of information sharing. This includes, for example, proactive intelligence gathering and input about weaknesses and expected attacks, inoculations to attacks that occurred in other organizations, use of professionals to help analyze security events, and more.

Another reason for the change in organizational approach to information sharing is the direct and indirect business value in meeting standards and regulations. In certain critical sectors, like finance, healthcare, energy and communications, even private organizations are required to allow state supervision. Most regulations demand information sharing between the organization and some oversight body when it comes to cyber events or attempted attacks. In addition to the obligations, the regulations may have direct and indirect value: a financial organization subject to the Basel III regulation[5]–a standard relating to financial institutions requiring transparency on security events vis-à-vis the regulatory body–enjoys the direct benefit of improved capital allocation for the credit it extends, creating a greater profit margin. An example of indirect benefit may be found in an organization providing services that can make a bid on a government tender that requires bidders to meet the ISO-27032 standard,[6] which also entails information sharing.

Technological Principles in Information Sharing

Secure information sharing among organizations is, in many ways, a technological and operational challenge, from goal and policy articulation to implementation and use. The methods required to meet the challenge

must balance many different components: the ability to support a very large range of organizations and easily add them to the sharing endeavor (scalability); the ability to make use of information after establishing correlation and analyzing it in close to real time so as to produce maximal benefit (usability); and a system of controls to ensure the existence of the "CIA" principles: confidentiality, integrity, availability.[7] The steps towards constructing a system of sharing must include, among other things, goal articulation and participant definition, the privileges and obligations of the participating organizations, technological architecture, trust and oversight model, and work processes.

Information sharing among different entities requires the creation of a system of trust in order to ensure that the information is correct, complete, beneficial and useful. Trust is the basis for all the practical models and examples discussed in this essay. When it comes to trust, the sphere of discussion and solutions ranges from a product's components such as a computer, through the incorporation of various products into a system, to the trust between different systems in different organizations, such as, for example, internet commerce. Standards institutions, such as the Trusted Computing Group,[8] deal with many aspects of the topic, but cyber information sharing is a challenge for which the existing models have not yet provided a complete answer, hence the need for separate debate and the establishment of standards on this point precisely.

When building infrastructure for information sharing, there are three possible models.[9] The first is the "hub and spoke" model in which a central site receives information from the end organizations, fuses it to accommodate different needs and then disseminates it.[10] The hub serves as a clearance center protecting privacy and the intellectual property of all the participating organizations; its use is made possible in part by the accelerated technological development in the field of big data. This allows the processing and analysis of tremendous amounts of information and is a basic building block in constructing the ability to fuse information from different sources. The drawbacks of this model are primarily the consequences from its centralization: the challenge of size, dependence on a central site, delays in processing and disseminating the information.

The second model is the post-to-all architecture in which information is directly distributed among the participating organizations. Since the data distributed is raw, this model requires infrastructure for analysis in every

organization. The third model incorporates aspects of the first and second, striving to take advantage of the relative strengths of each. However, it is relatively complex and expensive to implement.

Technologically speaking, realizing the goal of sharing must take into account protecting an organization's assets and privacy in two ways: first, control of the information being shared based on the participants' goals, and a standardized agreed-upon format. Some of the definitions are meant to conceal the true sources of the information–as in the field of intelligence gathering– so that unnecessary details do not leak outside the organization. The second way entails limiting access to the information, and includes control of its distribution, where it is sent and who sees it, and must be based on a standardized sharing protocol.

Another fundamental choice that must be made is between the automated sharing model and the manual sharing model. Manual sharing means that an authorized party within the organization with access to the sharing system sends and receives information, and controls access to the information. The manual model has a prominent drawback: the human factor creates a bottleneck, especially when the organization is under attack. Other drawbacks include human error and difficulty of managing constant updates.

Automated sharing forces one to decide on a uniform, normalized format, a system of sensors in the organization that will gather and disseminate information, a monitoring system for local reception of warnings, and meticulous realization of controls designed to prevent unwanted distribution of sensitive information. This method overcomes the limitations of manual sharing, but it requires organizations to confront attack scenarios in which the automated sharing system is exposed, such as database poisoning.[11]

Some cyber information sharing standardization activities are already taking place. The most advanced, which has also been adopted by the US Department of Defense, involves a format called the Structured Threat Information eXpression (STIX™).[12] This format defines the structure of a database in which information relating to a user and/or traffic is proactively sent from the organization to an external entity or from an external entity to the organization while containing a range of structured details about a security event. Another relevant standardization for automating sharing is called Trust Automated eXchange of Indicator Information (TAXII™),[13] and it contains the structure of messages and network protocols supporting the transmission of STIX-type messages among different entities. There

are several other peripheral protocols under a wider architecture called Cyber Observable Expression (CyBOX),[14] supported by the US Department of Defense as part of the effort to automate sharing.

It seems that most theoretical models suggested by academics[15] and the practical models suggested by various research institutions[16] are based on automated realization, trust, and a "hub and spoke" sharing architecture. The standardization efforts referred to above suit the spirit of the academic and practical models, so that it seems that, technologically, there is a consensus over the right way to construct such a system. And, indeed, significant parties, such as the US Department of Defense, are working to advance projects based on this outline.[17] Nonetheless, the road to realizing effective information sharing remains long because of the multiple technological, commercial, operational, legal, and (some would claim) moral challenges faced by the sharing initiative members.

Benefits and Risks in Information Sharing

The value of sharing differs depending on the interests of the parties involved. In the case of commercial enterprises, sharing allows a heightened level of security and a reduction in response time in case of an attack, or inoculation against a possible attack in the future by means of receiving warnings and help in identifying, analyzing and confronting attacks. An experiment carried out by a South Korean research team supports this assessment.[18] Sharing also facilitates a reduction in the cost of security thanks to at least partial outsourcing of the analysis and response to a third party. Furthermore, the organization can benefit from regulatory relief as the result of increased transparency and meeting reporting obligations and other conditions.

In the case of the vendors and solutions and services providers, this is a new, technologically-oriented market segment with great growth potential that can distinguish them by creating sustainable, competitive advantages. One of the primary services this sector can offer is identification of possible attack patterns and the distribution of inoculations and warnings to organizations on the basis of fusing information about attacks and attackers gathered from the organizations themselves.

In the case of governments, it is in the interest of regulatory bodies and government and intelligence agencies to encourage sharing because they increase the organizations' transparency, receive a broad situation

assessment of the availability of services and credibility of the information, undertake analysis across different networks and organizations to identify patterns of attacks that have taken place or might take place, and allow for the possibility of a rapid response while disseminating the information to other organizations for the purpose of inoculating them. A state-sponsored body has the ability to construct and maintain a high level of technological capability for its personnel, and to cooperate with organizations in terms of human and technological resources. Sharing is an obvious national interest, allowing the government to fight the national cyberwar and strike at cybercrime in the most effective way possible as well as control the availability of critical national, public and private infrastructures. An example of the realization of regulation with a similar orientation in a different field may be found in regulations on the emission of industrial pollutants, which in some countries require industries, continuously and online, to monitor and report data on air quality in chimneys and other sources of pollution.[19]

Despite the advantages listed above, there are several risks directly related to cyber information sharing among organizations. An analysis of these risks must occur in the setting of an organizational risk management strategy and include the probability of every risk, its effects, the controls required to keep it in check, and the ways to reduce it. For example, the way to reduce the risk of legal exposure to lawsuits for revealing personal or commercial information is by means of laws and guidelines providing legal protection by the government or regulatory body. Another example is the risk of loss of organizational information assets as the result of uncontrolled sharing. That risk can be reduced by using a built-in, standardized sharing format that does not include sensitive information, as well as other checks such as instructions, regulations or legislation that will force the organization to remove personal or commercial data from the information meant to be shared before sending it.

Business Opportunities

The development of cyberspace threats and changes in organizational attitudes towards sharing are a business opportunity for the manufacturers of technological solutions, integration companies and service providers that can leverage their base of products, knowledge and services to create added value in the context of the sharing challenge.

One example relates to the challenges posed by innovative attack technologies, such as the Advanced Persistent Threat (known as APT),[20] or taking advantage of undetected or untreated security breaches. Both of these attack mechanisms reduce the effectiveness of the traditional security measures[21] but can, to a certain extent, be addressed by an inter-organizational security sharing service. Such sharing could facilitate the identification of an anomaly in the cloud and comparison with organizational events not only with regard to its conduct within the organization but also to that within similar organizations, thus enhancing the identification mechanism and reducing the risk that harmless traffic will accidentally be identified as malicious (known as "false positive"). In addition, after the identification of an attack or attacker in a given organization, the components or the inoculation can be distributed to other organizations and thereby prevent similar attacks.

Several security systems manufacturers provide solutions to cyber information sharing based on a decentralized infrastructure of information gathering, using a system of probes, which may at times also serve as honeypot traps for attackers. These are installed in organizations and end clients or at central internet nodes belonging to the manufacturer. This infrastructure gathers information on attacks and attackers in real time, in cross-referencing geographical location and attack, and distributes it as a service to the organizations involved in sharing. The system serves as a share-based database on attackers and/or attacks in the cloud and may sometimes include a component that filters and blocks potential attacks on the basis of the information being dynamically updated.

In the case of cloud-based communications and storage service providers, sharing is an opportunity to reduce the rate of client dropout by means of providing the added value of another layer of protection.[22] The nature of a shared cloud allows the provider to improve the security policy for all the other hosted organizations in order to prevent its recurrence after identifying and stopping an attack in one organization.

Another business opportunity directly related to sharing initiatives is the construction of a solution for gathering, analyzing and distributing cyber information at the national or market sector levels. Several integration companies in the world have a comprehensive solution for creating a situation assessment, analyzing events, distributing inoculations, training simulators, and other components, at the scale of military and large

public systems. Moreover, there are solution manufacturers in the field of monitoring and in-depth analysis of traffic (deep packet inspection), allowing telecommunication service providers to selectively share information with the legal authorities so that the latter may listen in on telephone and internet networks for the sake of identifying threats. Some of these companies also provide the solution component responsible for information analysis based on smart logic, containing analysis of a tremendous amount of information gathered from various sources, study of anomalies, and correlations among the events.

One may assume that the wave of technological innovation in the world of security solutions will continue because of the need to adapt security systems to existing and emerging cyber threats. Furthermore, one may assume that the idea of sharing–taking on greater prominence in the security policies of key organizations–will continue to present business opportunities to commercial entities operating in the field.

Regulation and Privacy

There are fields in which the regulatory body and/or the law already require sharing information about cyber threats and cyber events, and it would seem that this trend is on the rise given governments' need to establish a national security system to fight cybercrime and maintain transparency regarding cyber-related events in public companies and strategic market sectors, such as communications, finance and healthcare. Moreover, various regulators, such as Basel III and ISO-27032, encourage sharing information between organizations and the authorities, both by means of guidelines and by offering economic benefits and relief to participating organizations. A paper analyzing the trade-off in financial institutions between investing in information security and sharing cyber information[23] concluded that the benefits of sharing among organizations increase in correlation with their interdependency, and the more sharing there is among such institutions the smaller their investment in information security. In many market segments (such as finances and telecommunications) the links between the organizations are critical to their everyday functioning, and an attack on one organization could propagate and damage the functioning of other organizations in the same sector. Examples are financial transactions between different banks and phone calls between different service providers.

Similar organizations also share similar challenges, some of which may be unique to their sector. For example, healthcare organizations share the unique challenge of confronting cyber attacks aimed at medical equipment. Cooperation among such organizations on the gathering of intelligence or hardening procedure for such equipment will save on the investment each of the organizations has to make on its own.

Several nations have iterated their intention to establish systems for gathering cyber information, including the incorporation of government bodies and private/public bodies of national importance.[24] The essence of this move is to create a comprehensive cyber situation assessment, providing the ability to respond to attacks with highly trained personnel, and immediately disseminate inoculations or information about the attack to all subordinate organizations. As noted, the technological base for creating such a system may require legislation, and requires cyber information sharing among organizations and the establishment of a center for fusing information and applying defense mechanisms to secure organizational assets and privacy. The British government has established a sharing initiative called the Cyber Security Information Sharing Partnership (CISP) as part of its national program for coping with cyberspace challenges.[25] The partnership already includes more than 250 key organizations as well as the legal authorities, and its purpose is to improve the ability to cope with cybercrime and cyberterrorism. Since the beginning of the 21st century, the United States has instituted sharing initiatives named Information Sharing and Analysis Centers (ISAC) in sectors such as healthcare, finance and more. Most of these initiatives are owned and financed by the participating organizations, but recently they have benefitted from technological and even financial support from the US Department of Defense, thus acknowledging the government's interest. Examples of involvement include providing access to the United States Computer Emergency Readiness Team (US-CERT)[26] and establishing a master initiative designed to unite all the inter-organizational information in the United States into a single system.[27]

It is obvious that fighting cybercrime and cyberterrorism, which by their very nature cross geographical and political borders, can succeed only through technological and legal cooperation among nations. One such initiative is the program for research cooperation in the field of cyberspace initiated by NATO and the EU.[28] Another initiative is the sharing infrastructure being built at NATO, in which the information

will be automated on the basis of STIX in order to allow sharing among various organizations in NATO member nations.[29] Legally, the Convention on Cybercrime (also known as the Budapest Convention) was formulated and signed with an eye to coordinate the various legislative systems of the EU member nations, improve joint investigative methods, and increase cooperation in dealing with computer crime.

A paper surveying international cooperation in protecting critical infrastructures against cyberattacks[30] reinforces the hypothesis that the chances of an information sharing system succeeding increase if the participating entities have similar interests and cultural and political outlooks. Information sharing among different entities is naturally challenging in terms of maintaining secrecy because it requires a definition of the limits on sharing and controls that can distinguish between private or intra-organizational information and information that may be shared.

Over the years, governments have received tacit cooperation, which is sometimes enforced through legislation, from infrastructure and service providers, as well as application vendors, both for the purpose of national security and for the purpose of fighting cybercrime. This phenomenon received much attention recently, especially after *The Guardian* revealed, on the basis of Edward Snowden's leaks, the US National Security Agency surveillance of computer traffic of leading US companies in the context of its PRISM program.[31] The newspaper also revealed that the NSA-equivalent British intelligence organization GCHQ, monitors the internet traffic on Britain's fiber optic network,[32] and that MI5, Britain's security service agency, intends to deploy technological measures to enable filtering key words and specific data in all information traffic in the country.[33]

The exposure of the surveillance programs in the United States raised the issue of privacy and limiting the power of the government as well as the possibility of imposing legal sanctions against the parties that share their information. So far, the United States Supreme Court has rejected lawsuits against local telecom giants and confirmed the legality of submitting information regarding Internet and telephone use to legal and intelligence agencies.[34] Still, the possibility of lawsuits against an organization that shares information is an obstacle to sharing that the government would like to remove.

Since the end of 2011, legislation on cyber information sharing has been advanced.[35] The purpose of the proposed law is to allow private and public

companies, in the context of cyberwar, to share information in real time with the government, law enforcement and intelligence agencies without risking lawsuits for violating secrecy or privacy. The bill passed in the House of Representatives, went through a round of adjustments in the Intelligence Affairs Committee,[36] and is still in the process of legislation in the Senate. Its opponents claim that it violates the Fourth Amendment to the Constitution,[37] which defines parameters for search and seizure of citizens' personal information, such as warrants or reasonable grounds. According to opponents of the bill, the new legislation would allow intelligence agencies to receive personal or commercial information from infrastructure and content providers without the checks delineated in the Fourth Amendment. Groups dealing with the problems inherent in the bill[38] are trying to enlist public support to oppose and prevent it from becoming a law, by running a campaign in the social media and on the internet in the United States.

The tension between supporters and opponents of cyber information sharing legislation is not unique to this area, but touches on the entire issue of privacy in the interface between the state and its citizens and the involvement of Big Brother. An example of a similar conflict may be found in the Smart City initiative in Britain, which includes covering cities with cameras and face recognition software.

Concluding Insights

Trends in the contemporary development of the cyber threat phenomenon include using attack methodologies focused on specific targets rather than being randomized, crossing geographical and legal borders, taking advantage of unidentified vulnerabilities, and using bits of malicious, modular code in cyberspace. The attackers maintain a flourishing, structured community with internal order and a supporting system of financing, allowing easy and rapid sharing of attack information. It seems that the realization of the community model on the defensive side and transitioning from a paradigm of isolated organizations to an information sharing initiative will lead to better results. In a broader view, one of the most significant resources coming into being in the 21st century is the wisdom of crowds. One can see examples of crowdsourcing in many fields and, in this sense, cyberspace is no exception.

The transition to models of sharing is supported by the congruence of interests of most of the market forces involved, including regulatory bodies,

governments, law and intelligence agencies, solution manufacturers and service providers, and even the organizations themselves. The value of sharing with external elements is, among other things, a product of the isolated organization's inability to fight its cyberwars on its own. Sharing contributes not only to significantly strengthening the security system and its survivability, but also to the organization's business success as it saves on investment, is granted preferential treatment by the regulatory bodies, and more.

The architecture of the solution and developing standards will, in the future, make it possible to create a technological structure connecting organizations while keeping their assets separate. They will also support links among separate sharing systems that can connect one another into a hierarchic structure of information, such as sharing within a market segment that will interface into cooperation at the national level.

Some of the success of the entire standardization process depends on support from the market forces. In this case, it seems that elements in the US administration, especially the Department of Defense, are determined to promote the process. Nonetheless, we still don't see effective large-scale information sharing because of the many challenges, not necessarily technological, and at times because of the conservative approach of organizational decision makers.

As the field comes of age, we may first expect to see sharing among similar organizations in the same sector and, later on, the implementation of information sharing on a larger scale. Shared interests, similar organizational cultures, and inter-organizational dependencies increase the chances of success of the initiative and reduce its risks.

Two of the prominent obstacles to sharing are the organizations' concern that if systems are linked, sensitive internal information may be exposed to the competition, and that they may receive incorrect cyber information because of the poisoning of a shared database, which might damage service provision. One can significantly reduce the risks inherent in both by technological means and standardized processes and protocols implemented both on premise and in the central sharing entity.

The greater challenge is faced by organizations whose business is essentially linked to cyberspace, such as security solutions, software products and services manufacturers, and the large project and integration bodies in the field. The question remains: is it possible to formulate a

worthwhile working model among these manufacturers so that they will share cyber information, even though security and cyberspace are part of the field in which they compete? Such a model must include both elements of competition and of cooperation (coopetition) in a way that would provide advantages to each of the partners over time.

The disagreement between supporters and opponents of information sharing will continue. Given that, and given all the aspects of the topic discussed in this essay, the question that must be asked is this: is there a different paradigm in the world of information technology that would allow dealing with current and future cyber challenges without the need for sharing, or is there no choice but to join forces in the battle and rapidly adopt uniform standards for a sharing infrastructure? Either way, such an infrastructure must maintain a balance between individual rights and the state's ability to defend its infrastructures, assets and citizens.

Notes

1 A zero day attack exploits a security breach in the attack target's component that is unknown to the component's manufacturer or anyone else other than the attacker, or one that is known to the manufacturer but for which it has yet to distribute a patch.

2 One study conducted in the past year by the RAND Corporation analyzes the way in which cyberspace black markets are constructed and operate, surveys historical trends, and provides forecasts for the future. Researchers at the institute conducted in-depth interviews with experts who are officially and unofficially involved in these markets, including academics, security researchers, journalists, security providers, and law enforcement personnel. The report concluded that the black markets in cyberspace are a multi-billion dollar industry with solid infrastructures and a clear social and organizational structure. L. Ablon, M.C. Libicki and A.A. Golay, *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

3 The approach supporting compartmentalization of cyber information is described in many sources as part of an organization's preparation for a cyber event. An example is the preparation model suggested by SANS, taken from a course dealing with the topic. E. Skoudis, ed., "Security 504: Hacker Techniques, Exploits & Incident Handling," *SANS Institute* (2006).

4 L.A. Gordon, M.P. Loeb and W. Lucyshyn, "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting & Public Policy* 22, no. 6 (2003): 461-85.

5 Basel III is a regulation in the field of finance that includes a chapter requiring financial organizations to share cyber information as part of their operational risks. For more information: *Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems*, http://www.bis.org/publ/bcbs189.pdf.

6 A standard which includes guidelines on cybersecurity, and the demand that organizations share information. "ISO/IEC 27032:2012–Information Technology–Security Techniques–Guidelines for Cybersecurity," July 16, 2012, http://www.iso.org/iso/catalogue_detail?csnumber=44375.

7 The three fundamental elements of CIA represent the classic basic principles of cybersecurity: confidentiality–protecting the contents from being read by unauthorized personnel; integrity–protecting the contents from alteration by unauthorized personnel; and availability–keeping the information and systems available.

8 TCG website, http://www.trustedcomputinggroup.org/.

9 "Cyber Information-sharing Models: An Overview," MITRE, October 2012, http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

10 Information fusion is a process designed to link and cross-reference data, information and knowledge in order to find correlations for the purpose of improving the ability to locate and identify entities about which information is being gathered, and for the purpose of assessing a situation and ranking risks. In addition, an assessment of the outputs quality is made and demands are created for information sources, as an integral part of the fusion process for the sake of improving the outputs.

11 Database poisoning using false information is liable to obstruct the organization's activity, internally or vis-à-vis outside bodies (denial of service). The advantage of an automated system of sharing is also its greatest disadvantage, and it is more prone to such poisoning than a manual sharing system because it does not include human monitoring in real time.

12 S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," February 2014, http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.

13 M. Davidson, C. Schmidt, "TAXII Overview," version 1.1, January 2014, http://taxii.mitre.org/specifications/version1.1/TAXII_Overview.pdf.

14 "CybOX–Cyber Observable eXpression–A Structured Language for Cyber Observables," 2014, http://cybox.mitre.org/.

15 An example of a fundamental architecture of sharing relating to the issue of trust in the context of academic research is an architecture called PEI proposed by Krishnan and colleagues. It includes three required layers: the policy layer, which sets out the goals of sharing and the articulation of objectives; the enforcement layer, which includes the basic solution architecture; and the implementation layer, which entails delving into the technological level of the details of sharing. R. Krishnan, R. Sandhu, and

K. Ranganathan, *PEI Models towards Scalable, Usable and High-Assurance Information Sharing* (New York: ACM, 2007), pp. 145-50.

16 The federally-financed MITRE research institute delineates the stages and decisions that must be made as part of a process of constructing a sharing model. Those decisions include the sharing architecture, the model of trust among the participants, automation of sharing, operations and participants. V.B. Bakis, "Cyber Partnership Blueprint: An Outline," MITRE, October 2013, http://www.mitre.org/sites/default/files/publications/Bakis_Partnership_Blueprint_Outline_0.pdf; The Bipartisan Policy Center has come up with a model in which a central body serves as a clearance center for shared information of critical infrastructure institutions in the United States. "Cyber Security Task Force: Public-Private Information Sharing," Bipartisan Policy Center (BPC), July 2012, http://bipartisanpolicy.org/library/cybersecurity-task-force-public-private-information-sharing/.

17 A. Merchant-Dest, "How the Department of Defense and the Department of Homeland Security are Taking Steps toward Information Sharing," *Federal Blue Print*, March 2014, http://federalblueprint.com/latest-news/department-defense-department-homeland-security-taking-steps-toward-information-sharing/.

18 The South Korean research team's experiment proves that sharing information among different parties (zones) shortens response time to attacks and raises the level of security. V. B. Chang, D. Kim, H. Kim, J. Na, and T. Chung, "Active Security Management Based on Secure Zone Cooperation," *Future Generation Computer System* 20, no. 2 (2004): 283.

19 The Israeli Ministry for Environmental Protection, "Procedures and Guidelines on Emissions of Industrial Pollutants." http://www.sviva.gov.il/subjectsEnv/SvivaAir/Industry/Pages/Regulations.aspx.

20 APT is a collection of cyber attack tools and methods aimed at a specific target and controlled by professional hackers, and which can therefore be developed and operated in a way that makes it very difficult to identify using standard security measures.

21 These two attack technologies reduce the effectiveness of the traditional security mechanisms whose main function is to identify clear patterns of attack. They require behavior based reference in order to identify the threat and a transition from developing signature based security products to behavior based anomaly detection products. Two of the main challenges in the latter is the need to create an organizational behavioral baseline that documents the normal behavior of the organization and its computer systems in order to identify anomalies, and the risk to disruption of legitimate transactions because of false positives.

22 Also called Managed Security Service Provider (MSSP).

23 K. Hausken, "Information Sharing among Firms and Cyber Attacks," *J. Account Public Policy* 26, no. 6 (2007): 639-88.

24 An example of a nation's strategy in constructing a national cyber system may be found in a document of the Finnish government that includes visions and principles in building a cross-organizational cyber system and a list of concrete recommendations to make it happen. *Finland Cyber Security Strategy*, Secretariat of the Security Committee, 2013, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

25 The British government's national program for confronting cyber threats. *The National Cyber Security Strategy, Our Forward Plans–December 2013*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf.

26 The US-CERT–United States Computer Emergency Readiness Team website, http://www.us-cert.gov.

27 The Information Analysis and Sharing Centers website– the National Councils of ISACs, http://www.isaccouncil.org/memberisacs.html.

28 *The Multinational Cyber Defense Capability Development (MNCD2) Program*, http://mncd2.ncia.nato.int/Pages/default.aspx.

29 *The Cyber Security Data Exchange and Collaboration Infrastructure (CDXI*); L. Dandurand, *Cyber Security Information Exchange*, http://www.rsaconference.com/writable/presentations/file_upload/sect-t08-cyber-security-information-exchange.pdf.

30 L. Tabanski, "International Cooperation in Critical Infrastructure Protection against Cyber Threats," *Atlantic Voices* 2, no. 9 (2012), http://sectech.tau.ac.il/node/114.

31 Electronic surveillance program carried out by the NSA, starting in 2007, to gather information for the purpose of intelligence from infrastructure, software and contents providers (Google, Yahoo, Microsoft, Apple, Skype, AOL). This activity was revealed through Edward Snowden's leaks to *The Guardian* in 2013.

32 E. MacAskill, J. Borger, N. Hopkins, N. Davies, and J. Ball, "How does GCHQ's Internet Surveillance Work?" *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

33 Monitoring technology allowing the filtering of key words in internet traffic is called "deep packet inspection."

34 The United States Supreme Court rejected a lawsuit against the giant telecom companies Verizon, Sprint and AT&T, and confirmed the legality of transferring information from emails and phone conversation to the NSA. B. Kendall, "High Court Lets Telecom Firms Wiretap Immunity Stand," *Wall Street Journal*, October 9, 2012, http://online.wsj.com/news/articles/SB10000872396390444024204578046312896501562.

35 The Permanent Select Committee on Intelligence, 2013, *Cyber Intelligence Sharing and Protection Act of 2013*, http://intelligence.house.gov/bill/cyber-intelligence-sharing-and-protection-act-2013.

36 The modified bill after the changes is called: "Cybersecurity Information Sharing Act of 2014." Continuous updating on the status of the legislation may be found at the Library of Congress, http://thomas.loc.gov/home/thomas.php.

37 The Fourth Amendment reads as follows: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

38 Two of the institutions active on the topic are the Electronic Frontier Foundation (EFF) and Fight for the Future. Both are running a campaign called "CISPA Is Back" to gather citizens' signatures on a petition against the legislation. http://www.cispaisback.org.

Developments in Iranian Cyber Warfare 2013-2014

Gabi Siboni and Sami Kronenfeld

In the course of 2013, Iran became one of the key players in the international cyber warfare theater. This development is a result of both defensive and offensive cyber force buildup processes and a measured relaxation of restraints on the part of Iranian decision makers with respect to offensive activity in cyberspace. Indeed, the Iranian activity points to major qualitative advances in Iran's technological and operational cyber capabilities. This article examines the activity and progress in Iran's cyber defense system, and the regime's use of this capability to restrain internal opposition. In addition, it looks at the offensive dimension, particularly cyber-attacks traced to Iranian agencies, agents, and allies.

Keywords: cyber, Iran, cyber security, cyber defense, networks isolation

Introduction

In an interview to the Atlantic Council, an American research institute, a senior source in the CrowdStrike Cyber Security Company rated Iran as a "third tier" country in regards to its cyberspace capabilities, stating that its cyber warfare capabilities were substantially inferior to those of "first tier" countries, such as the US, Russia, and the UK, as well as "second tier" countries such as China. This conception is in line with many Western intelligence specialists and administration officials. Iran is perceived as capable of harassing Western security systems and damaging "soft" targets, while lacking the knowledge and means to execute strategic cyber-attacks.[1] Nevertheless, during 2013, Iran became one of the key players in the international cyber warfare theater. It appears that this development is

Dr. Gabi Siboni is a senior research fellow and head of the INSS Cyber Warfare Program. Sami Kronenfeld is an intern in the Cyber Warfare Program at INSS.

This article was first published in *Military and Strategic Affairs* 6, no. 2 (2014): 83-104.

a result of a combination of a measured relaxation of restraints on the part of Iranian decision makers with respect to offensive activity in cyberspace, and a major qualitative advance in the Iranian cyber warfare apparatus, which has surprised many Western experts in the extent of its activity, its professional sophistication, and its ambitious selection of targets.

Events such as the Stuxnet attack, severely damaging Iran's centrifuges, and the widespread protest that accompanied the 2009 elections in Iran – in which social networks and the internet played a major role in organizing protests and escalating events – have turned cyberspace into an important theater for the Iranian regime. These events and other cyber-attacks against Iran have led the regime to establish a ramified cyber apparatus, including operational frameworks with a command structure and professional echelon specializing in a variety of areas. Iran has invested over $1 billion in developing technologies, setting up infrastructure, and training defensive and offensive personnel.[2] Iranian cyber strategy is devised and overseen at the highest levels, among them the President, commander of the Revolutionary Guards, and senior ministers serving on the Iranian Supreme Cyberspace Council – the senior agency coordinating the country's cyber activity.[3]

This article seeks to present an up-to-date analysis of Iranian activity in cyberspace. The article is divided into two parts; the first examines Iran's cyber defense system's progress and activity, and the use of these capabilities to restrain its internal opposition. The second examines the offensive dimension, mainly through cyber-attacks traced to Iranian agencies, agents, and allies. Concluding insights are provided at the end of the article.

The Defensive Concept

Iran is aiming to create a multi-level defense system combining security, monitoring, and supervising technologies with physical enforcement mechanisms for the aggressive pursuit of operatives operating against the regime in cyberspace. To this extent, Iran is taking action through three main channels: first, it is creating a protective envelope against attacks on its essential infrastructure and sensitive information, such as the Stuxnet attack that damaged its uranium enrichment program. Second, it is striving to neutralize cyber activity executed by opposition groups and opponents of the regime, for whom cyberspace constitutes a key platform for communications, information distribution, and organized actions against the regime. Third, it aims to prevent harmful Western content and ideas

from infiltrating Iran's internal cyberspace – ideas that could contribute to the development of a "soft revolution," undermining the regime's stability.

The targets and operational principles of the Iranian cyber defense apparatus, dictated by Iran's Supreme Council of Cyberspace, are implemented by central government agencies, such as the Passive Defensive Organization (belonging to the army), the Supreme Council of the Cultural Revolution (subject to the Supreme Leader), the Iranian Police, and Ministry of Communications.[4] Some of the technological and organizational infrastructure established by Iran has matured during the past year into operational agencies significantly contributing to strengthening Iranian defensive operations in cyberspace.

The Networks Isolation Project – Disengagement from the World

The Networks Isolation Program is one of the Iranian regime's main strategies in cyberspace. The project began materializing as early as 2009, when Iran's objective was to transfer the cyber activity in the country to an internal communications network, dubbed Halal Internet, isolated from the World Wide Web. The Iranian network was designed to operate in the spirit of the Shiite Muslim norms encouraged by the regime, and to enable the government to completely control and supervise the network's content, information, and users. From the regime's perspective, the establishment of an intranet network and the separation of Iranian cyberspace from global cyberspace is a key measure in strengthening its defense against cyber-attacks and espionage, preventing penetration by Western elements that do not coincide with those of the regime, and neutralizing its internal opposition.[5]

The first evidence of the Iranian network's operation was discovered in October 2012, when American cyber researchers, in cooperation with Iranian sources, noticed that Iranian Internet providers have begun allocating two IP addresses to every computer connected to the Internet – an ordinary internet address and an internal Iranian address, which could be accessed only from inside the country. The researchers estimated that the internal Iranian network was capable of managing 17 million IP addresses and that more than 10,000 home, commercial, and government computers were connected to it during 2012. In 2013, Halal Internet began to accumulate content (censored and supervised, of course), with a strong emphasis on development of local versions of popular internet services, such as e-mail, social networks, video and audio communications, map websites, and video websites.[6]

In July 2013, the Iranian regime inaugurated an e-mail service, @post.ir, requiring civilians to register and designed to constitute the main channel of communication between private citizens and the various governmental agencies. This service, which supports Farsi, English, French, and Arabic, is capable of providing e-mail addresses to about 100 million users. Each user is allocated a 50-megabyte mailbox, which can be expanded to up to two gigabytes. Opening the mailbox requires a person to give his name and address, and it appears that the email addresses provided are not encrypted – therefore enabling the regime to closely supervise the users and traffic in these addresses.[7] In December 2012, the Iranian State Broadcasting Authority launched a YouTube-like website under the name of "Mehr," displaying supervised content and enabling surfers to upload their own content under strict censorship rules.[8] The Iranian authorities also banned the use of foreign Information Security software, as they developed a local anti-virus system called "Padvish." According to Iranian sources, this system can protect networks and prevent malware penetration.[9]

In order to increase the number of Halal Internet and Iranian Internet services' users, the regime expanded its use of technological and legislative measures restricting Iranian citizens' possibilities for accessing the World Wide Web. The Iranian authorities blocked the use of Voice-over-IP software, such as Skype and Google Talk. Use of many VPN and TOR networks as well as filtering evasion software, important tools in bypassing government supervision and censorship of cyberspace, was also banned.[10] In addition, the Iranian cyber authorities began to deliberately slow external websites and Internet services (mainly services by Google, which are very popular in Iran), at times reaching 6 percent of the ordinary speed. The authorities are also carrying out websites and services migrating blocks, and are greatly restricting traffic on the encrypted Internet. These actions pose technical, legal, and psychological difficulties for Iranian citizens seeking to surf the World Wide Web, and are, in effect, forcing them to use the supervised and censored Halal Internet.[11]

Development of Defense and Supervision Technologies

As a supplementary measure to isolating the networks, Iran is investing in the development of its own cyber technologies and defense tools in order to reduce its dependence on foreign products that may prove to be Trojan Horses. A well-publicized ceremony attended by senior Iranian defense officials, including Minister of Defense General Hossein Dehqan

and Civil Defense Unit Commander Gholam Reza Jalali in December 2013 unveiled 12 technological developments by Iranian industry, including a secure cellular telephone designed to provide users with a communication line impenetrable by electronic surveillance, a secure operating system designed to eliminate Iranian dependence on American operating systems, a GPS device, an optical communications system, software and systems against malware and a firewall. A system for identifying a cyber-attack, and equipment for information security centers were also unveiled at the conference.[12] Furthermore, the Iranian news agency ISNA reported that Iran had begun using a national cyber protection system called "Shahpad." According to Mohammed Naderi, head of the project, the system facilitates fusing information from a variety of user stations and sensors, and generates an overall nationwide cybernetic picture. In case of an attack, Shahpad immediately informs the data security centers in the country, enabling them to respond quickly, and to take action to block the attack.[13]

Iran is not relying solely on local development in order to reinforce its cyber security capability. In September 2012, it signed an extensive technology cooperation agreement with North Korea including information technology. According to experts, it is very likely that the two countries that have both been targets of cyber-attacks, and both regard this field as strategically important, will combine forces under this agreement to develop information security, monitoring, and even offensive technologies.[14]

Iran is also cooperating with China in the cyber field, and previously purchased a surveillance system from a Chinese company named ZTE Corp., making it possible to monitor voice communications, text messages, and Internet browsing.[15] Cooperation with these and other countries, such as Russia, is of great assistance in strengthening Iran's cyber defense and ability to conduct surveillance of the Internet and its own citizens' usage.

Strengthening Defensive Deployments

Beyond the technological aspects, Iran is placing special emphasis on reinforcing various state agencies' ability to face and thwart cyber-attacks. The Iranian cyber apparatus had conducted a number of comprehensive cyber defense drills training civilian and military units. In addition, a cyber-war exercise was conducted as part of naval maneuvers by the Revolutionary Guards in the Strait of Hormuz in December 2012. As part of this exercise, a cyber-attack was launched against the fleet's computer network in order to retrieve information and insert malware. The commanders of the exercise

declared that the attack had been detected and foiled by the fleet's cyber defense system.[16]

In February 2013, the Iranian Fars News Agency, which is close to the regime, reported a comprehensive drill by the Revolutionary Guards' ground forces, examining and assessing the organization's cyber defense systems.[17] Another drill took place in October 2013 as part of the Passive Defense Organization's general defense maneuvers. As part of this drill, key government agencies' cyber defense apparatuses were examined, including nuclear installations, the Tehran metro subway network, the Iranian Broadcasting Authority, ports, the Iranian Central Bank, and the cellular communications' providers. According to the Passive Defense Organization commander, many security breaches in these organizations' cyber defense systems were found and managed. Following the drill, it was decided to establish a cyber-defense center at the Natanz nuclear facility.[18]

Restraining Regime Opponents

Iran is supplementing the technological measures it is taking in order to protect its cyberspace with aggressive physical enforcement action against its opponents at home, who use cyberspace extensively for subversive purposes. A key player in the Iranian regime's efforts to control its cyberspace is FATA, the Cyber Police, founded in 2011 under the command of the Iranian Police. Over the past year, FATA has become more aggressive in its efforts to enforce censorship restrictions and prevent subversive activity in cyberspace. The agency is engaged in locating and apprehending bloggers, online journalists, and opposition members supporting and voicing ideas and views that run contrary to the regime's positions.

The intense aggression against the regime's opponents exhibited by the Iranian Cyber Police gained global attention in November 2012, following reports of the death of Iranian blogger Sattar Beheshti in a prison near Tehran. Beheshti, who was arrested by FATA after he published a blog voicing criticism of the Iranian legal system (which he called "Khamenei's Slaughterhouse"), died as a result of torture and severe beating by the Cyber Police.[19] Reports of his death aroused a wave of criticism both within and outside Iran. As a result, the European Union imposed sanctions on FATA and other parties involved in his death, including judges and officials responsible for censorship in Iran.[20] International pressure led to the dismissal of the Cyber Police commander in Tehran,[21] but according to

international human rights organizations, FATA is persisting in its strategy of widespread arrests and aggressive action to locate and punish Iranians expressing opposition to the regime on social networks and in blogs.[22] In recent months, the Iranian Cyber Police tightened its supervision of the popular Internet Cafes, closing dozens for violating the state's stringent registration laws and restrictions.[23]

The regime's supervision and enforcement became particularly intensive and thorough in the months leading up to the presidential elections on June 14, 2013. Two days prior to the elections, Google reported that it had detected and thwarted a phishing attack launched by parties inside Iran aimed at tens of thousands of e-mail accounts belonging to Iranian citizens. The attack included sending an e-mail disguised as a maintenance message from the Gmail system asking the user to type in his e-mail user name and password. The information typed was then transferred directly to the attackers, providing them with untrammeled access to the user's e-mailboxes.[24] An analysis of the attack raised the suspicion that the attackers were the same Iranians who attacked the Dutch DigiNotar company's servers in 2011.[25] The attackers' targets were unclear, though it appears there is a close connection between the attack and the election campaign, and that the attackers wanted to enable the Iranian authorities to collect information about the actions and opinions of Iranian citizens, and to take action against "problematic" elements.[26] In addition, in the weeks leading up to the elections, a broad cyber-attack took place against Iranian opposition and communications websites. A group of hackers calling itself "The Unknown Cyber Jihad," and, claiming affiliation to Hizbollah, broke into a number of Iranian opposition websites and replaced their content with a message aimed against the regime's opponents. Key opposition websites, such as the Communist Movement in Iran, the Green Movement, and human rights websites, were blocked by the regime for many hours, and dozens of online activists and journalists were arrested and imprisoned by the Iranian security forces.[27]

Following the events that accompanied Ahmadinejad's re-election in 2009, Iranian activity against the opposition and opponents of the regime has developed and become more advanced. At the time, the opposition used cyberspace with relative ease to organize demonstrations, distribute ideas, and transmit information about events in Iran to a target audience outside of the country (mainly through the use of VPN networks). In the 2013 elections, however, the Iranian cyber apparatus was technologically

and operationally prepared and ready to control the dialogue that took place on the internet, and monitor subversive activity and the outwards flow of information from within Iran.

It appears that to date, the Iranian cyber defense system still has a long way to go before it is able to deal effectively and consistently with highly sophisticated cyber-attacks, such as Stuxnet and Flame, and to prevent any penetration by external content or ideas. Some describe this apparatus as no more than an improvised and less organized version of the Chinese "Cyber Wall."[28] Nevertheless, the great technological and organizational strides that Iran has made over the past year indicate a steep learning curve, and that it is likely to devise an effective and comprehensive defense system earlier than expected.

The Offensive Aspect – The Search for "High-Quality" Attacks

The Islamic Republic of Iran regards cyber warfare as an effective platform enabling it to inflict damage on enemies in possession of clear military superiority, while at the same time maintaining room for denial in order to avoid international condemnation, or even sanctions and counterattacks. This conception had led Iran to use cyber warfare as an important tool for attacking Western targets in response to sanctions, and as a means of deterrence against escalating sanctions actions against Iran by Western countries. The scope, targets, and relative success of cyber-attacks conducted over the past year and their attribution to Iranian groups indicate increased Iranian capabilities. Intelligence and administration officials in Israel and the US have also expressed concern regarding the speed of Iranian cyber warfare capabilities' development.[29]

Western sources attribute the progress in Iran's cyber warfare program to its success in integrating its capabilities, know-how, and trained personnel from Iranian computer science faculties[30] with the Iranian hacker community's extensive experience and highly developed abilities, many of whose members identify with the regime and its goals. The Iranian hacker community is one of the most dominant and active communities worldwide, and evidence suggests connections between its various groups and the Revolutionary Guards. The use of hackers, whose connections to the Iranian regime are vague, provides room for ambiguity and deniability when facing accusations of involvement in malicious and illegal cyber activity.

One of the leading Iranian hacker groups is the Ashiyane Digital Security Team, which is believed to have connections with the Revolutionary Guards, and whose members are ideologically motivated to support the Iranian regime and the revolution.[31] The Zone-H website, specializing in analyzing hacker activity in cyberspace, rates Ashiyane as second in the world in the number of websites into which its members have succeeded in breaking and corrupting, usually by replacing the content with the group's icon, or with pro-Iranian propaganda. The websites broken into by Ashiyane members include 26 Brazilian government websites, among them the Military Police website, and government websites in the UK and Pakistan.[32] According to Zone-H, besides Ashiyane, there are seven other Iranian hacker groups among the world's 40 most active hacker groups involved in corrupting websites. Such attacks are considered relatively minor, but they indicate a high level of technological capabilities, and in many cases serve as cover for information theft or introduction of malware and Trojan Horses.

Another factor contributing to the Iranian cyber warfare program's rapid progress is the Iranian cyber system's close relations with cyber criminals, hackers, and information security experts, primarily Russian, who are willing to hire out their capabilities for money. American sources regard these connections as a key element in Iran's rapid progress, and Congressman Michael Rogers, Chairman of the House of Representatives Select Committee on Intelligence, also stated that the wave of cyber-attacks against American banks' websites, which was attributed to Iranian groups, showed signs of involvement by Russian groups.[33] In addition to "importing" personnel, Iran can also purchase a powerful and technologically sophisticated cyber weapon which is available on the black market to the highest bidder. This Cyber Weapon enables the Iranians to rapidly enhance their capabilities and the threat posed by them.[34]

The Iranian cyber warfare capabilities' progress is reflected in a series of attacks that occurred in the second half of 2012 and in 2013, utilizing more sophisticated techniques, attacking high quality targets, and on a larger scale than earlier attacks attributed to Iran. One attack attributed to Iranian groups began in September 2012 and continued into 2013, including a large-scale attack on the websites of key banks and financial institutions in the US. Information security experts described this attack as "unprecedented in scope and effectiveness." Its uniqueness and quality lay in the method employed by the attackers: instead of attacking through

breaches in individual computers, they routed their attacks through data centers' computer networks. These data centers, operated by companies like Google and Amazon.com, are composed of giant computer networks connecting hundreds, sometimes thousands, of servers and computers, providing cloud computing services to a large number of companies and businesses throughout the world. The attackers succeeded in taking over part of these computing "clouds," utilizing their enormous computer power as a platform for attacks on the websites of US-based banks and financial companies. Security specialists described this maneuver as the "cybernetic equivalent of turning a Chihuahua into a fire-spitting Godzilla."[35]

A group of hackers calling itself Izz a-Din al-Qassam Cyber Fighters assumed responsibility for the service-denying attack against the websites of important banks in the US, which included Bank of America, Citigroup, and HSBC. Members of the group exploited the data centers' computer platform to channel enormous volumes of traffic to the banks' websites, causing them to crash and denying their customers access to their accounts. In addition to using traffic, the attackers employed a technique called Encrypted DDos (distributed denial of service). This method exploits the banks' own information encryption mechanisms, whose operation requires major system resources. The attackers flooded the banks' websites with transactions requiring encryption, thereby substantially slowing and hindering their activity. Nevertheless, the bank accounts were not broken into during the attacks, and customers' money was not stolen.[36]

Information security experts state that the high level of capabilities required to carry out an attack on such a large scale and with such great technological sophistication indicates that a country must be involved. An attack against a country's financial infrastructure, especially an economic power like the US, has serious consequences, and is liable to cause severe economic damage as it disrupts many commercial companies and households' regular financial activity.

Despite Iranian denials and the absence of physical proof, senior US administration and intelligence officials are convinced that Iran is behind the attacks as a response to the international sanctions against it and the cyber-attacks that damaged its infrastructure, for which it holds the US and Israel responsible. The US Secretary of Defense at the time, Leon Panetta, commented on the attacks against the banks, saying that they constituted a "significant escalation," without mentioning Iran by name.[37]

Another wave of attacks attributed to Iranian groups focused on American infrastructure and energy companies. It began to gather steam in early 2013, until the US Department of Homeland Security decided in May 2013 to issue an exceptional warning to energy and infrastructure companies regarding the escalating cyber threat to their computer networks. This warning stated that these were not routine attacks for the purpose of stealing information, industrial espionage, or inflicting damage on administrative systems; they were attacks seeking to gain control of their systems and damage their physical operations or the safety equipment of critical infrastructure, such as oil and gas pipelines and electrical systems. The American administration did not officially declare Iranian involvement, but experts and administration officials said that there was operational evidence indicating that the attacks had originated on Iranian soil, and that carrying them out required at least some support from the agencies in charge of Iranian cyberspace.[38] Any future sanctions escalation against the Iranian energy market is likely to cause Iran to take strategic measures against the international energy market, both as a deterrent measure and in order to increase the demand for its oil. [39]

Experts describe the attacks on the American energy companies' computer networks as a large-scale information collection operation, learning and assessing the systems in order to create knowledge infrastructure and gain experience in preparation for a future attack on the control systems that operate and regulate critical infrastructures' activity. Harming these systems is liable to cause significant damage and even loss of life on a large scale. Indeed, in the course of the attack, the attackers succeeded in bypassing some of the security systems and collecting information about their structure, capabilities, and their security breaches.[40] A senior source in Mandiant, an Information Security company, said that in at least one case, its investigators had succeeded in tracing the attack to a group of Iranian hackers whose connections with the regime were unclear. He added that the attackers' goal, moving within the American computer systems and studying their detection and security array, was to accumulate experience with "live" networks, and to explore their weak points.[41] Senior American officials stated that the attacks against the energy companies and the hackers' relative success indicated that the cyber offensive capabilities at the Iranians' disposal were improving and developing rapidly.[42] If Iran

obtains effective offensive capabilities against essential infrastructure systems' control, this is likely to constitute a strategic threat to its enemies.

Another significant attack attributed to Iran occurred in September 2013, when official US sources reported that an unclassified US Naval computer network had been compromised. The sources said that the attack had been committed by a group of hackers operating in the service of the Iranian regime, or at least with its consent and support. The network affected was the fleet's internal network, which, while unclassified, is used for correspondence and communications, among other things, and contains sensitive information, such as e-mail addresses of the fleet commanders and of senior officials. Administration sources reported that the attackers had succeeded in penetrating the network management systems, but claimed that no significantly valuable information had been stolen, and that e-mailboxes had not been broken into. Particularly alarming was the fact that the hackers continued operating in the fleet's computer network even after American security agencies had reported their successful removal from the network. The Iranian sophistication revealed in this attack is another sign of the development and progress in Iran's infiltration capabilities, and of Iran's readiness to target military cyber systems.[43]

In addition to the series of attacks against American institutions, groups affiliated with Iran assumed responsibility during the past year for cyber-attacks against Israeli institutions. In June 2013, Prime Minister Benjamin Netanyahu announced that there has been a steep rise in the Iranian cyber-attacks against important computer infrastructure in Israel.[44] In December 2013 and January 2014, a group of Islamic hackers calling itself The Islamic Cyber Resistance Group (ICRG) claimed that it had conducted a number of high-quality attacks against targets in Israel and the Middle East in revenge for the killing of senior Hezbollah leader Hassan al-Laqqis. The group, extensively publicized by the Iranian Fars News Agency, claims that it managed to penetrate the Israeli Civil Aviation Authority control systems, and was able to remain undetected within the system for months. In addition, the group claimed that it had succeeded in stealing sensitive information, and could, had it chosen to do so, take over the Authority's navigation and communications systems causing an air disaster.[45] ICRG also proclaimed that it had succeeded in penetrating the IDF computer servers, stealing secret information, such as the personal files of IDF soldiers, lists of officers, passwords, residential addresses and e-mail addresses, and

military codes. Aside from the attacks against Israel, ICRG announced that it had managed to break into the Saudi Arabian army database and the computers of companies owned by the Bin Laden family.[46] At the same time, sources in Israel stated that the rumored attacks boasted by the group were false, and were no more than propaganda and psychological warfare on the part of Iran.

In the midst of these events is the mysterious death of Revolutionary Guardsman Mojtaba Ahmadi, found dead in early October 2013. Reports in the West indicated that he had served as commander of the Revolutionary Guards' Cyber War Headquarters. His death was attributed to Israel at first, but the Revolutionary Guards strongly denied this allegation, stating that his death had resulted from a "strange accident."[47] Despite the great obfuscation surrounding this event, the possibility that Ahmadi's death had consequences for the organization's activity in the cyber sphere cannot be ruled out.

The Cyber Warfare Agents

Along with Iran's government cyber apparatus and its cooperation with the hacker community, Iran is redoubling its attempts to expand and strengthen its allies' cyber capabilities. It appears that Iran is seeking to create an effective system of agents acting in cyberspace on its behalf. One of its main foci in this area is Syria, which has strategic importance for Iran. At the beginning of the Conflict between the Assad regime and the rebel forces, the Iranians began to finance, equip, and train the Syrian security forces in methods of monitoring and controlling cyberspace, used by the rebels as a an important platform for organizing activity against the regime. Iranian advisers and specialists trained and reinforced the Syrian cyber police, and helped conduct surveillance of the computer and cellular networks in the country, thereby damaging the rebel's ability to transmit messages and information, both within and outside the country.[48]

A key player in this context is the Syrian Electronic Army (SEA). This group of Assad-supporting hackers began operating in 2011. During its first year of activity, it conducted mainly relatively amateurish vandalizing attacks against low-security websites that did not require significant technical ability: spam attacks, flooding talkback systems of various forums and news websites, etc.[49] In 2012, SEA began executing more complex operations against websites with a higher level of security, requiring greater technical

knowledge and capabilities. Western cyber experts and administration officials attribute this major improvement to the involvement and instruction of Iranian cyber warfare experts, training and equipping SEA's operatives. Former CIA Director and NSA Director Michael Hayden also stated that the Syrian group of hackers was for all intents and purposes, an agent of Iran.[50]

The development of SEA was reflected over the past year in a wave of attacks against communications agencies and human rights organizations' websites, perceived as hostile to the Assad regime. Among other things, SEA members attacked leading news websites, including the *New York Times*, BBC, al-Jazeera, the *Washington Post*, and the *Huffington Post*. The organization also attacked the Human Rights Watch website, which provides information about the number of civilians killed in battles in Syria. In addition, members of the organization succeeded in causing substantial damage when they took over the AP news agency's Twitter account, and published a false report about a supposed attack on the White House that injured President Obama. The report generated immediate panic on Wall Street, causing a nosedive in share prices and damage estimated at $136 billion. In April 2013, SEA assumed responsibility for crashing the Twitter Social Network, and for channeling surfers from the US Marines' recruitment website to a propaganda website against the rebels.[51]

Recently, it appeared that SEA had exhibited another major advance in its capabilities, and was beginning to use more sophisticated techniques and tools, such as phishing, malware, and Trojan Horses. Such tools have enabled the organization to carry out high-quality attacks against Internet communications companies' servers, such as TrueCaller which is the world's largest telephone index; the messaging and video service company Tango, and the communications applications company Viber. In the course of these attacks, the attackers succeeded in stealing huge quantities of information, such as personal information and e-mail addresses, which may very well have been handed over to Syrian intelligence and used to target the regime's opponents as well as for espionage.[52] The Iranian Fars News Agency also reported that the organization had attacked the water system of the city of Haifa,[53] but pictures attached to the report showed that SEA had merely penetrated the irrigation control system of a community in northern Israel.[54] Nevertheless, the attack on and penetration of the control system of Israeli infrastructure indicates an attempt by SEA to utilize and target more advanced cyber warfare methods.

These advanced capabilities, which many experts regard as the result of Iranian training, guidance, and assistance, have turned SEA into significant actor in the cyberspace arena, and have made cyber warfare in general a crucial element in Syria's deterrence strategy. When Syria sought to deter an American attack in response to the use of chemical weapons by Assad's forces, SEA operatives sent a message to the Reuters news agency saying that in the event of an American attack in Syria, the organization would escalate its attacks, and take action against more significant targets. Richard Clarke, Former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism and Special Advisor to the President on Cyber Security said that if the US attacks Syria, every response by Syrian agencies in cyberspace would be facilitated by Iranian groups.[55]

In addition to its support of the Assad regime's cyber capabilities, Iran continues its traditional support for its satellite and closest ally, Hizbollah's cyber deployment, which has become an active player in attacking Israel.[56] A report by the Meir Amit Center indicates intensive involvement and support by Iran for the Hizbollah's array of websites. These sites constitute a platform for propaganda and indoctrination in the ideas of the Islamic Revolution, including pro-Iranian propaganda, the glorification of Supreme Leader Khamenei and Hizbollah leader Hassan Nasrallah, and anti-Israel and anti-Semitic propaganda. The content of these websites was determined in cooperation with Iran, subject to the Iranian propaganda strategy. Part of the content is even operated from Iranian territory by parties close to the regime.[57]

Concluding Insights

Iran's cyber warfare capabilities are continuously progressing. Iran already constitutes a significant factor whose intentions should not be held lightly. It can be stated that the Iranian decision to operate in cyberspace on a large scale is due to two main considerations; the first is its experience as the target of serious cyber-attacks. As a country that had experienced the power and capabilities of a cybernetic attack, Iran recognizes the importance of establishing defensive capabilities and building and using attack capabilities. Iran's other motive concerns global technological development, allowing the expansion of its range of actions into cyberspace, in addition to the physical world. This development optimally fits in with Iran's asymmetric strategy concept.

An analysis of the cyber-attacks attributed to Iran and its satellites shows a broad range of targets, goals, and methods. One of the conclusions arising from this article is that Iran's cyber capabilities have recently matured on both offensive and defensive levels. Although it is likely that these capabilities are still inferior to those of the leading technological powers, it appears that the Iranians are bridging the gaps quickly and effectively.

One of the most dangerous trends in Iran's offensive cyber activity is its ability to target organizations and countries' core operational systems. These systems, controlling and overseeing manufacturing processes, supplies and essential services, are liable to be targets of Iranian attacks. Exploratory, scanning and learning actions discovered in the American energy companies' computer systems and traced to Iranian groups can be interpreted in only one way: Iran is trying to attain the capability and accessibility needed for an attack on critical infrastructure. This accessibility may avoid detection altogether, and can be utilized in the future for offensive purposes if Iran so decides. A successful attack on the energy, gas, and water facilities' control systems is liable to cause substantial damage. In the framework of the rules of the game, espionage and information theft in cyberspace is seemingly tolerable, but attempts to penetrate civilian infrastructure control systems cannot and should not be accepted. These attempts require a decisive response.

It appears that the realization that Iran poses a significant threat to its enemies in cyberspace is already inspiring close cooperation between the countries threatened by these capabilities. Upgrading intelligence and producing better defensive capabilities are not enough, however; they will never suffice against a determined enemy with operational, intelligence, and technological capabilities. Cyberspace makes possible a range of channels through which one can transmit messages below the threshold of physical warfare. These actions will require demonstration of the damage that Iran may suffer should it continue to act without restraint against sensitive targets. Particular information was recently published regarding a large-scale cyber offensive operation in Syria prepared by NSA in the spring of 2011, immediately following the outbreak of the Syrian civil war.[58] If this report is correct, the preparation of a cybernetic strike against Iran, combined with the occasional demonstration of qualitative capabilities, can help restrain its actions in the area of critical infrastructure.

Until a magic technological formula is found for identifying the source of cyberspace attacks at a level of certainty that can be legally proven, circumstantial evidence of the source of the attack can suffice in quite a few cases, and strong action in cyberspace below the physical warfare threshold can be taken against this source.

Above all, closer cooperation between the democratic countries is a cornerstone in facing Iran and its satellites. Better operational, intelligence, and technological connections are essential, as well as improvement in information sharing regarding the methods and tools used by Iran and its satellites. In addition, Israel is also likely to find allies against Iranian cyber warfare among the Sunni regimes in the Persian Gulf, headed by Saudi Arabia, which is under continual threat, and which has been damaged in the past by Iranian agencies. The cyber defense realm, in which Israel is a leader, is likely to serve as a basis for a fruitful strategic dialogue on broader regional issues, such as the Iranian threat in its general sense, the crisis in Syria, and the Palestinian issue.

The Iranian cyber deployment's aggressive behavior highlights the totalitarian character of the Iranian regime. Tight and intrusive supervision that violates the freedom of speech and expression of Iranian citizens, combined with the violence and aggression typical of agencies such as the Cyber Police, refute the image that the Rouhani regime is seeking to promote in order to break the international sanctions regime against Iran. Israel and other countries can use Iran's activities in cyberspace as an explanatory platform for highlighting the totalitarian and aggressive nature of the Islamic Republic.

This reality of Iran's rapid cyber warfare capabilities' development, its satellites, and its allies require Israel and other Western countries to act methodically and with determination to maintain their qualitative and operational edge in cyberspace. The importance of this space for Israel's security concept and the urgency of creating a "digital Iron Dome" were strongly emphasized by IDF Chief of Staff Lt. General Benny Gantz, who said he believed that Israel needed to do a lot more in the cyber realm: "We must not wait with this story."[59]

Notes

1 Barbara Slavin and Jason Healey, "Iran: How a Third Tier Cyber Power Can Still Threaten the United States," The Atlantic Council, 2013, http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf.

2 Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *The Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.
3 Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (2012): 77-99.
4 Ibid.
5 Majid Rafızadeh, "Iran's 'Halal' Version of the Internet," *al-Arabiya News*, July 12, 2013, http://english.alarabiya.net/view-renderer?mgnlUuid=cb92c5e3-f973-45ce-8d46-12b8fb4dfe17.
6 Sara Reardon, "First Evidence for Iran's Parallel Halal Internet," *New Scientist*, October 10, 2012, http://www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html#.UnZubT4UHVI.
7 Saeed Kamali Dehghan, "Iran Launches 'National Email Service,'" *The Guardian*, July 9, 2013, http://www.theguardian.com/world/2013/jul/09/iran-launches-national-email-service.
8 "Iran launches Own 'YouTube' Website," *AFP*, December 9, 2012, http://en-maktoob.news.yahoo.com/iran-launches-own-youtube-website-121634740.html.
9 F. Karimov, "Iran Introduces Domestically-Made Antivirus Padvish," *Trend News Agency*, June 30, 2013, http://en.trend.az/capital/it/2166121.html.
10 This blocking was accomplished, among other ways, by deliberately distributing malware disguised as filtering evasion software, which enabled the regime to trace illegal networks.
11 Urt Hopkins, "Why Iranians might Actually Use the Censored Halal Internet, " *The Daily Dot*, April 25, 2013, http://www.dailydot.com/society/iran-halal-private-internet-blocked-censorship; "Iranian Internet Infrastructure and Policy Report," *Small Media*, February-March 2013, http://smallmedia.org.uk/InfoFlowReportMARCH.pdf.
12 "Iran Unveils 12 Cyber Products," *Fars News*, December 14, 2013, http://english.farsnews.com/newstext.aspx?nn=13920923001322.
13 "Iran Launches Home-Made Defence Shield," *ISNA*, December 9, 2013, http://isna.ir/en/news/92091812343/Iran-launches-home-made-defense-shield.
14 Alastair Stevenson, "Iran and North Korea Sign Technology Treaty to Combat Hostile Malware," V3, September 3, 2012, http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware#.
15 Steve Stecklow, "Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012, http://graphics.thomsonreuters.com/12/03/IranChina.pdf.
16 "Iran for the First Time Stages Cyber Warfare Drill," *al-Arabiya*, December 31, 2012, http://www.alarabiya.net/articles/2012/12/31/257960.html.

17 "Drones, Cyber-Defence Feature in Iran Guards Drill," *Jerusalem Post*, February 23, 2013, http://www.jpost.com/Iranian-Threat/News/Drones-cyber-defense-feature-in-Iran-Guards-drill.
18 N. Umid, "Iran Holds Defence Exercises," *Trend News Agency*, October 22, 2013, http://en.trend.az/news/politics/2203465.html; "Iran Carries out Drills to Detect Cyber Vulnerabilities," *Tasnim News Agency*, October 22, 2013, http://www.tasnimnews.com/english/Home/Single/172473.
19 "Iranian Blogger who Told Supreme Leader Khamenei 'Your Judicial System... is nothing but a Slaughterhouse' Tortured to Death in Prison," *MEMRI*, November 19, 2012, http://www.memri.org/report/en/0/0/0/0/0/0/6819.htm.
20 European Parliament, *Resolution of November 22, 2012 on the Human Rights Situation in Iran, Particularly Mass Executions and the Recent Death of the Blogger Sattar Beheshti*, November 22, 2012, http://www.europarl.europa.eu/document/activities/cont/201301/20130109ATT58696/20130109ATT58696EN.pdf.
21 Thomas Erdbrink, "Head of Tehran's Cybercrimes Unit is Fired over Death of Blogger," *The New York Times*, December 1, 2012, http://www.nytimes.com/2012/12/02/world/middleeast/after-death-of-sattar-beheshti-iranian-blogger-head-of-tehrans-cybercrimes-unit-is-fired.html.
22 "Intelligence Ministry Admits Arresting News Providers, Blames Foreign Media," *Reporters Without Borders*, February 20, 2013, http://en.rsf.org/iran-intelligence-ministry-admits-20-02-2013,44099.html ; "Iran: Two Arrested for 'Insulting Regime Officials' on their Facebook Page, "*National Council of Resistance of Iran*, July 10, 2013, http://www.ncr-iran.org/en/news/human-rights/14138-iran-two-arrested-for-insulting-regime-officials-on-their-facebook-pa.
23 "Tehran Closes Dozens of Internet Cafes," *Mohabat News*, July 27, 2013, http://www.mohabatnews.com/index.php?option=com_content&view=article&id=7222:tehran-closes-dozens-of-internet-cafes&catid=35:inside-iran&Itemid=278.
24 Eric Grosse, "Iranian Phishing on the Rise as Elections Approach," *Google Blog*, June 12, 2013, http://googleonlinesecurity.blogspot.co.il/2013/06/iranian-phishing-on-rise-as-elections.html.
25 Siboni and Kronenfeld, "Iran and Cyberspace Warfare."
26 Betsy Isaacson, "Iran's Pre-Election Phishing Scheme Detected, Disrupted by Google," *Huffington Post*, June 13, 2013, http://www.huffingtonpost.com/2013/06/13/iran-phishing-google_n_3435811.html.
27 "Iranian Authorities Target Internet, Media before Elections," *CPJ*, June 13, 2013, http://www.cpj.org/2013/06/iranian-authorities-target-internet-media-before-e.php; Helle Dale, "Iran Clamps down on Dissidents before Election," *The Foundry*, June 12, 2013, http://blog.heritage.org/2013/06/12/iran-clamps-down-on-dissidents-before-election.

28 Neal Ungerleider, "Iran's 'Halal Internet' is really a 'Filternet,'" *Fast Company*, 2013, http://www.fastcompany.com/3009714/irans-halal-internet-is-really-a-filternet.
29 Thom Shanker & David E. Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers," *New York Times*, June 8, 2013, http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?nl=todaysheadlines&emc=edit_th_20130609&_r=4&pagewanted=all&.
30 Siboni and Kronenfeld, "Iran and Cyberspace Warfare."
31 Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," *A Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure, Protection and Security Technologies*, April 26, 2012, p. 5.
32 "Brazilian Military Police & 26 Govt Websites Hacked by Ashiyane Digital Security Team," *Hackread*, January 28, 2013, http://hackread.com/brazilian-military-police-26-govt-websites-hacked-by-ashiyane-digital-security-team.
33 Julian E. Barnes and Siobhan Gorman, "U.S. Says Iran Hacked Navy Computers ," *The Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB10001424052702304526204579101602356751772; Adam Kredo, Mike Rogers, "China, Iran and Russia Launching Cyber Attacks Against U.S. ," *The Washington Free Beacon*, July 22, 2013, http://freebeacon.com/mike-rogers-china-iran-and-russia-launching-cyber-attacks-against-u-s.
34 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers."
35 Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=1&ref=iran&&version=meter+at+6&region=FixedCenter&pgtype=Article&priority=true&module=RegiWall-Regi&action=click.
36 Ibid.
37 Julian E. Barnes and Siobhan Gorman, "Iran Blamed for Cyberattacks," *The Wall Street Journal*, September 27, 2013, http://news.walla.co.il/?w=/15/2569449, "Iran Launches Powerful Cyber Attack against Banks in US," Walla!, January 9, 2013, http://news.walla.co.il/?w=//2605254.
38 Ellen Nakashima, "U.S. Warns Industry of Heightened Risk of Cyber Attack," *The Washington Post*, May 10, 2013, http://www.washingtonpost.com/world/national-security/us-warns-industry-of-heightened-risk-of-cyberattack/2013/05/09/39a04852-b8df-11e2-aa9e-a02b765ff0ea_story.html; see also an analysis of the capabilities required to carry out a high level cyber-attack: Gabi Siboni, Daniel Cohen, and Aviv Rotbart, "The Threat of Terrorist Organizations in Cyberspace," *Military and Strategic Affairs*, Volume 5, No. 3, Institute for National Security Studies, December 2013,

http://d26e8pvoto2x3r.cloudfront.net/uploadImages/systemFiles/The%20Threat%20of%20Terrorist%20Organizations%20in%20Cyberspace.pdf; Nicole Perlroth and David E. Sanger, "New Computer Attacks Traced to Iran, Officials Say," *The New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html?_r=1&.

39 This article was written as nuclear negotiations were taking place between Iran and the great powers. One cannot rule out the possibility of escalating energy sanctions should the negotiations fail.

40 Siobhan Gorman and Danny Yadron, "Iran Hacks Energy Firms, U.S. Says," *The Wall Street Journal*, May 23, 2013, http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968.

41 Chris Strohm, "Iran-Based Hackers Traced to Cyber Attack on U.S. Company," *Bloomberg News*, May 14, 2013, http://www.businessweek.com/news/2013-05-14/iran-based-hackers-traced-to-cyber-attack-on-company-inside-u-dot-s-dot.

42 Shanker and Sanger, "U.S. Helps Allies Trying to Battle Iranian Hackers."

43 Barnes and Gorman, "U.S. Says Iran Hacked Navy Computers."

44 Gili Cohen, "Netanyahu Confirms: U.S. is Working with Israel on Cyber Defence, Iranian Attacks Increasing," *Ha'aretz*, June 9, 2013, http://www.haaretz.com/news/diplomacy-defense/.premium-1.528728.

45 "Israel's Aviation Agency under Muslim Hackers' Control for Months," *Fars News*, January 8, 2013, http://english.farsnews.com/newstext.aspx?nn=13921018001457.

46 "Saudi Army, Al-Qaeda Company, Israeli Army Hacked in Revenge for Assassination of Hezbollah Leader," *Fars News*, December 16, 2013, http://english.farsnews.com/newstext.aspx?nn=13920925001699.

47 Damien McElroy and Ahmad Vahdat, "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination," *The Telegraph*, October 2, 2013, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html; Lisa Daftari, "Internal Plot, not Israel, Eyed in Latest Hit on Iranian Scientist," *Fox News*, October 8, 2013, http://www.foxnews.com/world/2013/10/08/internal-intrigue-not-israel-eyed-in-latest-hit-on-iranian-scientist.

48 Simon Tisdall, "Iran Helping Syrian Regime Crack Down on Protesters, Say Diplomats," *The Guardian*, May 9, 2011, http://www.theguardian.com/world/2011/may/08/iran-helping-syrian-regime-protesters; Lisa Daftari, "Iranian General Admits 'Fighting Every Aspect of a War' in Defending Syria's Assad," *Fox News*, August 28, 2012, http://www.foxnews.com/world/2012/08/28/iranian-general-admits-fighting-every-aspect-war-in-defending-syria-assad; Geneive Abdo, "How Iran Keeps Assad in Power in Syria, "*Foreign Affairs*, August 25, 2011, http://www.foreignaffairs.com/articles/68230/geneive-abdo/how-iran-keeps-assad-in-power-in-syria.

49 Ronald Deibert, "Waging the Cyber War in Syria," *National Post*, May 21, 2013, http://fullcomment.nationalpost.com/2013/05/21/ronald-deibert-waging-the-cyber-war-in-syria.
50 Joseph Menn, "Syria, Aided by Iran, Could Strike Back at U.S. in Cyberspace," *Reuters*, August 29, 2013, www.reuters.com/article/2013/08/29/us-syria-crisis-cyberspace-analysis-idUSBRE97S04Z20130829.
51 Sarah Hurtubise, "Syrian Hacker Army Could be Advancing with Iranian Help," *The Daily Caller*, April 9, 2013, http://dailycaller.com/2013/09/04/syrian-hacker-army-could-be-advancing-with-iranian-help; Andrea Peterson, "The Post Just Got Hacked by the Syrian Electronic Army. Here's who they are," *The Washington Post*, August 15, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are.
52 Kenneth Geers and Ayed Alqartah, "Syrian Electronic Army Hacks Major Communications Websites," *FireEye*, July 30, 2013, http://www.fireeye.com/blog/technical/cyber-exploits/2013/07/syrian-electronic-army-hacks-major-communications-websites.html.
53 "Syrian Electronic Army Reveals Documents of Haifa Hack," *Fars News*, June 15, 2013, http://english2.farsnews.com/newstext.php?nn=9203180050.
54 Elad Salomons, "Did the Syrian Electronic Army Attack Haifa's Water Supply SCADA System?" *Water Simulation*, June 5, 2013, http://www.water-simulation.com/wsp/2013/06/05/did-the-syrian-electronic-army-attack-haifas-water-supply-scada-system.
55 Menn, "Syria, Aided by Iran, could Strike back at U.S. in Cyberspace."
56 Olivia Goldhill and Reuters, "Benjamin Netanyahu: Iranian Cyber Attacks on Israel 'Non-Stop,'" *The Telegraph*, June 10, 2013, http://www.telegraph.co.uk/technology/10110381/Benjamin-Netanyahu-Iranian-cyber-attacks-on-Israel-non-stop.html.
57 "Terrorism in Cyberspace: Hezbollah's Internet Network," *The Meir Amit Intelligence and Terrorism Information Center*, March 4th, 2013, http://www.terrorism-info.org.il/en/article/20488.
58 David E. Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times*, February 24, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?hp&_r=2.
59 Amos Harel and Gili Cohen, "2014: Iran out, Global Jihad in," *Haaretz*, February 1, 2014, http://d26e8pvoto2x3r.cloudfront.net/uploadimages/systemfiles/iran%20out,%20global%20jihad%20in.pdf.

Are Cyber Weapons Effective Military Tools?

Emilio Iasiello

Cyber-attacks are often viewed in academic and military writings as strategic asymmetric weapons, great equalizers with the potential of leveling the battlefield between powerful nations and those less capable. However, there has been little evidence to suggest that cyber-attacks are a genuine military option in a state-on-state conflict. In instances of actual military operations (e.g., Afghanistan, Georgia, Iraq, and Israel/Gaza), there is little accompanying evidence of a military conducting cyber-attacks against either a civilian or military target. Given that some of the nation states that have been involved in military conflict or peacekeeping missions in hostile areas are believed to have some level of offensive cyber capability, this may be indicative. More substantive examples demonstrate that cyber-attacks have been more successful in non-military activities, as they may serve as a clandestine weapon of subterfuge better positioned to incapacitate systems without alerting the victims, veiling the orchestrator's true identity via proxy groups and plausible deniability. Consequently, this paper provides a counter argument to the idea that cyber tools are instrumental military weapons in modern day warfare; cyber weapons are more effective options during times of nation state tension rather than military conflict, and are more serviceable as a signaling tool than one designed to gain military advantage. In situations where state-on-state conflict exists, high value targets that need to be neutralized would most likely be attacked via conventional weapons where battle damage assessment can be easily quantified. This raises the question: are cyber weapons effective military tools?

Key words: cyber-attack, cyber weapons, state-on-state conflict.

Emilio Iasiello has more than 12 years' experience as a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, as well as a private sector company providing cyber intelligence to Fortune 100 clients.

This article was first published in *Military and Strategic Affairs* 7, no. 1 (2015).

Terminology

There is no international consensus on the definitions for "cyber-attack" and "cyber weapon." However, it can be agreed that these terms refer to the execution of malware with the objective of denying, disrupting, degrading, destroying, or manipulating information systems or the information resident on them. Taking this into consideration, the following definitions have been adopted for this paper:

- **Cyber-Attack**: "actions taken through computer networks designed to deny, degrade, disrupt, or destroy an information system, an information network, or the information resident on them."
- **Cyber Weapon**: this paper accepts the definition created by Thomas Rid and Peter McBurney: "a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[1]Examples include distributed denial-of-service (DDoS) attacks and the insertion of malware designed to destroy information systems or the information resident on them.

Cyber as an Asymmetric Weapon

Military writings on cyber warfare – a subset of the larger information warfare umbrella – frequently cite critical infrastructures as key targets for military action during times of conflict, as they are seen as enablers of a nation state's military capabilities. The U.S. Department of Homeland Security defines critical infrastructures as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[2] Cyber-attacks in the information environment are important facets of force projection, particularly against soft targets such as communication systems, ports, airports, staging areas, civilian populations, critical infrastructure, and economic centers. In this context, cyber weapons are an ideal embodiment of an asymmetric strategy: the more technically sophisticated a powerful nation's information infrastructure, the more vulnerable it is to cyber-attacks.

Nation State Writings on Information Warfare

The fundamental principle of an asymmetric strategy is to convert the adversary's perceived strength into its weakness. Certainly, in no other area is this best exemplified than in the cyber domain where the very software and hardware complexities that increase military and societal effectiveness and productivity are also fraught with exploitable vulnerabilities. Academics and military theorists have been contemplating information warfare for many years. In the United States, the earliest reference to information warfare can be attributed to Dr. Tom Rona in the 1970s.[3] The first military adoption of this term was in 1992, when the U.S. Department of Defense published a more formalized definition of information warfare in its classified TS3600.1 policy document.[4] The U.S. military altered the definition throughout the years but the term had become part of its lexicon even if there were no formalized strategies to guide implementation during wartime.

The U.S. was not alone in cultivating progressive thinking on the nature of information warfare and how it could be leveraged for maximum effect. Chinese and Russian military theorists also wrote extensively on the topic. While initial writings seemed more of a mirroring of earlier published material, they did contemplate how such tools could be used as an implement of war. Despite cultural nuances, all agreed on the potential of information warfare as a weapon to bridge the differential gap between superior and inferior forces providing the latter with the means to strike without risking full force-on-force engagement. "Asymmetric" highlights this sentiment, and as one writer described it, is "roughly akin to the Japanese martial art of jujutsu, which is based on the idea that an opponent's strength and energy may be used against him rather than directly opposed with strength of one's own."[5] Unlike nuclear weaponry that requires significant resources and capability for production and management, information war and its instruments are easily accessible to the masses.

Chinese Writing on Information Warfare

The earliest Chinese writing on information warfare is probably the book entitled "Information Warfare," published in 1985 which had later become an article in the Liberation Army Daily.[6] However, it wasn't until Operation Desert Storm that Chinese theorists saw a military using advanced technology to defeat an opponent. In 1995, People's Liberation Army (PLA) Major General Wang PuFeng wrote "The Challenge of Information Warfare"

frequently referencing U.S. information warfare efforts against Iraq.[7] Another writer saw this battle as a "great transformation" where information and command and control revolutionized the battlefield.[8] Scholars considered "information dominance" a key concept to obtaining victory in future wars.

Two Chinese military doctrinal writings, the *Science of Strategy* and the *Science of Campaigns*, acknowledge information warfare as an important military tool for countering a superior adversary's informational and technological advantages. Influential military strategists from prominent Chinese military academies and schools have suggested that China's military should implement cyber or precision-weapon attacks against such critical infrastructure targets as ports and airports. Indeed, many of the more authoritarian writings regarding Chinese military thought advocate this course of action. In the *Science of Campaigns*, the author posits that information warfare is to be used:

> ...at the critical time and region related to overall campaign operations, to cut off the enemy's ability to obtain, control, and use information, to influence, reduce, and even destroy the enemy's capabilities of observing, decision-making, and commanding and controlling troops, while we maintain our own ability to command and control in order to seize information superiority, and to produce the strategic and campaign superiority, creating conditions for winning the decisive battle.

China's Integrated Network Electronic Warfare (INEW) theory places peacetime and wartime computer network attack and electronic warfare under one authority. Its mission is to disrupt the opponent's ability to process and use information. The strategy is characterized by the combined employment of network tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict.[9]According to Chinese thought, the strength of such attacks lies in its ability to surprise the enemy to great effect. A controversial text authored by two then- PLA colonels underscores the potential of cyber-attacks against the financial institutions of superior states,[10] particularly as a first strike option. According to James Mulvenon, a noted Chinese information warfare expert, "PLA writings generally hold that information warfare is an unconventional warfare weapon, not a battlefield force multiplier... that will permit China to fight and win an information campaign, precluding the need for military action."[11]

While information war encompasses a broader space of engagement, cyberspace is but one part of the larger information domain. Information space refers to "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself." [12] Per China's perspective, the main function of the information space is "for people to acquire and process data... a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases, and information, forming a landscape."[13] As such, China sees a larger threat space extending beyond the digital confines of the Internet.

Russian Writing on Information Warfare

Like China, Russia refers to "information space" as a holistic term. In 2010, the Russian government updated its Military Doctrine in which "cyber warfare" was notably omitted (like the Chinese, the Russians use the term "information" rather than the more popularized term "cyber"). However, there were several references to "information warfare" that by definition would include offensive attacks against information systems (i.e., computers) and/or the information resident on them. More importantly, the doctrine recognized the information space as a critical area that the military must protect from outside threats. This bolsters dictums in Russia's 2000 Information Security Doctrine, in which the protection against foreign harmful information and the promotion of patriotic values were identified as national security objectives.[14] Other objectives cited in the 2010 *Military Doctrine* include:[15]

> ...developing goals and resources for information warfare.....to create new models of high-precision weapons and develop information support for them...prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces.

Russian information warfare theory is rooted in the idea that Russia must "respond with war to the information war waged against Russia,"[16]and covers a broad range of actions including political, economic, cultural, and military, to name a few. Russian authors understand information warfare as influencing the consciousness of the masses as part of the rivalry between the different civilian national systems adopted by different countries in

the information space. These are put into effect by use of special means to control information sources as "information weapons."[17] Russia defines "information space" as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and the information itself."[18] As such, it is the technical (e.g., the physical destruction of an information system a la Stuxnet) and psychological (e.g., influencing and manipulating a population) effect of that space that worries Russia.

Consistent with this broad interpretation of the information space, Russia cites "information weapons" as weapons of concern. By their very definition, information weapons can be used in domains other than cyber, including the human cognitive domain,[19] and include geographic areas where the Russian language is used and a Russian diaspora exists.[20] Certainly Russia viewed the successes of the "Color Revolutions" and the "Arab Spring" as examples of failed information and social control.

U.S. Writing on Information Warfare

The U.S. views cyberspace as the networks and systems that comprise its architecture, rather than the entire information environment akin to the Chinese/Russian definition of information space. The U.S. has published numerous strategic and operational pieces providing insight into how the military should operate in the cyber domain via information operations (IO), of which cyber operations (aka "cyber warfare") is but one of several components. The 2011 Department of Defense's Strategy for Operating in Cyberspace as well as the 2012 revision of its Joint Publication on Information Operations (JP 3-13) reflects recent U.S. military thinking on cyberspace as a warfare arena. Indeed, the establishment of U.S. Cyber Command (CYBERCOM) is in line with the U.S. commitment to operating freely in cyberspace while hindering the adversary's capabilities. According to the Strategy document, CYBERCOM reflects the following goals:

> To ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.[21]

The JP 3-13 provides information as to the deployment of cyber capabilities. It sets forth doctrine and guidance governing the activities of the U.S. military in joint operations. According to JP-313:

> Information operations (which include computer network operations) are designed to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[22]

The key difference between the writings of China/ Russia and the U.S. lies in a holistic interpretation versus a more narrowed perspective of the threat space. China/ Russia prefer to combine the human and technological aspects, while the U.S. focuses solely on the technological aspects. The U.S. views a larger IO campaign as consisting of several separate, albeit possibly interrelated, military capabilities, whereas China/ Russia emphasize a more interconnected perspective where there is no clear separation between the activities conducted or the effects achieved. In this context, a cyber-attack can consist of malware deployment against a critical infrastructure (per the U.S. perception), or hostile information directed against the government or its populace by adversarial oppositionist forces (per the China/Russia perceptions).

Cyber-Attack Incidents

Several high profile cyber-attacks reveal an evolution from disruptive to destructive force. This is not to say that all future cyber-attacks will involve the destruction of information systems, only that in certain instances where opposing factions are entrenched in diplomatic confrontation, precedent has been established where destruction may be a viable option. In the incidents highlighted below, nation state direction or sponsorship was largely suspected but never proven, suggesting that if governments were involved in orchestrating attacks, they preferred to use them as surprise weapons during times of diplomatic tension, with plausible deniability, and in engagements with limited or non-existent force-on-force operations.

2013 South Korea Wiper Malware

In March 2013, "wiper malware" deleted data on three South Korean banks' systems and their insurance affiliates, as well as three broadcasting organizations. While the majority of the attacks occurred on March 20, evidence suggested that in some cases systems have been previously infected

with malware set to deploy on that date.[23] The malware overwrote the Master Boot Record of the computers running these networks, as well as disabling the antivirus program from a well-known South Korean company.[24] The attack was estimated to have compromised 48,000 computers.[25]

This event marked the fourth in a series of well publicized attacks employing wiper malware, the first being the April 2012 wiper malware against Iran's Khang Island facility, the second being the Saudi Aramco incident, and the third being the Qatari RasGas incident. Notably, this indicates a shift toward more destructive attacks by non-state actors during times of political tension. Like the Aramco incident, a previously unknown group ("WHOIS") claimed responsibility,[26] though the reliability of this attribution was called into question due to the questionable history and demonstrated capability to execute this level of attack.

South Korean officials believed North Korea military intelligence units were responsible, operating from Chinese IP addresses.[27] In the frameworks of the prolonged north-south conflict, political and diplomatic rhetoric has often spilled into the cyber domain at least since 2009 when botnets directed DDoS attacks against South Korean and U.S. websites.[28] Prior to March 2013, North Korea ramped up its threats against South Korea and the U.S. during the March 11-21 joint Key Resolve military exercises (which occurred right after the North Korean testing of its nuclear device in February 2013).[29] If North Korea was behind the attacks, they represented a divergence from a usually robust albeit benign DDoS activity. More importantly, the incident signaled to Seoul that the North was capable of conducting destructive cyber-attacks if it perceived transgressions against established "norms" between the two governments.

2012 Saudi Aramco Wiper Malware

In August 2012, a virus erased data on three-quarters of the corporate computers of Saudi Aramco, Saudi Arabia's national oil company, largely considered the world's most valuable company.[30] The malware was designed to accomplish two objectives: 1) replace the data on hard drives with an image of a burning American flag and report a list of infected addresses back to a computer inside the company's network, and 2) wipe the memories of the infected computers.[31] Labeled "Shamoon," the virus destroyed the hard drives on 30,000 computers.[32]

The event's significance lay in the fact that malware was purposefully deployed to destroy as many computer hard drives as possible in a company involved in critical infrastructure. The malware's sophistication is debatable; then-U.S. Defense Secretary Leon Panetta referred to the Shamoon virus as a very sophisticated tool,[33] while other security researchers from Kaspersky Lab suggested that coding errors in the code were indicative of amateurish work and the malware could have been more destructive.[34] The virus was released against Aramco the day before one of the holiest nights of the Islamic year.[35] This suggests that the attackers wanted to enhance operational success, correctly estimating that there would be limited monitoring during this period, allowing time for the virus to deploy and spread. The attack impacted oil production as well as business practices of the company as some drilling and production data was probably lost.[36] According to one source, it took ten days to replace infected hard drives.[37]

Though a previously unknown activist group called "The Cutting Sword of Justice" claimed responsibility for the attack, stating that it was a response to Saudi policies in the Middle East,[38] many people including unnamed U.S. government officials suspected Iranian involvement.[39] If Tehran was the orchestrator, it preferred to engage Saudi Arabia covertly using a proxy in order to maintain plausible deniability, particularly as the attack directly targeted a major global oil producer and critical infrastructure. While there has been no international consensus as to what constitutes a "red line" in cyberspace, it would stand to reason that the purposeful destruction affecting a global enterprise would be considered an act of force as defined by the International Humanitarian Law of Armed Conflict, which regulates the conduct of armed hostilities between nation states. In this context, the targeting of Saudi Aramco – a symbol of Saudi power – could be interpreted as an Iranian signal to Riyadh of its discontent regarding Aramco benefits from U.N.-imposed sanctions on Iran, as well as Riyadh's perceived collaboration with the U.S. over Iran's nuclear aspirations.

2010 Stuxnet Attack on Iranian Centrifuges

Stuxnet is believed to be closely related to three other equally, if not more sophisticated, malware items known as Duqu, Flame, and Gauss. Since their purposes are more consistent with cyber espionage, they are not included in the current paper.

In 2010, Tehran disclosed that a cyber-weapon, coined "Stuxnet" by a Microsoft researcher, had damaged gas centrifuges in an Iranian uranium enrichment facility. Stuxnet was described as a "highly sophisticated" and complex application designed for the sole purpose of sabotaging uranium enrichment centrifuges controlled by high-frequency converter drivers used by the uranium enrichment facility at Natanz.[40] Approximately 1,000 centrifuges were impacted by the malware, causing them to spin out of control and ultimately require replacement.[41]

Stuxnet was significant in that it was the first incident of a cyber-weapon created and deployed with the intent of degrading, disrupting, and destroying a specific information system. Perhaps more importantly, the malware's sophistication, as well as its clandestine appearance on an industrial control system network air-gapped from the Internet in a secured environment pointed directly at nation state sponsorship. Despite being discovered in 2010, Stuxnet is believed to have been deployed as early as 2009,[42] indicating that a surreptitious delivery against this target was a successful approach. No other group assumed responsibility.

Iran had made it clear on several occasions that it intended to exercise its sovereign right to develop its nuclear program for peaceful purposes,[43] causing great concern for the U.S., as well as other Western and Middle Eastern states, and even Iran-friendly China and Russia.[44] While Stuxnet remains officially unattributed to any government, it is widely suspected to be the result of a U.S./Israel partnership.[45] The successful deployment negated the need for a conventional military strike that risked escalatory retaliation. If the U.S. was behind Stuxnet, the incident could be interpreted as a U.S. signal to Iran that Washington remained committed to not allowing Iran to enrich uranium for weapons purposes, demonstrating that it was able to reach out and gain access to a sensitive and well protected facility with a weapon of destruction.[46]

2008 Georgia DDoS Attacks

In August 2008, Russian forces invaded Georgia as a result of Tbilisi's decision to launch a surprise attack against separatist forces in South Ossetia.[47] Prior to the Russian counter invasion, cyber-attacks were already being launched against Georgian governmental websites.[48] Lasting for most of August, these digital attacks consisted mostly of website defacements (particularly against government websites) and DDoS attacks that targeted

media sites, financial institutions, a Georgian hacker community site, and Georgian government sites.[49]

The cyber-attacks were notable for one main reason: they coincided with the Russian military invasion. In many ways, the 2008 cyber-attacks were very similar to the 2007 attacks: defacements and DDoS targeted the private and public sectors. The uniqueness of these attacks lay in their coordination and intensity, as opposed to gradual coordination as was the case in Estonia.[50] If the same actors or types of actors were involved, they made adjustments to their attack methodology for maximum effectiveness.

Like in Estonia, the attacks were attributed to Russian nationalistic hackers, with Moscow suspected as being their sponsor.[51] If Moscow was again the orchestrator, these attacks could be interpreted as a "lessons learned" exercise in targeting a country via cyber weapons. While infrastructure was the main target in Estonia, media and news organizations were the prime victims in Georgia. By targeting these outlets, the attackers sought to control Georgia's information space and prevent anti-Russian sentiment from being broadcast, a Russian information warfare concept conveyed by leading Russian information warfare theorists such as Igor Panarin.[52] Ultimately, however, these efforts to control information failed, with many believing that Georgia won the information war.[53] Nevertheless, this incident demonstrated that even during force-on-force engagement, Moscow preferred to maintain plausible deniability. One would think that once physical strikes were conducted, the need to conceal cyber operations – particularly if they were not seeking to destroy information systems or the information resident on them – would be moot, especially when considering a nation state that is equal to the U.S. in cyber capability.[54] Nevertheless, the Georgian DDoS attacks signaled to Russia's neighbors and former states that they may be targeted by the same type of activity should their governments enter heightened periods of diplomatic tension with the Russian Federation.

Actual Military Conflict

Not all military-on-military or force-on-force engagements featured cyber-attacks as a primary or supporting military component. This bears noting given that some of the countries involved are capable actors known to have formalized doctrinal writings on how cyber-attacks could and should be used in conflict scenarios. While the absence of strategic cyber-attacks

could be interpreted as a lack of viable strategic cyber targets, evidence suggests they were not employed largely because no strategic advantage would be gained, thereby calling into question the efficacy of cyber-attacks as viable weapons to achieve similar results as conventional weapons.

2014 Israel-Hamas Crisis

In July 2014, Israel launched a missile at Gaza's only electricity plant causing the termination of all electricity in the area, which would worsen existing problems with water and sewage, according to press reports.[55] The use of conventional weapons against this target could have been prompted by Israel's inability to successfully target the plant via cyber means. However, this seems implausible based on Israel's reputation as a leading cyber power and its suspected involvement in some well publicized cyber incidents such as the 2012 cyber-attacks targeting a power plant and other Iranian industries,[56] the 2010 Stuxnet attacks against Iranian nuclear centrifuges,[57] and the 2007 cyber-attacks against Syrian air defense systems.[58] In order to achieve the strategic objective of disabling a key target, it can be inferred that the implementation of kinetic weapons was preferred as a more reliable course of action to support the immediate objectives of the mission.

2014 Ukraine-Russia Crisis

During the 2014 Ukraine-Russia crisis, the Ukrainian telecommunications company Ukrtelecom reported that armed men raided its facilities in Crimea on February 28 and tampered with fiber optic cables, causing outages of local telephone and Internet systems.[59] Given assessments of Russia's proficiency in cyber operations,[60] as well as the fact that much of Ukrainian telecommunications was built when it was part of the Soviet Union, one would think that a cyber-attack would be a feasible course of action given knowledge of the target and the benefits of disrupting cyberspace. Previous Russian nationalist hacker activity (e.g., 2007 Estonia and 2008 Georgia) would further suggest that such an action could have been viable, if not preferential. However, cyber-attacks against the Ukraine did not ensue. Furthermore, while open source reports referenced "cyber skirmishes" transpiring between pro-separatist and pro-Ukraine interests, as of June 2014 there was no evidence of significant activity impacting key critical infrastructure or command-and-control targets.

2013 Syrian Civil War

According to a 2014 *New York Times* article, when Syria experienced an uprising against its government, the Pentagon and the National Security Agency developed a battle plan that featured a sophisticated cyber-attack on the Syrian military and President Bashar al-Assad's command structure.[61] However, according to the same article, President Obama turned it down (as well as other conventional strike options) based on the limited strategic value of the mission, coupled with the untested ability of cyber weapons during a military conflict.[62] The Obama administration remained unsure whether cyber weapons were a useful military tool, or if they should be reserved for covert operations.[63]

2011 Libyan Civil War

In 2011, the U.S. considered deploying cyber weapons against Libya. According to open source reports, the goal would have been to break through the Libyan government's firewalls to sever military communications links and prevent early-warning radars from gathering information and relaying it to missile batteries aimed at NATO warplanes.[64] However, once the U.S. militarily committed to the use of force, the U.S. relied on conventional weapons to accomplish the same task. While there has been some debate as to the reason behind this (two popular beliefs are that the U.S. did not want to show its capabilities, and it did not want to be the first to use cyber-weapons in this manner),[65] perhaps a more pressing concern was whether or not cyber-attacks could have achieved the same level of military effectiveness as conventional missile strikes.

Conclusion

There is little doubt that foreign governments are developing cyber capabilities, whether to bolster their respective intelligence collection apparatuses or as instruments of nation state power. The military and academic writings of three prominent nation states advocate the use of cyber weapons, particularly against critical infrastructures, in time of state conflict. History is ripe with incidents in which a military targeted an adversary's critical infrastructures during wartime for both tactical and strategic advantage. Therefore, it follows that computer-based weapons could be leveraged in a similar manner.

Nevertheless, most of the observed cyber activities executed against state targets have come during times of diplomatic tension and conducted largely by non-state actors operating as state proxies. Cyber-attacks have been most effective as first-strike weapons benefiting from surprise and the anonymity afforded to them by the difficulties of attribution. In conflicts where military forces were involved (and therefore the need for non-attribution is less important), there were limited instances where cyber-attacks were implemented as either a decisive or supporting component to achieving a military objective. In most cases, physical strikes were the chosen course of action, perhaps as a more reliable and expedient alternative.

In the immediate future, it appears that cyber weapons are better built for surreptitious activity and state signaling rather than as imposing wartime game-changers. That is not to say this will not change in time, but it is going to require nation states to actually use them during conflict, experience the problems that occur during their deployment, and apply lessons-learned to improve their effectiveness. Thus far, this has not been done begging the question: do cyber weapons have a role in conflict? As militaries include technology into their operations, the answer is "yes" – just not a resounding one.

Notes

1 Thomas Rid and Peter McBurney, "Cyber Weapons," *Rusi Journal*, February/March 2012, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf.

2 Department of Homeland Security, "What is Critical Infrastructure?" November 1, 2013, http://www.dhs.gov/what-critical-infrastructure.

3 Daniel T. Kuehl, "Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age," *International Law Studies* 76 (2002).

4 "DoD Directive TS3600.1," *IT Law Wiki*, http://itlaw.wikia.com/wiki/DOD_Directive_TS3600.1

5 Michael Breen and Johsua A. Geltzer, "Asymmetric Strategies as Strategies of the Strong," *Parameters* (Spring 2001), http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011spring/Breen-Geltzer.pdf.

6 Shen Weiguang, "Focus of Contemporary World Military Revolution—Introduction to Information Warfare," *Jiefangjun Bao* (November 7, 1995): 6.

7 Major General Wang PuFeng, *The Challenge of Information Warfare* (1995), http://fas.org/irp/world/china/docs/iw_mg_wang.htm

8 Liu Yichang, ed., *Gaojishu Zhanzheng lun* (On High-Tech War) (Beijing: Military Sciences Publishing House, 1993), p. 272

9 Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept on Information Warfare," *Journal of Defense Studies* 4, No. 2 (April 2010).
10 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), p. 168.
11 James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, Mulvenon and Yang, eds. (Washington DC: RAND, 1999), pp.175-86.
12 Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English," 2013 5th International Conference on Cyber Conflict, (NATO: CCD COE Publications).
13 Ibid.
14 Doctrine of Information Security of the Russian Federation. (2000). Taken from http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.
15 Russian Military Doctrine (2010). Taken from http://carnegieendowment.org/files/2010russia_military_doctrine.pdf
16 Jolanta Darczewska, "The Anatomy of Russian Information Warfare," *Point of View* 42 (May 2014), http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.
17 Ibid.
18 Giles and Hagestad, "Divided by a Common Language."
19 Ibid.
20 Darczewska, "The Anatomy of Russian Information Warfare."
21 Department of Defense "Department of Defense's Strategy for Operating in Cyberspace – July 2011," http://www.defense.gov/news/d20110714cyber.pdf.
22 Joint Publications 3-13 Information Operations," Department of Defense, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
23 Matthew J. Schwartz, "North Korea Behind Bank Malware, South Korea Says," *Dark Reading (*April 10, 2013), http://www.darkreading.com/attacks-and-breaches/north-korea-behind-bank-malware-south-korea-says/d/d-id/1109474?.
24 Michael Mimoso, "Theories Abound on Wiper Malware Attack against South Korea," ThreatPost (March 21, 2013), http://threatpost.com/theories-abound-wiper-malware-attack-against-south-korea-032113/77654.
25 Schwartz, "North Korea Behind Bank Malware."
26 "Wiper Malware Analysis Attacking Korean Financial Sector," Dell Secure Works (March 21, 2013), http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/.
27 Sean Gallagher, "North Korean Military Blamed for Wiper Cyber-Attacks against South Korea," ArsTechnica (April 10, 2013), http://arstechnica.com/security/2013/04/north-korean-military-blamed-for-wiper-cyber-attacks/.

28 Choe Sang-Hun and John Markoff, "Cyber-Attacks Jam Government and Commercial Websites in U.S. and South Korea," *New York Times* (July 8, 2009), http://www.nytimes.com/2009/07/09/technology/09cyber.html.
29 Comprehensive Nuclear Test Ban Treaty Organization, "On the CBTO's Detection in North Korea," February 12, 2013, http://www.ctbto.org/press-centre/press-releases/2013/on-the-ctbtos-detection-in-north-korea/.
30 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S Sees Iran Firing Back," *New York Times* (October 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.
31 Ibid.
32 Kelly Jackson Higgins, "The Long Shadow of Saudi Aramco," *Dark Reading* (October 14, 2013), http://www.darkreading.com/attacks-breaches/the-long-shadow-of-saudi-aramco/d/d-id/1140664?.
33 Phil Stewart, "Shamoon Virus Most Destructive Yet for Private Sector, Panetta Says," *Reuters* (October 11, 2012), http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012.
34 Fahmida Y. Rashid, "Coding Errors in Shamoon Malware Suggest It May Be the Work of Amateurs," *Security Week* (September 12, 2012), http://www.securityweek.com/coding-errors-shamoon-malware-suggest-it-may-be-work-amateurs.
35 Paul Roberts, "Whoddunnit? Conflicting Accounts on Aramco Hack Underscores Difficulty of Attribution," Naked Security (October 30, 2012), http://nakedsecurity.sophos.com/2012/10/30/whodunnit-aramco-hack/.
36 John Roberts, "Cyber Threats to Energy Security as Experienced by Saudi Arabia," Platts (November 27, 2012), http://blogs.platts.com/2012/11/27/virus_threats/#comments.
37 Roberts, "Whoddunnit?"
38 Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back."
39 Siobhan Gorman and Julian E. Barnes, "Iran Blamed for Cyber Attacks," *Wall Street Journal* (October 12, 2012), http://online.wsj.com/news/articles/SB10000872396390444657804578052931555576700.
40 Matthew Schwartz, "Stuxnet Launched by United States and Israel," *Information Week* (June 1, 2012), http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202.
41 Ellen Nakashima, Greg Miller, and Julie Tate, "U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post* (June 19, 2012), http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.
42 "Stuxnet Effect: Iran Still Reeling," Industrial Safety and Security Source (August 3, 2011), http://www.isssource.com/stuxnet-affect-iran-still-reeling/.

43 "Timeline of Iran's Controversial Nuclear Program," *CNN* (March 19, 2012), http://www.cnn.com/2012/03/06/world/meast/iran-timeline/.
44 Max Fisher, "Nine Questions about Iran's Nuclear Program You Were Afraid to Ask," *Washington Post* (May 19, 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/11/25/9-questions-about-irans-nuclear-program-you-were-too-embarrassed-to-ask/.
45 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times* (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.
46 Emilio Iasiello, "Cyber-Attack: A Dull Tool to Sharpen Foreign Policy," 2013 5th International Conference of Cyber Conflict, 2013, http://www.ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf.
47 Council of Europe Parliamentary Assembly Resolution 1633 (2008) on "The Consequences of War Between Georgia and the Russian Federation," available at http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=12031&Language=en.
48 EnekenTikk, KadriKaska, and LiisVihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defense Center of Excellence, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf
49 Ibid.
50 Eneken, Kadri and Liis "International Cyber Incidents."
51 Ibid.
52 Darczewska, "The Anatomy of Russian Information Warfare."
53 Clifford J. Levy, "Russia Prevailed on the Ground but not in the Media," *New York Times* (August 21, 2008), http://www.nytimes.com/2008/08/22/world/europe/22moscow.html?_r=0.
54 Keir Giles, "Information Troops – a Russian Cyber Command?" 2011 3rd International Conference on Cyber Conflict (CCD COE Publications: 2011), http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf
55 Alan Greenblatt, "Israeli Bombing Ruins Gaza's only Power Plant," *NPR* (July 29, 2014), http://www.npr.org/blogs/thetwo-way/2014/07/29/336386340/israeli-bombing-destroys-gazas-only-power-plant.
56 Rick Gladstone, "Iran Blames US and Israel for Spree of Cyber Attacks," *Sydney Morning Herald* (December 27, 2012), http://www.smh.com.au/it-pro/security-it/iran-blames-us-and-israel-for-spree-of-cyber-attacks-20121226-2bwa1.html.
57 Ellen Nakashima and John Warrick, "Stuxnet Was Work of US and Israel, Experts Say," *Washington Post* (June 2, 2012), http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

58 John Leyden, "Israel Suspected of Hacking Syrian Air Defenses," *The Register* (October 4, 2007), http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.
59 Polityuk, P. and Finkle, J. "Ukraine Says Communications Hit, MPs Phones Blocked." *Reuters* (April 3, 2014), Taken from http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304.
60 Smith, D., *Russia Cyberoperations* (Washington, D.C.: Potomac Institute Cyber Center, 2010), http://www.potomacinstitute.org/attachments/article/1273/Russian%20Cyber%20Operations.pdf.
61 David E. Sanger, "Syria Stirs New U.S. Debate on Cyberattacks," *New York Times* (February 25, 2014), http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html.
62 Ibid.
63 Ibid.
64 Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *New York Times* (October 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.
65 Jack Goldsmith, "Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya," Lawfare Blog (October 18, 2011), http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/.

The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case

Gil Baram

The past decade has witnessed rapid developments in computers and information technology, leading to far reaching changes in almost all areas of life, including the military and defense spheres. Many changes have occurred in the nature of warfare and the design of military forces, owing, among other things, to developments in strategic thinking and the formulation of military doctrines that are tailored to a changing reality. In the 1990s, attempts to assess the consequences of the transition to the information age for defense endeavors led to the emergence of the notion of a "revolution in military affairs – RMA." This notion was conceived as a result of new technological innovations that improved the quality and availability of intelligence, the flow of information, and the precision of weapons. In the ensuing years, especially in the 21st century, advanced technologies for cyber warfare were developed, changing the face of the battlefield and the pattern of modern military action.

The cyber technology used in warfare affects the way the latter is conducted. A country possessing this technology enjoys battlefield superiority, high quality and comprehensive intelligence, a precise and rapid attack capability, the ability to protect essential infrastructures, enhanced command and control capabilities, and so on. These capabilities contribute to a nation's power, and strengthen its national security. Cyber warfare technologies have the potential for enormous advantages, along with new and unfamiliar risks. Given the sweeping innovation in this field, the understanding of its nature and consequences has only begun.

Gil Baram is a Masters student in Security Studies at Tel Aviv University and a research fellow at the Yuval Ne'eman Workshop for Science, Technology, and Security.

This article was first published in *Military and Strategic Affairs* 5, no. 1 (2013): 23-43.

Many countries, headed by the US and Israel, have intensified their cyber activities in recent years. While this activity constitutes a source of strength for them, it also exposes their weak points; this is because the infrastructures essential for the functioning of each country have become dependent on computers. Discovering the optimal way of handling the threat posed by the technological development of cyber warfare has been a key challenge facing Israel in recent years.[1]

Israel's national interest focuses on maintaining its security against those seeking to harm it and undermine its very existence. This interest, along with Israel's geopolitical location, necessitates superiority in cyberspace as an integral part of its ability to defend itself against conventional and cyber attacks, and an integral part of its deterrent attack capability in the Middle East theater and beyond.

Israel is considered a global leader in its ability to handle cyber attacks. A comprehensive report that examined the preparedness of 23 countries in the cyberwar sphere accorded Israel the highest rating – four and a half stars out of five. The report indicates that at any given moment, Israel is subject to about one thousand cyber attacks. This figure particularly impressed the writers of the report, who praised the Israeli defense systems and noted that Israel was well prepared to deal with a cyber attack against it.[2]

The development of Israel's operational capabilities in the field of cyber warfare is a key element in maintaining its national strength. Its economy, industry, security, education, and preservation as a democratic, open, and established society depend mainly on its ability to protect its essential computer networks against an attack liable to disrupt its way of life. The increasing reliance on computer systems in Israel and throughout the world has brought new challenges with it, demanding immediate solutions at the national level.[3]

The aim of this article is to present the role of cyber warfare technology in Israel's security doctrine and to examine Israel's preparations for dealing with the cyber threat by evaluating three necessary levels: (1) formulating a regular strategy for handling the threat posed by the development of cyber warfare technology; (2) allocating resources and budgets; and (3) effecting changes in the manner in which Israel builds its forces. An assessment of government publications will presumably demonstrate the importance of this topic for decision makers and the resources they allocate for dealing

with it. The aim here is to portray the situation in Israel and attempt to point out the existing gaps in this field.

The article is based on current literature on the subject as well as unclassified public information that includes newspaper reports, press releases, government documents, and interviews with key people in the field. There are few official publications in Israel that deal with how to handle the cyber threat, especially in comparison with Israel's cyber attack capabilities. Therefore, given the nature of security in Israel, one can assume that a great deal of information on cyber operations and their budget allocations remains classified.

A number of difficulties encountered in this research are attributable to the fact that since this research field is relatively new, there is still not sufficient historical knowledge on the subject of the effect of the development of cyber warfare technology on changes in the existing strategies and the way forces are built. Nevertheless, because the field is very important, it is preferable to begin studying it in depth despite the existing knowledge gaps. While this study focuses on cyber warfare, which comprises the country's defensive and offensive preparations, it does not deal with the use of computers for communications and warfare management. Since computers are currently used in many communications and military operations, this area is very wide-ranging, and exceeds the scope of this article.

The Role of Cyber Warfare Technology in the Israel Security Concept

The many changes that have occurred in cyber warfare technology are challenging the current defense doctrine, and necessitate a renewed assessment of its basic concepts. A situation has emerged in which protecting essential energy, water, computer, communications, transportation, and economic infrastructures is of supreme importance in the civilian and the defense sectors alike. The necessary adjustments in the defense doctrine should therefore be made in order to be able to provide a solution to the new threats.[4]

In April 2006, a proposal was submitted to then-Minister of Defense Amir Peretz for a revision of Israel's security doctrine. A committee headed by Dan Meridor whose members included the chairman of the National Security Council, the head of the Israel Security Agency, the official responsible for security in the defense establishment, and others prepared the proposal.

The committee report indicated that Israel had entered an era of major and rapid strategic changes, including far-reaching technological changes.[5] Among other things, the committee recommended adding defense to the three traditional elements (deterrence, alertness, and decision),[6] and recommended in particular the procurement of unmanned aerial vehicles and the protection of the national computer systems against penetration by hostile parties.[7]

In the wake of the committee's discussions, the possibility of adding a fourth basic term to the "security trio," namely, "defense" or "protection," was raised.[8] Israel did in fact invest a large proportion of its budget and defense efforts in passive protection. In addition to passive protection tools, the "defense" idea was expanded to include tools for attacking individual targets aimed at thwarting high trajectory barrages and terrorist attacks below the escalation threshold.[9]

Defense is of supreme importance in the realm of cyber warfare because effective defense ensures that a country's essential computer systems continue to operate. Furthermore, advanced cyber capabilities enable a country to protect its critical infrastructures effectively, thereby providing a solution to the need for an active defense, as noted in the Meridor Committee report.

For a long time, it was common practice to refer to the protection of computer systems as "information security," reflecting the idea that the most important thing to be protected was sensitive information (classified or business information). Over the years, this approach evolved to encompass other threats besides an attack on information: disruption of services, paralysis of essential computer-based processes, and so on. At the national level, the concept of protecting computer systems has been extended, and can now be called "cyber defense."[10]

Since the committee report was published, the use of cyber technology for various warfare needs on the battlefield has risen steeply. It would therefore be appropriate to assess the role of cyber warfare technology in the processes of updating Israel's security doctrine.

A look at the history of Israel's wars reveals that technology has played a more important role from one war to the next, and has become more sophisticated with time. Basic differences exist between Israel and Arab countries, and there is a clear quantitative asymmetry. If we take the major quantitative gaps into account, Israel's relative advantage in diverting warfare

to the technological plane stands out. It is easier for Israel to contend with the Arab world in sophisticated air battles and cyber operations (according to foreign sources) than in throwing stones or hand to hand fighting. The quantitative gaps become less significant and high quality weapon systems and personnel become more valuable when more advanced technologies are involved. The IDF excelled at identifying the great potential inherent in computers, and began using various types of computer warfare as early as the 1990s.[11]

Dealing with the threat posed by cyber warfare technological developments fits in with the Israeli security doctrine: home-grown Israeli capabilities are used, relying on "Jewish" developments and inventiveness in combination with global technologies. This field is well known to young people living in Israel, which was dubbed the "start-up nation,"[12] and is based on the importance of quality over quantity.

It is evident that the three original pillars of the Israeli security doctrine are relevant for dealing with the cyber threat:

a. *Deterrence*. Advanced cyber capabilities will enable Israel to create deterrence against its enemies. One example is the Stuxnet virus, attributed to the US and Israel, which was perceived as a major advance in the two countries' cyber attack capabilities and the power of their effect, was widely reported in the global media, and helped strengthen Israeli deterrence.[13]
b. *Warning*. Cyber capabilities enable Israel to amass a large volume of information about its enemies while simultaneously denying them access to its own stores of information. Israel can thus be effectively alerted to their intentions against it.
c. *Decision*. Israel is one of the world's leading countries in cyber capabilities. These capabilities afford it an advantage in battle through the use of advanced cyber tools, which can tip the outcome in its favor. It is important to note that both the concept of deterrence and the concept of decision in the cyber sphere are elusive, and their significance in a cyber context has not yet been fully realized. Nevertheless, it is now clear that cyber superiority combined with advanced kinetic capabilities is likely to prove decisive in battle.

From Israel's inception until the present day, its security doctrine has rested on the principle that quality is more important than quantity. Cyber warfare technology is consistent with this principle: the use of cyber tools,

which requires the training of expert manpower rather than the exertion of great physical force, facilitates operations that help bolster Israel's deterrent capability, and garners it great prestige in the international arena.

Thus it appears that integrating cyber warfare capabilities into Israel's security doctrine can be relatively simple, if indeed this is done soon. These capabilities are consistent with the three basic principles on which the security doctrine is based. Furthermore, developing independent cyber warfare capabilities and tools clearly embodies the principle of quality over quantity: all that is necessary is a high level of trained manpower for developing systems that make it possible to carry out operations against remote targets without risking human life and without requiring many resources.

Formulating a Regular Strategy for Cyberspace

The cyber threat is a result of the critical role played by computer systems in the national infrastructures and everyday life. This virtual space was generated by the decentralized development of various systems and sectors in the context of accelerated economic and technological development, without any significant connections to security. When the need to deal with the security aspects of the cyber realm arose in recent years, it sparked the question of who was responsible for its security.[14]

Information security and protection of computerized infrastructures are not new topics in Israel. Israel was one of the first countries in the world to recognize the importance of protecting essential computer systems. As early as 1996, the government made decisions about the best method of defense against cyber attacks.[15] The Tehila Project ("Government Infrastructure for the Internet Age" – The Governmental Internet Service Provider), whose purpose was to protect the connections of government ministries to the internet and provide secure internet surfing for government ministries, was launched in 1997.[16] Later, in 1998, the Law for Regulating Security in Public Organizations, which dealt with defining essential computer systems and their security, was enacted.[17]

The Decision to Establish a National Information Security Authority

Israel does not have a regular publication in which it publishes its policy vis-à-vis dealing with the cyber threat. Most of the existing information is based on media reports and academic research. At the same time, a number

of published official decisions are shedding light on the situation. In February 2002, a ministerial committee for national security made a decision on the subject of "Responsibility for Protecting Computer Systems in Israel" (Decision B/84). This decision designed the outline for the protection of critical computerized infrastructures in Israel, thereby providing a basis for implementing the Israeli response to the cyber threat to essential national computer infrastructures. The decision provided for the establishment of two special agencies: a steering committee for regular examination of the identity of public and private entities essential for Israel's functioning, and a national authority for the protection of computerized systems.

Following the ministerial committee's decision, a steering committee was immediately convened, headed by the chairman of the National Security Council. The steering committee's goal was to formulate an array of measures for the protection of the country's essential computer systems. The committee set forth the principles of the protection doctrine, the threats involved, and the agencies that would be obliged to take protective measures.[18] It also acted as a team for guiding the National Information Security Authority for securing computer infrastructures in the Israel Security Agency (ISA).

The National Information Security Authority, which was established the same year, operates in the framework of the ISA Law. The Authority guides the entities defined as essential in matters of computer security and protection of networks, and supervises the implementation of information security and protection. It is also authorized to enforce sanctions against entities that fail to comply with its guidelines. Significantly, the various security agencies take independent action to protect critical infrastructures without any official guidance from the Information Security Authority.[19]

The Decision to Establish the Israel National Cyber Bureau

In November 2010, the Prime Minister authorized National Research and Development Council chairman General (ret.) Prof. Isaac Ben-Israel to present a working plan for a national initiative for coping with the cyber threat.[20] The initiative team's recommendation included the establishment of a national cyber defense bureau for promoting cyberspace defense in Israel (recommendation 1A) and expanding the ISA's authority to the civilian sector.[21]

The key document in the matter is the Cabinet resolution of August 7, 2011 on the subject of "promoting national capability in cyberspace."[22]

This decision provided for the founding of the National Cyber Bureau, and established its goal as "promoting national capability in cyberspace and improved handling of its current and future challenges." One of the Bureau's jobs is "to recommend a national cyber policy to the prime minister and the government, provide guidance for the relevant parties concerning the policy decided... implement this policy, and control its implementation."[23] The decision to establish the bureau, which was announced publicly, indicated significant progress in the government's handling of the cyber threat, and constituted a turning point on the issue.

While government agencies, military branches, and defense establishment entities are protected under the law, most of the business sector and ordinary civilians remain without adequate protection in this area. The business sector is not subject to official supervision, and is not subordinate to any national agency whatsoever that is responsible for checking its ability to handle an attack on its essential computer systems in an emergency. This is a significant weak point for Israel, whose economy depends on the production and export power of its business and industrial sector.[24]

Decision makers in Israel expect the next war to include the use of cyber warfare tools. In spite of this, there is currently no official agency in Israel directly responsible for the protection of the business sector. It is true that a national authority cannot replace the managers responsible for their businesses, but since some of the private organizations in the economy provide essential services for the continuation of normal life on the home front, there are grounds for government intervention in guidance, regulation, and supervision.[25]

With the establishment of the National Cyber Bureau, its chairman, Dr. Eviatar Matania, stated that in his opinion, there were five areas concerning cyberspace in which the state should intervene:

a. Creating a system-wide perspective on the national level: Cyber defense requires multi-system assessment because public systems and private and business systems are highly interdependent.
b. Pooling of resources, actions, and information: Pooling means consolidating resources from various sources into a single integrative entity for the sake of handling the threats facing Israel in an optimal manner.
c. Creating international cooperation: Israel should take the initiative in creating such cooperation by partnering with allies throughout the world.

d. Creating an arrangement in cyberspace: Standardization, licensing, and approval, as well as introducing a system in which organizations and individuals are able to protect themselves according to clearly defined standards.[26]
e. Promotion of processes by the state: Just as the state acted in the 1960s to promote aviation in Israel by establishing an aeronautics faculty at the Israel Institute of Technology (Technion), so it should supply tools and leverage as incentives for academic and industrial development in the cyber field.[27]

According to Matania, the goal of the National Cyber Bureau is to draft a general plan of action in the field of cyber defense: strengthening security in organizations by creating an arrangement tailored to the databases, encompassing various sectors, as well as an individual arrangement for each sector. Another element involves devising national programs, cooperation, and information sharing, especially between the defense and civilian systems.[28]

The substance of the Bureau's activity concerns the regulation, integration, and promotion of general government activity affecting the cyber realm from a broad perspective, both military and civilian. The Bureau acts in the spirit of the Cabinet decision, together with the relevant entities, to formulate a defense policy, devise a national defense doctrine, and generate cooperation between all the entities operating in the field. It also formulates comprehensive programs and constructs mechanisms for nurturing human capital in the cyber field; develops technological and research infrastructures in the universities and industry; promotes cooperation among the private business sector, the public sector, industry, the universities, and the defense establishment; promotes public awareness of the cyber threat, and so on.[29]

All this activity indicates that Israel has correctly identified the looming threat to its national infrastructures, and has acted to set up a defense apparatus at the national level. Two watershed events were the establishment of a national information security authority in 2002, and the Cabinet decision in 2011 to "promote national capability in cyberspace" and to establish the National Cyber Bureau. Nevertheless, the Israeli government has not yet disseminated a regular and unified strategy in this matter to the public.

Israel is one of the world's leaders in cyber capabilities. Typically, however, this is not appropriately reflected in the institution of a regular strategy or in a clear statement of an official course of action. It appears

that Israel has yet to formulate a strategy in this field,[30] and that most of the information comes from press releases and media reports, rather than from official government sources. The government has taken an official decision in the matter, but has not yet published an orderly strategy.

Allocation of Resources

This section will examine the budget and resource allocations for coping with the threat posed by the development of cyber warfare technology, on the assumption that a budget assessment will make it possible to draw conclusions about the importance of the subject for decision makers in Israel.

In 2007, the National Research and Development Council initiated and financed research on the topic "Indices for Science, Technology, and Innovation in Israel," in cooperation with the Central Bureau of Statistics. The purpose of the study was to examine the budget allocations for scientific and technological matters in Israel. The study showed that Israel had spent NIS 30 billion annually on civilian research and development (R&D) over the past decade. An examination of the proportion of GDP invested in R&D showed that Israel led the world in 2009 – 4.3 percent, as compared with a 1.8 percent average in Organization for Economic Cooperation and Development (OECD) countries. Most of this investment in Israel (79 percent) comes from the business sector. Direct government spending on civilian R&D totals NIS 5 billion, in addition to the funds allocated for R&D in the defense sector.[31]

The figures show that Israel and its business sector invest considerable amounts in R&D in the technological field. To this can be added the various budgets distributed over the past year for R&D in applied and theoretical topics in the cyber sphere.[32] The total figure means that we can assume that R&D in the cyber field is being budgeted because its growing importance for the nation's security has been acknowledged. The exact allocations have not been publicly disclosed.

One of the principal items in the 2011-2012 state budget consists of allocations for the "defense and public order category." This category includes the allocation from the general state budget for defense and public order. Funds from this budget are allocated to various defense agencies responsible for the cyber sphere. The budget for this category totaled NIS 61.8 billion in 2011 and NIS 63.4 billion in 2012. From these sums, the highest amount was allocated for spending on activities of the

Ministry of Defense, which accounted for 18 percent of the total budget spending.[33] It can be assumed that the Ministry of Defense also invests considerable amounts in the development of cyber warfare by agencies for which it is responsible.

Another recommendation by the National Cyber Initiative team was to establish a national R&D program for building cyber capabilities in cooperation with the defense establishment, the universities, and industry. The plan included a recommendation for directing the existing national resources and adding resources where necessary. The aim of all this is to place Israel among the five leading countries in the world in cyber capabilities by 2015.[34] While this does not necessarily involve military-security development, it is highly probable that at least some of the money will be allocated to cyber security development.

The Cyber Bureau Budget

In the August 2011 Cabinet decision to establish the National Cyber Bureau, it was decided that an allocation for the bureau would be made, via the Office of the Prime Minister, from Ministry of Finance sources.[35] The full budget allocated for the Bureau's activities is not mentioned in the decision – only a minor amount (NIS 4.5 million) allocated for "establishing and operating the Bureau" in 2011.

The Cyber Bureau budget is currently NIS 2.5 billion for the next five years – about NIS 500 million per year. Of this, NIS 100 million will be allocated from the state budget as a designated amount for the Cyber Bureau, and NIS 400 million will be given following a process of pooling money from various sources.[36] According to Major Tal, a senior figure in the Cyber Bureau, the Prime Minister regards the cyber field as being of the greatest importance, and is actively promoting it. There is a desire to develop the field, and the budget allocations reflect this. The cyber threat is gathering steam, and a long term program to guarantee its budget is being planned.[37]

A May 2012 Knesset Finance Committee meeting explicitly allocated money for the continuation of the Bureau's activity, in addition to the already allocated budget.[38] The Bureau's request, as submitted for the Committee' approval, included NIS 12 million for two main items. The first was an operating budget, including payment of salaries to Bureau staff, the creation of computer infrastructures, and physical security for

the classified agencies required for infrastructures of this type. The second was the initial budget funding for the Bureau's regular activity.[39]

In recognition of the importance of links among the universities, industry, and the Cyber Bureau, the Bureau, in cooperation with the Ministry of Science and Technology, allocated NIS 50 million over three years for scholarships and research in various sub-sectors of the cyber sphere in order to make Israel a global leader in the field.[40] In addition, the Chief Scientist of the Ministry of Industry, Trade, and Labor announced an NIS 80 million allocation for Project KIDMA[41] for the purpose of promoting R&D and entrepreneurship in cyber security.[42] Here, too, one can assume that some of these scholarships will be allocated to areas dealing with cyber warfare.

Given the paucity of statements dealing with this budget, it is difficult to make an accurate estimate of government investment in Israel for the purpose of coping with the cyber threat. Nevertheless, the figures presented above show that the threat posed by the development of cyber warfare technology has not escaped the attention of Israeli decision makers, and that considerable resources are being channeled into this field.

Public disclosure of cyber budget allocations began in 2011. Taking into account the defense establishment's leading role in the handling of cyberspace over the past decade and the secrecy surrounding it, it is almost certain that various allocations in this field are not openly publicized. At the same time, following the official Cabinet decision in August 2011 to establish the National Cyber Bureau, information about allocations for military buildup and R&D in the field began to be made public.

Changes in Force Buildup

Cyber warfare technology has altered the weapon systems used on the modern battlefield, rendering them more precise and effective. Following the many changes that have taken place in Israel's external environment, the security challenges facing it have multiplied, and the importance of intelligence in Israel's security doctrine has increased. Israel is now at the forefront of technology, and has integrated cyber technology tools on all fronts in order to deal with the threats against it.[43]

Developments of this type have had a considerable effect on the principles of warfare and the changes that have occurred in the structure of armies, including the IDF. Upon examining the role of technology in Israel's wars,

Prof. Ben-Israel asserted that a more technologically advanced battlefield signifies that flexibility and versatility play a more crucial role in modern warfare. For example, the Yom Kippur War clearly demonstrated that constructing electronic weapon systems against the enemy's known threats was insufficient; it is necessary to construct them so that they will be able to handle changes made by the enemy in the electronic parameters of its systems during the course of the fighting.[44]

Following is an analysis of the principal changes in the government and defense establishment agencies in Israel, given the growing recognition of the risks resulting from the development of the cyber threat and the appearance of cyber technology on the battlefield.

The National Cyber Bureau

In August 2011, the Prime Minister announced the establishment of the National Cyber Bureau, whose main function is to strengthen capabilities for the defense of Israel's critical infrastructure systems against terrorist cyber attacks by either foreign countries or terrorist groups.[45] The Bureau, which has been operating for over 18 months and is in the throes of a growing process, currently consists of four main departments: security, civilian, intelligence and situation assessment, and organization and policy. In addition, a control room that operates 24/7 and is in continuous contact with the security agencies dealing with the field has been established in Jerusalem. The control room facilitates a comprehensive perspective of all the threats as well as the possibilities for coping with them, so that when a cyber attack against one agency takes place, it will be possible to know in real time which other agencies should be protected.

The Cyber Bureau is responsible for three main areas:

a. Formulating Israel's official security doctrine in cooperation with the agencies responsible for defense. The doctrine operates on two levels: increasing the general level of security and increasing the level of national security.
b. Developing infrastructures and promoting Israel's leading position in the cyber field, among other things by increasing its human capital and supporting the topic of scholarships for cyber-related research.
c. Taking the lead in national cyber processes, such as by regulating the security market, creating national security infrastructure through

legislation and emergency exercises, bolstering relations with various countries, and so on.[46]

The decision to establish the Bureau was an important step in Israel's engagement with the cyber challenge. It is still vital, however, to ensure that the Bureau acts according to a national strategy, to be formulated as soon as possible. Given Israel's procrastination in setting an orderly and publicly declared strategy, it is highly important that the Bureau be granted wide-ranging authority. Only then can it begin to narrow the national gap in comprehensive strategic management of all the civilian and military entities operating in the cyber sphere.[47]

The National Information Security Authority

The oldest entity dealing with the various aspects of information security is the National Information Security Authority, a branch of the Israel Security Agency (ISA). This authority grew out of a unit that handled conventional information security for decades, until it became responsible in 2002 for instructing all the national civilian infrastructure entities in defending against a possible cyber attack.

The ISA was legally sanctioned to regulate agencies like the Israel Electric Corporation, Mekorot National Water Company, Israel Railways, and the natural gas companies. The categories of regulation include issuing instructions about how to prevent a remote hostile takeover liable to cause severe damage to critical systems by pressing a key, and the like. In recent years, the list of entities instructed by the Authority has been extended as a result of national recognition of the growing cyber threat.[48]

Tsafrir Katz, who until recently headed the ISA Technology Division, provided a rare insight into what goes on there when he said that 20 percent of ISA personnel were technology specialists. The character of the ISA has changed since the 1980s, when it was not technologically inclined. For several years, it was necessary to develop new forms of employment for younger people. From his perspective, this revolution continued throughout the past decade.[49]

The Israel Defense Forces (IDF)

In 2009, then-Chief of Staff Lieutenant General Gabi Ashkenazi defined cyberspace as "a strategic warfare and operating space for Israel." An IDF cyber bureau was then established to coordinate and guide the IDF's cyber

endeavors for the General Staff. This bureau was founded in Unit 8200 of the IDF Intelligence Branch.[50]

A cyber defense department, most of whose activity is classified, was set up in the C[4]I Corps (Teleprocessing Corps). The department enables operations on land, sea, and in the air to be conducted in an age when the IDF relies more than ever on computer technology. The department operates in cooperation with most of the IDF's elite units, utilizing an array of technological means to neutralize the enemy's cyber attacks.[51]

In order to protect the IDF's computer systems, the C[4]I corps developed a training program called the "Cyber Defense Course." In May 2012, the corps' first class completed the course. After a few months of intensive study, the soldiers were qualified to carry out defensive computer-mediated operations based on the developing technological reality.[52]

Ministry of Defense

In January 2012, it was reported that the Ministry of Defense was about to set up a special administration for cyber warfare, which would coordinate all operations by security agencies and the defense industries involved in developing advanced systems in the field. During that year, special cyber warfare sections were established in the main defense industries, namely, Elbit Systems, the RAFAEL Armament Development Authority, and Israel Aeronautics Industries. Israel Military Industries is also considering entering the field.[53] It has not yet been decided who will head the new administration, but according to defense sources, the decision to establish a new authority "will raise the endeavor to a new level."[54]

Israeli Law, Information, and Technology Authority

The Israeli Law, Information, and Technology Authority (ILITA) was established by the Ministry of Justice of Israel in September 2006 to become Israel's data protection authority. ILITA's mission is to reinforce personal data protection, regulate the use of electronic signatures, and increase the enforcement of privacy- and IT-related offenses.[55] It also acts as a central knowledge base within the government for technology-related legislation and sizable governmental IT projects, such as e-gov (available online government).[56] ILITA is currently investigating the particulars of an event in which a large amount of personal information, including credit card

data, was published on the internet by parties identifying themselves as Saudi Arabian hackers.[57]

"Available Government" – e-gov.il (Tehila)

The "available government" system was established in the Ministry of Finance's Accountant General's Department in 1997 as the Tehila unit. Its purpose is to enable people to carry out a broad range of operations through the internet, at the same time ensuring the security of the transferred information and safeguarding the user's privacy. The system utilizes many resources to safeguard privacy, including an expert information security team and some of the world's most advanced security technologies.[58]

Israel has done a good job of identifying the features of the cyber threat and making many corresponding changes in the way it constructs its forces: a National Information Security Authority has been established to deal with protecting the country's critical infrastructures; military agencies have instituted very important changes: the IDF Cyber Bureau was set up in Unit 8200, and the C^4I Corps has begun to develop a special cyber training program; the most important change was the establishment of the National Cyber Bureau, whose objective is to integrate cyber defense into both the various defense agencies and the civilian sector. A Law, Information, and Technology Authority has been set up to take responsibility for maintaining internet privacy and the security of personal information. It appears that over the past decade, particularly in the past two years, the state, recognizing that the cyber threat is liable to affect all facets of life, has stepped up its treatment of the cyber threat by establishing advanced designated entities.

Conclusion

Israel has been extremely efficient in identifying the features of the cyber threat arising from the development of cyber warfare technologies. It has begun to make the necessary changes, and there appears to be a close connection between how the cyber threat is addressed and national security. The handling of the problem focuses on three aspects: (1) defense organizations, the IDF, the intelligence community, and the defense industry, which as of now are taking independent action to protect their systems without direction from the ISA; (2) critical national infrastructures, which are subject to cyber attack, and which are being directed by the National

Information Authority; (3) the private sector, in which civilian companies are exposed to cyber attacks. Although this aspect is partially addressed by ILITA, the bulk of the problem is not addressed at all.[59]

The cyberwar is raging in full force, and Israel is a leading player in it.[60] The dry facts are impressive: a National Cyber Bureau has been established in the Office of the Prime Minister; grants totaling millions of shekels will be allocated for cyber research and educational activities in each of the next few years; responsibility in the IDF for cyber affairs has been divided between the Intelligence Branch (offense) and the Teleprocessing Branch (defense); and the National Information Security Authority is expected to broaden its operations.[61] It appears that the treatment of cyberspace is gathering momentum in a number of key aspects: information about government activity concerning the cyber threat is being openly published, special budgets have been allocated for research in the field, and an attempt is being made to provide the National Cyber Bureau with a regular budget. At the same time, various agencies have been set up or have been greatly developed for the purpose of handling the growing cyber threat in an optimal manner.

The rapid technological changes that have occurred in recent years have affected the priorities of decision makers in Israel in various ways. Official Cabinet decisions have been publicized, and special agencies have been designated to address the cyber threat. Nonetheless, although at first glance it appears that Israel has made great strides in dealing with the growing cyber threat, there is still room for taking additional measures in order to achieve a clearer definition of the preferred policy for handling the matter comprehensively.

Notes

1 Isaac Ben-Israel et al., "Cyber Warfare – Israel's Preparation for Attacks on Computer and Communications Networks," in Protocol No. 95 – A Meeting of the Science and Technology Committee, Monday, July 4, 2011, http://www.knesset.gov.il/protocols/data/html/mada/;2011-07-04.html.

2 According to a report published in February 2012 by an international defense think tank (Security and Defense Agenda – SDA), in cooperation with the McAfee information security company, "Cyber-Security: The Vexed Question of Global Rules – An Independent Report on Cyber-Preparedness Around the World with the Support of McAfee." The report gave the US a four-star rating, http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf. See also Ehud Keinan, "Report: Israel More Prepared for

Online Attacks than the US," *Ynet*, January 31, 2012, http//www.ynet.co.il/articles/0,7340,L-4183126,00.html.

3 A discussion paper at the High Committee for Science and Technology entitled "The National Cyber Venture" – a proposal to devise a national plan for building cyber capabilities that includes R&D, economic, academic, industrial, and national defense needs aspects, Tel Aviv, November 2012, p. 18.

4 Shmuel Even and David Siman-Tov, "Warfare in Cyberspace: Concepts, Trends, and Implications for Israel," Memorandum No. 109 (Tel Aviv: Institute for National Security Studies, 2011).

5 Ze'ev Schiff, "Meridor Committee Report: Concern that Middle Eastern Countries Will Acquire Nuclear Weapons in the Wake of Iran," *Haaretz* website, April 24, 2006, http://www.haaretz.co.il/misc/1.1100503.

6 Shay Shabtai, "Israel's National Security Concept – New Basic Terms in the Military-Security Sphere," *Strategic Assessment* 13, no. 2 (2010): 8-10.

7 Amir Buhbut, "Changing the Security Concept," *NRG Maariv*, April 24, 2006, http://www.nrg.co.il/online/1/ART1/076/915.html.

8 The government did not officially approve the proposal due to disagreements between the leaders. Nevertheless, the "defense" element has unofficially become part of the Israeli security concept.

9 Shabtai, "Israel's National Security Concept," pp. 8-10.

10 Rami Efrati and Lior Yafe, "That's How You Build a National Cyber Defense," *Israel Defense*, August 11, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2960.

11 Isaac Ben-Israel, "Technology Lessons," *Maarachot* 332 (1993): 13.

12 Amos Yadlin, "Cyber-Warfare – A New Dimension in Israel's National Security Doctrine," *Mabat Malam*, January 2010, p. 4, http://www.intelligence.org.il/KotarPort.aspx#http://malam.barebone.kotar.co.il/KotarApp/Viewer.aspx?nBookID=94837032&sSelectedTab=tdBookinfo%231.undefined.3.fitwidth.

13 Reuters News Agency, "Stuxnet Virus Used on Iran Was 1 of 5 Cyberbombs," *Ynet*, November 29, 2011, http://www.ynet.co.il/articles/0,7340,L-4168852,00.html.

14 Efrati and Yafe, "That's How You Build a National Cyber Defense."

15 Lior Tabansky, "Protection of Critical Infrastructure against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (2011): 72.

16 For more information about Tehila, see the final section, which discusses the design of forces.

17 Efrati and Yafe, "That's How You Build a National Cyber Defense."

18 "Protection of Computer-Based Systems," from the National Security Council Counter-Terrorism Bureau website, http://www.nsc.gov.il/NSCWeb/Templates/CounterTerrorismActivities.aspx.

19 Tabansky, "Protection of Critical Infrastructure against Cyber Threats," pp. 72-73.

20 In November 2010, the Prime Minister ordered the formation of a special team to formulate a national plan for placing Israel among the five leading countries in the cyber field. Work on this task, called the National Cyber Initiative, was led by the National Council for Research and Development, headed by Prof. Isaac Ben-Israel. The team, which included members from key agencies involved with the cyber realm in Israel, was composed of a number of sub-committees that examined the essential elements for coping with the cyber threat, and analyzed national welfare from an economic, academic, and national security perspective.

21 "The National Cyber Initiative," from the National Research and Development Council 2010-2011 report, July 2012, pp.10-17, http://knesset.gov.il/committees/heb/material/data/mada2012-10-15.pdf.

22 The decision was taken following comprehensive staff work by a national team headed by National Research and Development Council chairman Prof. Isaac Ben-Israel.

23 "Promoting National Capability in Cyberspace," Cabinet resolution No. 3611, August 7, 2011, from the website of the Office of the Prime Minister, http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx.

24 Efrati and Yafe, "That's How You Build a National Cyber Defense."

25 Yehuda Konfortes, "Wanted: An Iron Dome for Cyber that Will Protect the Home Front," *People and Computers*, February 1, 2012, http://www.pc.co.il/?p=79406.

26 Yossi Hatoni, "Dr. Eviatar Matania: Cyberspace Requires a Business and a National Policy Treatment – Not an Easy Task," from the CyberSec Conference that took place in February 2012, *People and Computers*, February 12, 2012, http://www.pc.co.il/?p=80025.

27 Ibid.

28 Speech by Dr. Eviatar Matania, 2nd International Cyber Conference, Tel Aviv University, June 9, 2012.

29 Efrati and Yafe, "That's How You Build a National Cyber Defense."

30 Except for publishing the Cabinet's decision to establish a National Cyber Bureau.

31 "National R&D Policy as a System of Integrated Tools," from a speech by Isaac Ben-Israel at the 2011 annual Herzliya Conference, http://www.herzliyaconference.org/_Uploads/dbsAttachedFiles/OriSlonim2.pdf.

32 "An Appeal for Scholarships in the Field: Cyber Defense and Advanced Computing," Ministry of Science and Technology and the Cyber Bureau, Office of the Prime Minister, http://exactsci-info.tau.ac.il/exact_sciences/site/temp/cybersco.pdf.

33 *State Budget Proposal for the 2011-2012 Financial Year, Main Points of the Budget and the Multi-Year Budget Plan*, Jerusalem (2010).

34 A paper for discussion by the National Council for Research and Development on the subject of the National Cyber Initiative – a proposal to establish a national program for building cyber capabilities that will

combine R&D, economic, academic, and industrial aspects with national security needs, Tel Aviv, November 2012, p. 20.

35 "Promoting National Capability in Cyberspace."

36 From an interview with Prof. Isaac Ben-Israel at Tel Aviv University on the subject of the Cyber Initiative, August 5, 2012.

37 From an interview with Major Tal, a senior Cyber Bureau department head, at the Cyber Bureau in Ramat Aviv, August 23, 2012.

38 Ibid.

39 Protocol No. 1069, Meeting of the Knesset Finance Committee, Monday, May 1, 2012, www.knesset.gov.il/protocols/data/rtf/ksafım/2012-05-01-02.rtf.

40 "Prime Minister Netanyahu approved the National Cyber Bureau budget and work plan," from the Office of the Prime Minister's website, June 6, 2012.

41 The head of the National Cyber Bureau announced the launching of the KIDMA – Promotion of Cyber Security Research – Program on November 13, 2012. The program is a result of cooperation between the Bureau and the Chief Scientist of the Ministry of Industry, Trade, and Labor aimed at promoting R&D and entrepreneurship in cyber security in order to maintain and bolster the competitive potential of Israeli industry in this field in the global market.

42 A memorandum from the Chief Scientist: "The KIDMA – Promotion of Cyber Security Research – Program for improving the capabilities of Israeli industry in the cyber security sphere," November 21, 2012, http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf. See also "NIS 80 Million for Cyber Promotion," *Israel Defense*, December 30, 2012, http://www.israeldefense.co.il/?CategoryID=760&ArticleID=3796.

43 Shmuel Even and Amos Granit, *The Israeli Intelligence Community – Whither? Analysis, Trends, and Recommendations*, Memorandum No. 97 (Tel Aviv: Israel Institute for National Security Studies, 2009), p. 64.

44 Isaac Ben-Israel, "Technology Lessons," *IDF Publishing House*, 332 (1993): 10.

45 As discussed in detail in the section dealing with the formulation of strategy.

46 From an August 23, 2012 interview with Major Tal.

47 From a speech by Prime Minister Benjamin Netanyahu at the 1st International Cyber Conference at Tel Aviv University, June 9, 2011.

48 Amir Rapaport, "A Cyber Attack on National Infrastructure," *Israel Defense*, December 8, 2011, http://www.israeldefense.co.il/?CategoryID=536&ArticleID=1421.

49 Amir Rapaport, "Responding Quickly in Order to be Relevant," *Israel Defense*, April 3, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2153.

50 Amir Oren, "The IDF's New Battlefield is Found in Computer Networks," *Haaretz*, January 1, 2010, http://www.haaretz.co.il/misc/1.1182490.

51 "Computer Professions – A Cyber Defense Course," Communications and Teleprocessing Corps website, http://www.tikshuv.idf.il/site/General.aspx?catId=60698&docId=76101.
52 Hadas Duvdevani, "The first IDF cyber course has been completed. The goal is three classes a year," IDF website, May 3, 2012, http://www.mako.co.il/pzm-soldiers/Article-595ec4bc4611731006.htm&sCh=3d385dd2dd5d4110&pid=1093150966.
53 "Disclosure: A New Cyber Administration," *Israel Defense*, January 12, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1657. No other reports about the administration in the Ministry of Defense have been published; a reasonable assumption is that the information is classified.
54 Amir Rapaport, "Disclosure: Cyber Defense Exercise," *Israel Defense*, January 19, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1706.
55 From a September 5, 2012 interview with ILITA head Adv. Yoram HaCohen in the government compound in Tel Aviv.
56 The Law, Information, and Technology Authority (ILITA) website, http://www.justice.gov.il/MOJHeb/ILITA/.
57 A press release by the Law, Information, and Technology Authority, Ministry of Justice Spokesman's Bureau, http://www.justice.gov.il/NR/rdonlyres/4C39E414-E501-48C2-9C53-8EB533FD8B7D/32913/dover5.pdf.
58 "All About Available Government," Available Government website, http://e.gov.il/AboutUs/Pages/AboutUs.aspx.
59 Yossi Hatoni and Gabi Siboni, "There is an entire layer of organizations that is unprotected against cyber attacks," from the CyberSec Conference at the Institute for National Security Studies on February 12, 2012, *People and Computers*, February 15, 2012, http://www.pc.co.il/?p=80466.
60 Foreign reports attribute Stuxnet, Flame, and other cyber events to Israel.
61 Amir Rapaport, "A Cyber Attack on National Infrastructure."

Cyber Weapons and International Stability:
New Destabilization Threats Require New Security Doctrines

Guy-Philippe Goldstein

Though cyberspace is a domain of strategic importance, cyber weapons have not yet been associated with publicly well-enunciated doctrines of use comparable to that of the nuclear age. Taking two very different approaches from the strategic literature—Jervis' security dilemma and Zagare & Kilgoure's perfect deterrence model—cyber weapons are demonstrated in both cases to induce a higher level of international instability. In particular, instability is favored by the attribution issue and the lack of clear thresholds. The outline of a cyber defense doctrine, focusing on the two mentioned informational issues, is then suggested.

Keywords: cyber weapons, deterrence, doctrine, security dilemma, perfect deterrence, attribution, thresholds, escalation

In 2013 cyberspace is a domain of strategic importance.[1] The threat of cyber attacks has been placed at the top of the list of national security risks in the "Intelligence Community Worldwide Threat Assessment of 2013,"[2] and computer network warfare is one of the only military areas in both the US and in NATO countries that is expected to grow.[3] Beginning in 2009, the United States Cyber Command, for example, was established as a unified command under the United States Strategic Command. As was stated quasi-officially by the *Wall Street Journal* in June 2011, computer sabotage that is generated in another country is sometimes considered by the Pentagon as an act of war. In that sense, since the effects of cyber weaponry could

Guy-Philippe Goldstein MBA, HEC (France), is the author of *Babel Minute Zero*, a bestseller about international cyber warfare.

This article was first published in *Military and Strategic Affairs* 5, no. 2 (2013): 121-139.

be substantially vast, key decisions require direct approval from the US President, as they "should be unleashed only on the direct orders of the commander in chief."[4]

There is, however, no doctrine of use that is as clearly communicated as the doctrine of nuclear deterrence. First, many rules remain secretive and strictly in the realm of the highest echelon of the executive powers. Second, the domain itself is not clearly defined: it may be a in the war fighting domain,[5] or not.[6] Is cyberspace critical only because it is conducive to military assurance?[7] Or is it critical in its own right due to the increasing value of the data stored and protected in cyberspace? Finally, the development of a doctrine takes time and historical precedents. Though concepts of nuclear deterrence began emerging in 1946 following the works of Brodie,[8] Mutually Assured Destruction (MAD) did not come to the forefront before the late 1950s.[9] In the USSR, the nuclear strategy's "learning curve" was even less advanced.[10] Certainly, the field of cyber studies is still relatively young, and cyber weaponry in itself is constantly evolving in scale and scope.

The lack of a doctrine poses a significant problem because without the proper management framework—or doctrine of use in international relations—the introduction of any untested and disruptive technologies has the potential to yield unexpected consequences. This is particularly true in the business of war. To rely solely on technological solutions without the context of a doctrine does not guarantee the preservation of the status quo. Stability during the Cold War was not assured by defensive techniques, such as efficient anti-ballistic missiles systems. Not only were these technological solutions elusive, but they were also not desirable in the preservation of the balance of terror at the heart of the MAD doctrine. Both conclusions led to the signing of the Anti Ballistic Missile (ABM) Treaty of 1972.[11]

That does not preclude the necessity of developing specific technologies, such as Submarine-Launched Ballistic Missiles (SLBM) that guarantee a capable and survivable second strike force, but they should espouse the logic of a doctrine in order to reinforce it. This is particularly true for cyberspace, whose nature and risks should indicate the necessity of such an effort. Although the topic is still relatively new, it is not an emerging issue anymore. More than 15 years have passed since the 1997 US Eligible Receiver exercise, which triggered the first real concerns at the federal level with regard to cyber warfare.[12] In addition, the past five years were marked by several "cyber" episodes in international relations, from the

Russian-Estonian cyber guerilla wars of 2007[13] to the 2012 foreign attacks against Saudi Arabia's Aramco, possibly originating from Iran.[14] Sufficient examples of recent years can supply the first guidelines on these issues and doctrines. Moreover, the field can be approached by some of the more classical legal and political frameworks. Though attention must be paid to the specificities of the domain, there are many examples that could be a baseline for the establishment of such doctrine. A recent study that could be used for the writing of such doctrine is the *Tallinn Manual on International Law Applicable to Cyber Warfare*, which managed to apply legal precedents to cyber warfare situations.[15] Following this example, the article will apply frameworks from the "classical" strategic literature in a more formal way to assess the risks cyber weapons pose to international stability and also identify the very core issues of cyber defense that must be addressed by future doctrines.

The Nature and Current Risks of Cyberspace

The Nature of Cyberspace

The definition of cyberspace has been debated extensively. The focus was usually given to the technological components (e.g., electromagnetic spectrum, information-communication technologies, and so on).[16] In this article I suggest a complementary view that asserts cyberspace is currently the name for all information systems that are based on digital data. An analog electro-magnetic radio, for example, is not considered a part of cyberspace as it does not know how to "speak digitally." A DNA computer, however, is conversant in digital data and is therefore a part of cyberspace, as is an electro-magnetic tape, which is encoded in digital data even though it is played in an analog tape recorder.

Digital information is the language humans have created to communicate with machines, which dates back to the Industrial Revolution and the invention of the Jacquard loom (1801), when the rising complexity of new machines required the creation of such a language. It took nearly two centuries for the language to spread among other machines, especially after the inventions of Turing machine computers and the internet protocol. By nature, this language consists of three components: hardware (including telecommunication equipment), software (including data exchange protocols), and "brainware," the human component that takes part of the data transmission by constituting very vulnerable interception points[17]

and by writing code. Some of the most dangerous weapons in cyberspace today are, in fact, the codes produced by talented hackers. Functionally, cyberspace can be split into two: the physical support that materially affects communication and calculation, and the semantic domain that transforms physical support actions into data or instructions, providing them with meaning and controlling its own physical support.

This simplified description of cyberspace explains the current urgency to define the conditions for cyber defense and sheds light on the most critical pain points in cyberspace.

First, the distinction between digital and analog data makes clear why cyber warfare has become a strategic topic only in recent years. Although computers have been in use since the end of World War II, in 1986, digital data comprised only 0.6 percent of global data for storage, communications, and broadcasting, increasing to 24 percent in 2000. It exploded in 2007, however, reaching 93 percent, while "old" analog information capabilities became noncritical.[18] By the second half of the 2000s, information systems—what is usually most critical to any institution or organism—was fully transferred into the digital format. This may explain why the number of cyber attack episodes increased in frequency and gravity over the last few years. Civilization, including warfare, has turned digital. To use the words of Marc Andreessen, "Software has eaten the world."[19]

Second, the semantic dimension highlights and reflects the heart of networked information systems. The objective of ARPAnet, the ancestor of the internet, was to "emphasize robustness and survivability, including the capability to withstand losses of large portions of the underlying networks."[20] Packet switching networks are designed to withstand material hardware degradation. In cyberspace, the most severe damages are obtained when data are corrupted and their meaning manipulated, as was evident in "Operation Orchard"[21] and Stuxnet. In both cases, a maximum effect was obtained because human controllers were manipulated by corrupted command and control systems. In addition, the corruption of the industrial controllers that set the speed of rotors in P-1 centrifuges increased the level of sabotage.[22]

Characteristics of Cyber Attacks in Brief

In ancient Greece, the term *logos* equally signified the uttered word, the sentence, the direct meaning, and the higher level of ideas expressed.[23] It

was a confused but rich definition, which also led to the development of the first hackers, the sophists, who manipulated words and syntax in order to corrupt meaning. What we call cyberspace today is, essentially, a digitalized *logos*, i.e., the language designed to communicate with machines on anything from physical support through immediate semantic translation of ordering machines or humans, and to Gibson's "consensual hallucination."[24] In this digital form of *logos*, modern sophists act like *The Sorcerer's Apprentice* of Paul Dukas: the code alters the man-made environment of machines, which causes the machines to alter the physical world by believing wrong arguments or instructions. In that sense, the quality of the attack depends first and foremost on the talent of the wizards.

The flaws used by offensive cyber weapons were developed either mistakenly or purposefully during the production stage of the equipment[25] or code or during their human handling, and were then exploited for further actions. To more precisely assess the attack's impact in the physical world, cyber warriors created models to test attacks.[26] Cyber weapons can also be designed to hide their signature and origin.[27] These characteristics give an asymmetrical advantage to the attacker once a flaw (or "exploit") has been found: only the attacker knows what the exploit is and the identity of the attacker. Since cyberspace is continuously updated by software upgrades, however, the cyber physical environment changes constantly as well, which makes the potency of exploits limited and transient: searching or manufacturing exploits requires permanent efforts.

The effects of these attacks occur as soon as the machines receive the message—the code strikes at "zero day," and their range is extremely large due to the wide use of digital-speaking machines: from espionage (penetration of machines that store information) and economic sabotage (penetration or corruption of machines storing financial values or IP addresses) to physical sabotage (attacks against machines that control and command all sorts of civilian industrial processes or weapon systems ranging from the tactical to the strategic). Because "software has eaten the world" and continues to do so, there are no potential limits to what can be attacked, and these effects have a psychological component as well. While equipment that was damaged by a kinetic attack must be replaced, equipment that was harmed by a cyber attack might appear to operate properly but doubts regarding its capabilities will remain permanently.

Geopolitical Instability Induced by Cyber Weaponry

Pro-Offense and Speed

The pro-offense, rapid, and possibly large extent of the effects mentioned above and their potential characteristics creates a military technological environment that is tilting toward the rupture of the status quo. Rober Jervis' seminal analysis on the offense-defense theory stresses that the terms of the security dilemma rely on two crucial variables: "whether defensive weapons and policies can be distinguished from offensive ones, and whether the defense or the offense has the advantage."[28] Combining these two variables to create four possible worlds, Jervis states that world powers will have the greatest difficulties in maintaining the status quo in a reality where "offensive posture is not distinguishable from [the defensive] one" and where "the offense has the advantage." Here, beliefs are as powerful as technology. For example, World War I was the product of such a world, which was termed "doubly dangerous": the technologies of machine guns and railroads gave the defense an advantage,[29] but because of Bismarck's quick victories in the preceding decades, great powers believed that military technologies were still yielding an advantage to offense.[30]

The parallelism with a military environment shaped and dominated by cyber weaponry should be obvious. First, there is a widespread belief that cyber weapons give an advantage to the offense,[31] which may lie in the perceived asymmetry of information between offense and defense. By definition, the defense ignores the existence of the flaw before it materializes, but when it does, correcting it may be too late. This argument may need to be refined and further examined, as the advantage given to the offense could be limited and transient in reality, but it is immaterial to the application of Jervis' model. As with Europe following Bismarck's victories, what matters is the belief expressed by the general consensus. Second, cyber weapons cannot be monitored, as one can hardly distinguish between offensive and defensive capabilities. Dual doctrines of use, including those of defensive and offensive uses, have been drafted in China and in major Western countries.[32] Core capabilities include assets that when examined from afar can be construed for defensive or offensive use, like IT infrastructure or code writers. Currently in cyber weaponry, there are no equivalents to Salt II's "observable differences" used to single out bombers carrying long-range Air-launched Cruise Missiles (ALCMs).[33] Defensive capability development

itself is hardly distinguishable from offensive capability development since it stems in large parts from Red-Team exercises.[34]

The "doubly dangerous" risks could also be exacerbated by a rapid offense, used in a first strike. Such a "bolt from the blue" attack would be so decisive it would preempt any reactions from the defender. In an initial analysis of mutual deterrence games, Zagare showed that the fewer moves there are in a game, the more harm would be made to the status quo.[35] The incentive to strike first is shared by peer powers that are at about the same level of technological development. In that case, the perception that the attack is of equal risk to both sides would lead to Schelling's "reciprocal fear of surprise attack."[36] As Schelling writes, "Military technology that puts a premium on haste in a crisis puts a premium on war itself... If the weapons can act instantaneously by the flip of a switch, a 'go' signal, and can arrive virtually without warning to do decisive damage, the outcome of the crisis depends simply on who first finds the suspense unbearable."[37]

These lines were written a few years before ARPAnet was even established. They are echoed in the writing of US Air Force officers on war in the Information Age, stating that "preemptive employment of force may become a prerequisite for success."[38]

The dynamics leading to a conflict are also exacerbated by the ongoing technological investment in R&D cyber weaponry. The impetus for further investment is fed by the branching out of cyberspace into additional domains of civilian and military life and the need to protect these new realms of cyberspace. Since defense and offense R&D capabilities are hard to distinguish, this naturally triggers an arms race. Cyberspace's internal rate of the conversion of offline processes conversion into online ones is not always controlled by the military. Different from other revolutions in military affairs that were driven by actual contests, the thrust for digitalization of the US military continued at a high pace after the collapse of the USSR.[39] This may have been the result of the manifestation of the autonomous dynamics of digital data and software as they continue to "eat" the military. In this case, it is the qualitative evolution of technology itself that can also disrupt the status quo stability. As noted by Kissinger, countries that are opposing one another live in fear that their "survival may be jeopardized by a technological breakthrough on the part of [their] opponent[s]."[40] As stated by Joynt & Corbett, the rate of change creates an "intrinsic uncertainty about advancing technologies...{as they] cannot supply the sufficient conditions

for stable deterrence."[41] Indeed, as a regional example, Horowitz notes that the cyber arms race in East Asia fuels instability.[42] Finally, beyond the growing scope of cyberspace's reach, the dynamic internal competition and constant upheaval of the IT industry generates an ongoing upgrade of cyberspace itself. These enhancements also constitute the sources of new alterations in the fabric of cyberspace and, thus, can generate new flaws. Independent from the political or military competition, this factor mechanically exacerbates the arms race.

Attribution and Thresholds

In addition to the perception that the cyberspace environment is pro-offense and prone to haste and to the field's technological domain that is constantly changing, cyberspace is also characterized by the ability to wage attacks without a clear attribution or a clear identification of the thresholds at stake following the initial impact. These factors constitute additional triggers for instability.

The lack of signature (the attribution issue) gives an advantage to the offense. If attacked, the defender does not know against whom to retaliate. This impedes the defense because the defender is not able to strike a counter-blow that could stop or deter the attacker. Without a clear aggressor, the defender will also encounter difficulties in mobilizing diplomatic relations in order to organize counter-pressure. If the defender retaliates or elevates defense against the wrong party, it may actually isolate itself more or trigger international escalation.

Attribution is therefore not a trivial issue: in war games one of the very first questions asked by the player acting as the defending head of state concerns the attacker's identity.[43] To gain weight diplomatically, attribution needs to reach a high level of certainty. This is technically hard to obtain in a limited amount of time.[44] Potential aggressors can claim "plausible deniability" and neutralize the international audience, reducing the margins of maneuver for the defender. Attribution can be inferred from the international context,[45] but this would not equate producing an incontrovertible "smoking gun," which would be required for securing diplomatic and external military support, especially in the context of the intelligence failures leading to the invasion of Iraq in 2003. Similarly, the international context could be muddied. Since the 1986 "BrainVirus" infection of digitally encoded floppy disks across the world prior to the web's existence,[46] most malware infections

have been global in nature. All machines that speak the digital language are vulnerable to digital infections. Though Stuxnet is said to have targeted specific nuclear enrichment installations in Iran, it was also found in India, China, Russia, and the US.[47] That makes "plausible deniability" even easier for the attacker, which can portray itself as a victim among others.

Non-recognition of thresholds also clearly undermines stability. Schelling posits the importance of thresholds to articulate the "idiom of war."[48] For thresholds to efficiently structure the dialogue in the violent atmosphere of war, they need to possess "simplicity, reconcilability and conspicuousness,"[49] for example, the crossing of a river or a mountain, or the general mobilization of an army.

The question is all the more critical because each player's calculus depends on other players' "curve of credibility"[50]—i.e., the stakes that a country has invested in a conflict from its own volition or which was forced on it by its opponent. These stakes are delimited by the above mentioned thresholds. They are positioned within a hierarchical disposition that credibly organizes the perceived modus operandi of a government. The underlying sense of proportionality is related to the above-mentioned hierarchical disposition and is also the key to credibility. This, in turn, allows the violent dialogue to be controlled. If an error was created in understanding the opponent's curve of credibility, there is de facto a perceived "imbalance of resolve"[51]—potentially leading to the conflict's spiraling. The massive retaliation policy defined in the NSC-162/2 document, for example, was noted by William Kaufman as lacking credibility, as it was "out of character for the US" to implement it.[52] On the other hand, as identified by Frank Zagare and Marc Kilgour in their work on Perfect Deterrence Theory, the credibility of nuclear deterrence lies on the preference for retaliation over backing down.[53] This preference is assured by a capable threat (especially a survivable second strike force), but also on a rational calculus of retaliation, as this rational preference establishes credibility. If a nation's core population centers were hit, and the nation can retaliate and inflict a major cost to the aggressor, there is a high probability it will do so. Higher stakes change the pay-back calculus. In this situation, if population centers were indeed destroyed, the state can more easily mobilize internal resources by way of national cohesion and consensus around revenge response. The option of a more forceful reaction becomes credible. Early in the nuclear age, Liddell Hart noted that "victims of aggression are driven by an uncontrollable impulse to

hit back regardless of the consequences" and therefore an "aggressor may hesitate to employ atomic bombs" because of the likelihood of retaliation.[54]

Herein lies another difficulty with cyber attacks: they do not easily offer simple, recognizable, and conspicuous characterization in terms of thresholds. Would difficulties in online banking lead to financial panic or an economic disaster, and at what point would this occur? If the capital state of an attacked country had suffered a blackout, how many people would die after one day? When the Northeastern region of the US was struck by the blackout of 2003 that lasted more than 52 hours, the effects were surely not negligible but were also relatively minimal.[55] The evolution of the impact does not develop in a linear model. Difficulties are compounded by lack of precedents in the use of constantly evolving weaponry. A foreign force invading another nation's airspace is considered a breach of sovereignty, but what about cyber attacks of foreign countries that repeatedly corrupt servers used by national companies? Finally, effects may be caused by indirect and psychological actions; for example, by instilling doubts on the safe use of military or industrial capabilities, cyber weapon may induce paralysis but not directly provoke it. Is it the same when the paralysis is the consequence of a direct kinetic hit?

The consequences of lack of attribution and clear thresholds on stability can be analyzed through Perfect Deterrence Theory,[56] which posits that for a threat to be deterrent, it must be capable of creating significant pain to the threatened party so that it would prefer not to suffer from it. The threat must also be credible, as the threatening party must be perceived as preferring to use the threat rather than backing down. Without signature, however, the deterrent threat is not viable anymore, as the defending party does not know against whom to retaliate, and the secret offender is not threatened. The defender may also not be credible if it threatens to hurt everything and everyone in response to attacks of unknown origins. Similarly, even if attribution is realized but the effects are hard to measure and the distinctive thresholds at risks cannot be identified, the retaliation will not be "in kind," rather either too hard or too weak.

At a macro level, it is coherent with strategic literature that asymmetry or gaps in the information available to each party would lead to conflict. Spiraling is being modeled as triggered by errors of appreciation, or as Zagare and Marc Kilgour put it, "strategic uncertainty and unanticipated response, and both may be broadly construed as mistakes traceable to an

intelligence failure, bureaucratic bungling, miscalculation, or some other cognitive or information-gathering deficiency."[57] The risks of spiraling are higher if countries retaliate against attacks that aim to create false information in the opponent's system. War can also be seen as a process that resolves an information problem: how much harm can a nation do to its opponent?[58] Resolving this question establishes a hierarchy among nations, which serves as an ordered bargaining system that is understood by all. These explanations show why war is much more probable when the two countries facing each other are of the same strength rather than when they are not, in which case the outcome would be obvious.[59] Cyber warfare's modus operandi, however, is to create confusion in data. This mode of action threatens to corrupt strategic information, create uncertainty, and pose risks that would upset the status quo.

The absence of large scale demonstration of cyber attacks has been one of the factors limiting the risk of spiraling. The capability to damage this type of weaponry is not as clearly assured as that of a kinetic or a nuclear weapon. However, both the potency of the Stuxnet worm and the understanding that "software is eating the world" have left major global powers more prone to the risks of this new class of weapons. Perceptions are transforming following changes on the ground and public declarations. The psychological frames at play, according to Jervis and Perfect Deterrence Theory, become applicable to a geopolitical environment that is under stronger influence of cyber weaponry.

Conclusion: The Need for "Escalation Control" Doctrines in Cyber Defense

There are no reasons to believe that "the diplomacy of violence"[60]—a term coined by Schelling to evoke the phenomenon of warfare—is going to vanish with the immersion of our civilization into cyberspace. Similarly, during the internet bubble of the 1990s, Michael Porter demonstrated that although the internet's "new economy" may emphasize types of cost advantages over others in the search for competitive differentiation,[61] it would still not suspend the old rules of strategy. Instead, the winners would be the ones who are able to "view the Internet as a complement to, not a cannibal of, traditional ways of competing."[62] Furthermore, the "power to hurt" is fully embodied in cyberspace, but does not supersede the laws of strategy.

Cyber power can be analyzed through the classical dimensions of strategy, as elucidated by John Sheldon, Michael Howard and Colin S. Gray.[63]

New technologies do not eliminate the risks of spiraling in warfare. Instead, this depends on the effects of any technology that triggers general warfare—effects such as the perception that strategic military capabilities lean towards the offense; the possibility that defensive military capabilities could also be used by the offense; the rapid mode of action that would shorten the length of the military "game"; or the perception that quick technological change has the potential to reshuffle the balance of military forces. The strength of these factors ends up affecting the threat capability and credibility of each player, and thus alters the underlying deterrence relationship between the players. Ultimately, the deterrence balance can be summed up as an informational problem: does the party accurately recognize its enemy's capabilities and those of itself? Does the party have a good sense of its intentions and red lines, and are they clear to its enemy?

On all these accounts, and especially because of the corruption of data and strategic information, cyber weapons increase the risk of informational errors whereby a crisis escalates into overall warfare. In particular, the above discussion on lack of attribution and clear thresholds explains why this risk is so well materialized with the use of cyber weapons. Furthermore, the solution for both issues is rendered even more pressing due to the nature of a game, which becomes shorter by an innately speed-of-light technology that is perceived as pro-offense. All this shows how pressing the need is for a doctrine to manage this informational crisis. Thus, a doctrine for cyber stability will not be based solely on the capabilities for reprisal, such as a demonstrable, survivable second strike force at the heart of nuclear deterrence, but just as importantly, it would also be based on the capabilities for elucidation at the strategic level. If the truth about attribution and damage assessment cannot be established, then the defending party is at risk of either conceding defeat to an unknown attacker, or of engaging in reprisals "in the dark" with a high risk of spiraling. On the other hand, if the truth is fully established in the "brainware" of the strategic decision makers—if not in the whole of the software and hardware systems of the defending nation—then at least the defender can unlock all of its other traditional options from diplomatic to strategic threats in order to credibly force the offender to back down. The parallels with the truth-seeking objectives of intelligence services should not be surprising: if in cyber, as

in intelligence, "the truth shall make you free,"[64] then it is partially due to the fact that both fields operate in information domains, with one based in the digital format and the other on "secrecy."[65]

The outline of such cyber defense doctrines could resemble that of elucidation actions like counter-intelligence or police investigations, but it must be strategically led by the head of state. These investigations would be supported by strong technical capabilities and operated by state-of-the-art methodologies aimed at truth-seeking from deductive testing for attribution to systems simulation for red-lines assessment. They would also have a strong diplomatic component, leveraging some circles of very close cooperation. The establishment of the truth cannot be dictated by one center. It consists of a social process based on either the sharing of the data supporting the conclusions, carefully taking into account the constraints posed by the intelligence context, or the ability to replicate experiments.[66] In that respect, military defense doctrines in cyberspace are somewhat parallel to the disciplined, scientific approach to problem solving that has been taken recently by the management of corporations from marketing[67] to human resources.[68] To attain the highest ground in an informational domain is to reach for the truth.

Notes

1 This article explores the strategic risks of cyber weapons and the need to develop specific doctrines for cyber defense in order to offset the risk of out-of-control crisis escalation. To detail such doctrines would go beyond the scope of the current article. The author will explore some of the doctrinal solutions to the stability problems exposed here in an upcoming article.

2 Luis Martinez, "Intel Heads Now Fear Cyber Attack More than Terror," *ABCNews*, March 13, 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber attack-terror/story?id=18719593.

3 Despite austerity cuts, the UK's cyber security budget has been expected to grow by some £650m ($1.07bn) over the 2012-2015 period. In James Blitz, "Country Profile: UK Defences are Boosted to Fight e-Crime," *Financial Times*, June 2, 2011.

4 David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *New York Times*, February 3, 2012.

5 Keith B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly* 46, no. 3 (2007): 58-61.

6 Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 325-40.

7 Libicki, "Cyberspace is Not a Warfighting Domain."

8 Bernard Brodie, "The Development of Nuclear Strategy," *International Security* 2, no. 4 (1978): 65-83.
9 Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: Palgrave Macmillan, 2003), pp. 234-36.
10 Freedman, *The Evolution of Nuclear Strategy*, pp. 243-44.
11 See for example Freedman, *The Evolution of Nuclear Strategy*, p. 338.
12 See PBS interview with former Deputy Secretary of Defense John Hamre in Michael Kirk, "Cyberwar!" *PBS*, April 24, 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html.
13 See BBC World Service, "Estonia Hit by 'Moscow Cyber War," *BBC News*, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.
14 See Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012.
15 Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).
16 See Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), pp. 26-28.
17 Human errors in security configurations have been also identified as "responsible for 80% of Air Force vulnerabilities," in James A. Lewis, ed., *Securing Cyberspace for the 44th Presidency* (Center for Strategic and International Studies, 2008), p. 55. The rise of social engineering and phishing attacks has accentuated the importance of the "human factor" in cyber security. - It's not a quote—it's an expression. Kevin Mandia notes, "While previous generations of attacks targeted technology such as networks and servers and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses." Kevin Mandia, "Cyber Threats and Ongoing Efforts to Protect the Nation," *Permanent Select Committee on Intelligence, US House of Representatives*, October 4, 2011.
18 Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate and Compute Information," *Science* 332, no. 6025 (2011): 60-65.
19 Marc Andreessen, "Why Software is Eating the World," *Wall Street Journal*, August 20, 2011.
20 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, *A Brief History of the Internet* (The Internet Society, 2012), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.
21 See David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis," *Aviation Week & Space Technology*, October 3, 2007, and David A. Fulghum,

"Israel Used Electronic Attack in Air Strike against Syrian Mystery Target," *Aviation Week & Space Technology*, October 8, 2007.

22 See Nicolas Falliere, Liam O Murchu ,and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010).

23 Barbara Cassin, CNRS, "Logos et Polis: La Force du Discours," in Catherine Golliau ed., *La Sagesse Grecque* (Paris: Le Point Référence, 2011), pp. 41-43.

24 William Gibson, *Neuromancer* (New York: Ace Science Fiction, 1984).

25 See the issue of kill switch in chips in Sally Adlee, "The Hunt for the Kill Switch," *IEEE Spectrum*, May 1, 2008.

26 For example, according to David Sanger, when Israel and the US developed a "bug" to derail nuclear enrichment operations at the Natanz plant in Iran, research teams "began building replicas of Iran's P-1 centrifuges" since "the bug needed to be tested." See David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012. In particular, the Dimona complex in Israel may serve as a testing ground for cyber attacks of centrifuges—see William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

27 The issue of cyber attacks attribution is a major difficulty explored in fiction—see for example, Guy-Philippe Goldstein, *Babel Minute Zero* (Paris: Denoel, 2007—and illustrated in real life episodes such as the cyber attacks against Estonia in 2007. See Mikko Hypponen,"9thof May," *F-Secure Weblog*, February 15, 2010, http://www.f-secure.com/weblog/archives/archive-052007.html.

28 Robert Jervis, "The Security Dilemma," *World Politics* 30, no. 2 (1978), p. 187.

29 See a detailed discussion in Charles L. Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (1998): 44-82.

30 Robert Jervis, "The Security Dilemma," p. 190.

31 In 2009, Gregory J. Rattray highlights the "offense dominance" in Cyberspace - see Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), pp. 253-74. Three years later, David T. Fahrenkrug from the Office of Net Assessment / Office of the Secretary of Defense, notes that "Current accepted wisdom in cyberspace is that the attacker has the decisive advantage" - in David T. Fahrenkrug, *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*, 4th International Conference on Cyber Conflict (Tallinn: NATO CCD COE Publications, 2012).

32 New military development programs announced in 2012 for both DARPA and the US Air Force indicate- a clear interest in offensive weaponry. See Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive," *World Affairs*, January/February 2013; additionally, in March 2013, "General Keith Alexander, who heads the US National Security Agency and Cyber

Command, told lawmakers Tuesday that the military is creating at least 13 units which would have offensive capabilities in cyberspace." in "Obama Calls China Cyber Attacks 'State Sponsored,'" *News Wires*, March 13, 2013. In France, the project for the 2013 "Livre Blanc" mentions the need for LIO, aka "Lutte Informatique Offensive" or Offensive Cyber Warfare—in Vincent Lamigeon, "Livre Blanc de la Defense: Les 5 Nouvelles Priorités Imposes à l'armée Francaise," *Challenges*, April 29, 2013.

33 See Thomas K. Longstreth and Richard A. Scribner, "Verifications of Limits on Air Launched Cruise Missiles," in Frank von Hippel and Roald Z. Sagdeev, eds., *Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals* (New York: Gordon and Breach, 1990), p. 185

34 For a very short US overview, see Zachary Fryer-Biggs, "Building Better Cyber Red Teams," *Defense News*, June 14, 2012.

35 Frank C. Zagare, *The Dynamics of Deterrence* (Chicago: University of Chicago Press, 1987), pp. 48-56—see discussion on rules relaxation and lengthening the game.

36 See Chap. IX, "The Reciprocal Fear of Surprise Attack," in Thomas C. Schelling, *The Strategy of Conflict* (Harvard University Press, 1960).

37 Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 225.

38 See David S. Fadok, Major, USAF, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell Air Force Base: School of Advanced Air Power Studies, 1995), p. 49. One year earlier, John Warden stated already that "Capturing and exploiting the datasphere may well be the most important effort in many future wars." The conquest of "datasphere" is implicitly defined as a priority for military success. See Col. John A. Warden III, USAF, "Air Theory for the Twenty-first Century," in *Challenge and Response: Anticipating U.S. Military Security Concerns*, ed. Karl P. Magyar (Maxwell AFB, Ala.: Air University Press, 1994)

39 See Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York: Cambridge University Press, 2010), p. 129.

40 Henry Kissinger, "Arms Control, Inspection and Surprise Attack," *Foreign Affairs* 38, no.4 (1960): 557-75.

41 Carey B. Joynt and Percy E. Corbett, *Theory and Reality in World Politics* (London: Macmillan Press, 1978), pp. 92-93.

42 Michael Horowitz, "Information Age Weaponry and the Future Shape of Security in East Asia," *Global Asia* 6, no. 2 (2011).

43 On the issue of US Defense officials publicly struggling with the issue of attribution, see John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, January 26, 2010; David E. Sanger and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," *New York Times*, May 31, 2011.

44 In a recent example, after facing a simultaneous shutdown of computer networks at several major broadcasters and banks on March 20, 2013, South Korea first said that cyber attacks came from China, in Warwick Ashford, "South Korea Says Cyber Attack Came from IP Address in China," *Computer Weekly*, March 21,2013. South Korea publicly admitted a mistake the next day. See Warwick Ashford, "South Korea Admits Mistake in Linking Cyber Attacks to China," *Computer Weekly*, March 22, 2013. Three weeks later, South Korea accused North Korea. See Warwick Ashford, "South Korea Accuses North Korea of Launching Cyber Attacks," *Computer Weekly*, April 11, 2013.

45 For a thesis minimizing the "attribution problem" by analysis of the international context, see Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington D.C.: National Defense University Press, 2009), pp. 309-42.

46 Rupert Goodwins, "Ten Computer Viruses that Changed the World," *ZDNet*, August 3, 2011.

47 Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010), p. 6 and "Chinese infections in Stuxnet 'Cyber Superweapon' Moves to China," *AFP*, September 30, 2010.

48 Schelling, *Arms and Influence*, p. 135: "Finite steps in the enlargement of a war or a change in participation. They are conventional stopping places or dividing lines. They have a legalistic quality, and they depend on precedents or analogy. They have some quality that makes them recognizable, and they are somewhat arbitrary....We don't make them or invent them, but only recognize them....Apparently, any kind of restrained conflict needs a distinctive restraint that can be recognized by both sides, conspicuous stopping places, conventions and precedents to indicate what is within bounds and what is out of bounds, ways of distinguishing new initiatives from just more of the same activity."

49 Schelling, *Arms and Influence*, p. 137.

50 See Carey B. Joynt and Percey E. Corbett, *Theory and Reality in World Politics* (Pittsburgh: University of Pittsburgh Press, 1978), pp. 94-95.

51 See Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge Studies in International Relations, 2000), p. 301.

52 See Freedman, *The Evolution of Nuclear Strategy*, pp. 96, citing William Kaufman, *Military Policy and National Security* (Princeton University Press, 1956), p.21, 24-25.

53 Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence*, chapter 3.

54 See Freedman, *The Evolution of Nuclear Strategy*, p. 40 citing B. M. Liddell Hart, *The Revolution in Warfare* (London: Faber and Faber, 1946) pp. 85-86.

55 In New York City, during the blackout, there were significant increases in respiratory, cardiac, and other EMS calls. See Gary Kalkut, MD, MPH, "Effects of the August 2003 Blackout on the New York City Healthcare

Delivery System: A Lesson for Disaster Preparedness," *Critical Care Medicine* 33, no. 1 (2005), pp. S96-S101. Reports by the press, as cited on Wikipedia, accounts for 11 indirect fatalities (http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003); however, a further study indicates that "there was minimal morbidity and mortality reported that could be attributed to the event." See J. Kile, S. Skowronski, M.D. Miller, S.G. Reissman, V. Balaban, R.W. Klomp, D.B. Reissman, H.M. Mainzer, A.L. Dannenberg, "Impact of 2003 Power Outages on Public Health and Emergency Response," *Pre-hospital and Disaster Medicine* 20, no. 2 (2005): 93-97. The estimates of total costs in the United States range between $4 billion and $10 billion US dollars, or less than 0.1% of US GDP. sSee U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (2004), p.1.

56 See Zagare, and Kilgour, *Perfect Deterrence*.

57 Zagare and Kilgour, *Perfect Deterrence*, p. 302.

58 Put differently, if states knew the outcome of a possible war and had perfect information on each other's capabilities and resolve, they would probably avoid war. See James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379-414 and Dan Reiter, "Exploring the Bargaining Model of War," *Perspective on Politics* 1, no.1 (2003): 27-43.

59 See empirical analysis in Stephen L. Quackenbush, "General Deterrence and International Conflict: Testing Perfect Deterrence Theory," *International Interactions* 36, no. 1 (2010): 1-26.

60 Schelling, *Arms and Influence*, chapter 1.

61 See Michael Porter, "Strategy and the Internet," *Harvard Business Review*, March 2001.

62 See Porter, "Strategy and the Internet."

63 John B. Sheldon, "The Dimensions of Strategy for Conceptualizing Cyberpower: Laying the Foundations for Sensible Cyber Security Policy and Doctrine," presented to the panel on "Comparative Cyber Security Strategies: Theory and Practice," International Studies Association Conference, San Diego, 2012.

64 Extract from the Gospel according to St. John, initially inscribed on the CIA building's facade. See https://www.cia.gov/news-information/featured-story-archive/ohb-50th-anniversary.html.

65 See for example Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence* 46, no. 3 (2002), pp. 20-21.

66 Sharing of data is a core requirement for any submission to peer reviewed journals. See for example the recommendations for *Nature*: http://www.nature.com/authors/policies/availability.html; Evidently, in intelligence matters, sharing must balance the gain from sharing with the risks of exposure for the source—what Director of National Intelligence (DNI) James R. Clapper has referred to the need to find the "sweet spot" between sharing and protecting information. See Remarks and Q & A by Director of National

Intelligence, Mr. James Clapper, 2010 Geospatial Intelligence Symposium, New Orleans, Louisiana, November 2, 2010, quoted in Richard A. Best Jr., "Intelligence Information: Need-to-Know vs. Need-to-Share," *Congressional Research Services*, June 6, 2011.

67 See the impact of A/B Testing in management of Silicon Valley startup companies up to Google in Brian Christian, "The A/B Test: Inside the Technology That's Changing the Rules of Business," *Wired*, April 25, 2012.

68 See Steve Lohr, "Big Data, Trying to Build Better Workers," *New York Times*, April 20, 2013.

Cyber Defense from "Reduction in Asymmetrical Information" Strategies

Guy-Philippe Goldstein

This essay confronts two main problems in cyber defense: the attribution issue (who is attacking?) and the threshold issue (is it worth all-out war?). Starting with a war-game scenario, an analytical framework based on the *Tallinn Manual* is suggested to delineate cases for wars and areas of crises. The prosecution of cyber crises is then proposed through two "reduction in asymmetrical information" strategies. The threshold issue can be alleviated with a better understanding of observable and simulated effects on the defending networked nation modeled as a system, drawing on the initial concept proposed by Col. John Warden. The attribution issue must be solved through excellence in elucidation methods and internationally supported coercive investigation, inspired by Thomas Schelling's compellence. The growing preeminence of the digital domain in our modern societies could make these strategies among the building blocks of a new doctrine for military and political stability in the twenty-first century.

Keywords: cyber weapon, cyber defense, deterrence, doctrine, compellence, attribution, thresholds, escalation, *Tallinn Manual*

Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Sun Tzu, *The Art of War*[1]

Guy-Philippe Goldstei, MBA, HEC (France) is the author of Babel Minute Zero, a bestseller about international cyber warfare.

This article was first published in *Military and Strategic Affairs* 5, no. 3 (2013): 129-155.

Introduction: A Regional Scenario

It is 9:00 in Country X. In the capital state, bank ATMs have stopped working. Some online customers cannot access their bank accounts at the top three national banks. In some cases, the balance in online accounts has been wiped to zero. Cell phones are barely functioning. The attack seems to be of a new kind. The effects are the same as with the Estonia cyber attacks of 2007. However, technically, it does not look like a distributed denial of service attack: no massive amount of IP-packets clogging servers has been detected. No immediate remedy is at hand. How long will this last? Can data be recovered? Is this a first wave announcing further attacks? On the streets of Country X, anxiety is quickly ramping up.

Country X is not alone. A week earlier, a prominent software security firm from Country B identified a new malware: GlobalWorm. Though its mode of action was unknown at the time of discovery, GlobalWorm seems to have infected many systems across various countries. In an alert bulletin, the software security firm is now linking the current attack against Country X to GlobalWorm. Furthermore, other countries infected by GlobalWorm are experiencing difficulties, including friends as well as foes of Country X. However, only Country X is suffering severely harmful effects.[2]

Who is responsible for the attacks on Country X with GlobalWorm? What type of threats does GlobalWorm pose to Country X? How should Country X retaliate?

The first two questions frame the third one. To further complicate matters, the security software company that knows GlobalWorm best has tight links to the military apparatus of Country B – and Country B is not a close ally of Country X. As the National Security Council of Country X convenes, the questions around the table coalesce: Is this another blow from Country Y, the proverbial enemy of Country X? Did Country Y not just increase investments in cyber weaponry?...Or is this coming from Country Z, a country whose relationship with Country X has dramatically soured over the last five years?

The head of state of Country X asks the three questions that are foremost on his mind:

a. Can you prove to me that this is related neither to Country Y nor to Country Z?
b. How much time do I have left before I am forced into retaliation?

c. How can I retaliate if I do not know the answers to my first and my second questions?

The head of intelligence for Country X confirms that at this stage, there is no clear indication that Country Y or Country Z is behind the attacks – though it is possible, he emphasizes. However, the possibility of manipulation by Country B cannot be dismissed either. Additionally, although the attacks have shocked the population, they have not escalated in kind over the last eight hours. It is not possible to say how the threat will evolve – if indeed it does evolve. What is clear is that Country X has been weakened. Without some form of elucidation, restoration, and retribution, its status as a cyber power will be contested. This does matter. In this day and age, it is understood that there will be major combat operations in cyberspace. So the domination of cyberspace becomes a test of overall military power.

The minister for foreign affairs says Country A, one of the closest allies of Country X on the international scene, does not possess clear indications about the origin of GlobalWorm's infection. However, as Country A considers it a global problem, Country A will not allow Country X to retaliate without evidence being put to the fore. To top that, Country A says that retaliation needs to be closely coordinated in case of cyber reprisals. After all, neither Country X nor Country A understands what tricks lie inside GlobalWorm. The situation is different from scenarios in which Country X is the attacker: Country X controls neither the test nor the environment. A wrong maneuver could be perilous for Country X, perhaps for everyone else too. All sorts of manipulations can be envisioned. There are just too many unknowns.

This state of strategic confusion is perhaps what the offender had in mind when designing the attack. Country X does not know yet what bargain is at work, nor with whom. The only clear offer comes from Country B: via its software security firm, it could bring unique expertise and support of GlobalWorm. But this help would probably come at a price. Additionally, Country A and Country B are global peer competitors. Country A may object to Country B helping Country X. Relationships between Country A and Country X could be damaged.

In this scenario, conventional or strategic deterrence tools are not operative. Country X is actually faced with strategic paralysis.

Perfect deterrence theory posits that "response in kind" is an optimal strategy.[3] It demonstrates that the defender has a credible retaliatory

threat. At the same time, it signals that Country X is not necessarily seeking escalation – what Huth describes as a "firm-but-flexible" negotiation style.[4] Additionally, not to commit to full-fledged escalation but to engage in firm response allows opening up options without exercising them. This is the position most favored by politicians as well as financiers. It is also an optimal situation with regard to the decision laws of cybernetics. But in the current predicament for Country X, response in kind is not possible. First, there is a major obstacle: Country X does not know against whom to respond in kind. It is faced with an attribution issue.[5] But even if it knew with certainty, Country X would still face a second major obstacle: it may not know exactly how to respond in kind.

Let us assume for a moment that Country X has established that Country Y is the aggressor. Since bank ATMs, online banking accounts, and some cell phone networks have been breached, Country X tries to respond in kind. Let us also assume that Country Y has not hardened the cyber security in advance around what it would know to be the respond-in-kind targets of Country X's reprisals. An in-depth examination is still needed as to whether Country X would be able to inflict a level of degradation at least equal to what Country X suffered. If Country X tries but cannot equal the first blow, then its threat credibility will be further diminished. Yet if it retaliates too hard, it could trigger unexpected consequences and the conflict's spiraling. Unfortunately, at the current stage of technical advancement, cyber weapons' effects are hard to predict precisely – even more so if improvised for battle in the context of rapid retaliation. Country X is faced with a second problem: a thresholds issue.[6] Country X does not have a response-in-kind solution, that is, a credible retaliatory threat. A doctrine of "massive retaliation" policy in cyberspace may be subject to the same critiques as the one formulated by Will Kaufman against Eisenhower's NSC-162/2 in 1954[7] – with the added caveat that "massive" is hard to define, unless it applies to assured mass civilian casualty. At the same time, the absence of retaliation evidently goes against the principles of response in kind. It would invite further aggression.

At this stage, there are no good retaliatory options for Country X. If attacks have reached certain damage thresholds and Country X feels otherwise threatened by its geopolitical situation, then it may want to intimate to neighboring countries that attacks will have consequences. It will then try to respond in kind imperfectly by highlighting its most capable and

credible non-cyber, kinetic threat, for example by flexing muscles through a show of air or ground forces. This measure will have adverse diplomatic consequences if attribution is not well established, and it could backfire if cyber attacks continue, actually raising the credibility stakes for Country X now that it has exposed its conventional forces. However, if a cyber attack does not seem to exact too high a price and if its origins remain efficiently obfuscated, then Country X may want to defuse tensions and lower the stakes. Difficulties could be attributed to non-state or technical origins. Then Country X could accept the help from Country B via the software security firm. Of course, as noted, this help would come at a price.

A First Strategy of "Reduction in Asymmetrical Information": Elucidation of Thresholds

An Evaluation Framework

An optimal course of action may exist for Country X. First it must understand what types of attacks it is facing in order to devise the best response. In particular, two main informational issues, mentioned above, must be solved: attribution and thresholds.

Attribution must be strictly linked with the issue of "plausible deniability" because at stake are the political and diplomatic consequences of lack of attribution. Threshold definition is an even more complex problem: there is an inherent difficulty in defining "simple, recognizable, thresholds" in cyber-attacks.[8] Actions leading to thresholds can be split into two types: (i) those with direct effects on a nation (such as industrial disruption or loss of life) and (ii) military preparations that precede these effects (such as military mobilization or reconnaissance operations). Does the setting of logical trap doors in an opponent's electrical grid constitute an act of war? Is there an equivalent in cyber warfare for enemy mobilization and massing at the borders? These questions cannot be easily answered, especially as they refer to issues such as the thresholds for retaliation along the "curve of credibility."[9] The *Tallinn Manual*, written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence, is a necessary starting place but does not at this time authoritatively answer all of these questions.[10] In a more general and historical sense, these are issues at the heart of the strategic conduct of nations, answered on a case-by-case basis and grounded in practical reality, but they have not been comprehensively formalized. Cyber strategy may necessitate an additional

effort at conceptualization. Though the task is beyond the scope of this article, some initial shortcuts may be noted.

A starting place, cited in the growing literature on cyber warfare studies as well as the *Tallinn Manual*, is direct effects.[11] This is an approach that can be understood by many militaries around the world, starting with the US Air Force, still a proponent of Effect-Based Operations, linking actions, effects, and objectives.[12] As highlighted by the *Tallinn Manual*, it also has legal precedents, especially around the term of "scale and effects."[13] Yet what effects constitute crossing a red line for the defender? It is easiest to start with what is benign or tolerable, then explicate what can never be tolerable and would automatically elicit military retaliations. In between lies the territory of the crises.

For example, espionage is tolerable (albeit not officially). It enjoys international tolerance because it is "an extension of monitoring regimes" that thereby enables functional cooperation.[14] This tolerance seems to have extended to some cyber applications of espionage.[15]

What is never tolerable, what would automatically elicit military reprisals, is action leading directly to significant loss of life among non-combatants. In general, this action would be interpreted as a voluntary breach of the laws of armed conflict with regard to *jus ad bellum* as expressed in the 1949 Geneva Convention and clearly restated by the *Tallinn Manual*.[16] In strategic terms, what is never tolerable, what means war, is also initially obvious: destruction of a part or the totality of the sanctuary. This extends to any significant attempt at suppression of the protective institutions of the sanctuary. Because the state holds the monopoly on large-scale violence,[17] both the capabilities for large-scale violence and the monopoly-holding decision center commanding their use must be protected. In practical terms, preserving the sanctuary means first and foremost protecting the life of civilians. War then becomes inescapable if the nation suffers a significant loss of life.

With regard to large-scale violence capabilities, some weapons are essential: first and foremost the nation's survivable second strike force, but also any weapon systems deployed so widely that malfunctions would significantly hamper the defense of the sanctuary. These include the specific networked communication systems and sensors required for the proper use of those weapons. They also include the intergovernmental communication systems necessary for the head of state and staff to command and control

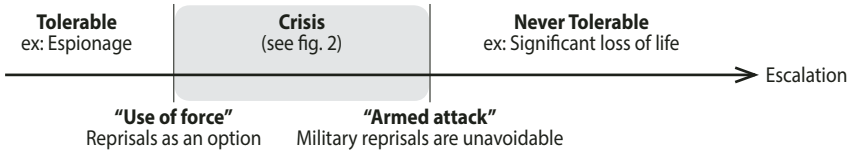
these capabilities, as well as for heads of states to communicate. Such provisions were agreed upon by the two superpowers during the Cold War. The 1971 Accident Measures Agreement and Hotline Modernization Agreement established protection of satellite communications essential to US-USSR communications in times of crisis, as well as the communication facilities for missile warning systems.[18] In addition, attempts at first responder forces and at medical assets that limit significant loss of life constitute red lines. Elements reflecting this understanding were agreed upon by Russian and American diplomats in 2011 and were included in the *Tallinn Manual*, as a way to more generally align the conduct of cyber operations with the current laws of armed conflict.[19] These measures include assets and communication systems for command and control for medical and first responder forces, including with the head of state. Protecting the communication systems does mean preserving data from external corruption: if data cannot be protected then, de facto, the communication systems as means of sending the right instructions are being sabotaged.

Finally, there is the question of economic protection of the sanctuary. At what point do economic damages become so harsh that war is inescapable? Political literature hints that economic hardship can bring about political change: recessions can lead to changes of the ruling party in democracies[20]; depression can bring about regime change in the form of the rise of extremist movements, as shown in the interwar period.[21] If such economic upheavals are brought about by cyber sabotage, they constitute a coercive action intended to destroy the political integrity of the State.[22] This political result would come on top of the resource constraints imposed on the military by economic hardships, which in themselves constitute a threshold if there is significant reduction in military preparedness. Other scenarios could also hint at direct manipulation of the political control organs of the state (for example, electronic corruption of voting systems or mass electronic blackmailing of elected officials). If political majorities could be defeated by such cyber sabotage, it would constitute a significant attempt to weaken the integrity of the state, and thus the crossing of a red line.

In this framework, those effects that are never tolerable hurt so severely that they are easily and blatantly recognizable as such. In the *Tallinn Manual*, attacks yielding such effects are construed as "armed attacks."[23] At this threshold, military reprisals are a certainty. If the identity of the attacker is known, then it is subject to the idiom of military action established among

states. The rules of this idiom apply, ensuring what Thomas Schelling has called the diplomacy of violence.[24] States are entering a game of escalation, from conventional retaliation to potentially strategic reprisals. Cyber weaponry becomes an adjunct to other weapon systems.[25] States can credibly respond in kind with non-cyber weaponry. This will bring clarity and recognizable accents to this dialogue, as illustrated in figure 1.

Figure 1. Decision Framework with Tolerance for Effects



If the effects are recognizable and have an impact on civilian populations or assets although the identity of the attacker is unknown, then the action can be construed as terrorism. Hackers enabling these attacks without a recognized national attribution are acting as unlawful combatants[26] or unprivileged combatants,[27] that is, civilians who directly engage in an armed conflict in violation of the laws of war. Because they cannot be linked with a state bound by the limitations of the 1949 Geneva Convention while conducting military operations against military targets, they pose a de facto threat to any civilian targets the moment their attack causes harm that is never tolerable. The response to such a terror campaign must lead to the arrest of the hackers, or at a minimum to punishment of the state harboring them, as per the evolving legal standard applied in the attack against the Islamic Emirate of Afghanistan after the events of September 11, 2011, and in particular in light of UN Security Council Resolutions 1368 (2001) and 1373 (2001).[28] As in the case of nuclear terrorism with lack of attribution, the collection of intelligence becomes central for any retaliatory measures.[29] This issue is explored below in the section on joint compellence.

In the area between the tolerable and the never tolerable exists the territory of crises and its many shades of gray. The harm is conspicuous enough to be construed as a use of force but its severity is not elevated enough to identify it with certainty as an armed attack.[30] According to the International Court of Justice, as cited in the *Tallinn Manual*, "not every use of force rises to the level of an armed attack."[31] The crisis can be kept outside of the public eye – a default option to avoid tying one's hands too much

within the unchartered waters of cyberspace. Still, the crisis will be real. Uncertainty here has many sources. The never-tolerable effects may not be observable yet, but they could be perceived as an imminent outcome: if online banking problems spread and last a few weeks, would they lead to financial panic? Could losses be easily recovered? The same questions apply if the energy grid is breached. On Day 2, it might be hard to tell. Additionally, not only might direct effects be hard to assess; the meaning of the enemy's military actions in cyberspace, its "virtual mobilization," might also be difficult to evaluate. The last point is critical because, following the rules of warfare first described by Sun Tzu, surprise is the key to victory[32]: the better warrior will not create patterns or precedents. His or her moves will be difficult to evaluate.

Nonetheless, this grey area must be addressed and charted. The escalation categories delineated by Herman Kahn in *On Escalation*[33] are useful here. What is the intensity of the attack, as a probability of reaching the never-tolerable level? How many different components of the nation seen as a system are being attacked? What is its evolution and tempo – especially as intense acceleration could be indicative of impending physical military actions? Using Herman Kahn's delineation, a simple distinction can be drawn between:

a. What is not benign, but reflects self-limitation in escalation: the attack is limited in intensity and cannot be construed as threatening non-combatants; it is limited in scope: only one type of targets is being attacked; it is limited in its temporal dimension: it happens only once or a few times, or has a date of termination. These attacks can be labeled as limited.
b. What is not benign and can be construed as potentially escalating: the intensity or scope of the attack seems not to be self-constrained and could be escalating; or there is repetition and acceleration along the temporal dimension, without a distinct termination date. These attacks can be labeled as escalating attacks.

For example, if GlobalWorm was recognizably set to alter the functioning of only very specific software or equipment, if the software or equipment specifically targeted by GlobalWorm was only for military use or dual-activities, if the effects did not lead to significant collateral damage among civilian personnel or civilian life, and if GlobalWorm had a recognizable date of expiration – for example with digital certificates protecting it and it

was due to expire at a certain time – then the GlobalWorm attack against Country X would be a limited attack. This does not seem to be the situation in the Country X case. Effects are not limited and circumscribed to specific equipment, but are escalating. They are also hard to recognize: what may be the secondary effects of 48 hours without online banking?

In simplified terms, effects that are recognizable (that is, they can be acknowledged with all immediate consequences fully understood)[34] but escalating ,and effects that are hard to recognize (that is, not all immediate consequences are fully understood) can be grouped together: both pose a high risk of surprise, miscalculation, and escalation (figure 2).

Figure 2. Decision Framework for "Crisis" (Detail)

		Discerning Effects	
		Recognizable & Limited	**Hard to Recognize/ Recognizable & Ascalating**
Discerning Identity	Known	Special Ops/Limited Strike Warning shot	Attacks against some tactical weapon systems Low intensity attacks against civilian
	Unknown	Convert Ops Espionage Operation (uncovered)	Sabotage campaign Low intensity terror Reconaissance Operation

An Evaluation Process

The "hard to recognize" category of effects remains highly problematic. A sufficient level of prediction for these effects is difficult to achieve: these are not what the *Tallinn Manual* terms "reasonably foreseeable" harms.[35] To rely on observation of effects as comprehensively as possible with centralization of intelligence, or to develop an analysis of the mode of action of the malware in its software environment is not sufficient. The impacts on a "nation seen as a system," to use the concepts of Col. John Warden,[36] cannot be understood through these necessary but insufficient first steps. Such an evaluation is the purview of modeling, simulation, and analysis of system of systems, including economic and social components. The objective of this evaluation is to determine the expected political harm against the defending state.

In a defense context, the further analytical step will naturally lead to a reverse-engineered "Effect Based Operations" (EBO) analysis. The point here is not to achieve the required precision necessary for an offensive use of EBO that has been elusive so far with current software tools.[37] The objective is different: it is, in a defensive use, to deploy an idiom for cyber warfare made of internationally recognized thresholds. This baseline would link cyber actions with direct effects and intended objectives. It would also serve to legitimate all options reactions, including diplomatic or kinetic actions. Here, "simple, recognizable, and conspicuous" will trump "most precise." To be trusted, this idiom can only be enunciated by the most preeminent cyber powers.

However, international participation in its development by other nations, perhaps along the logic of concentric circles, will ensure that it is recognized by many and thus becomes conspicuous. To be credible, it will have to reflect the real impacts on a nation's curve of credibility. To that effect, it may follow the path laid down by Col. John Warden, and pursue a robust course of studies and simulations to understand the networked nation as a system. Not only could the internet be tested in virtual "cyber ranges;" sub-components of the nation could also be simulated. All sorts of organizations and infrastructures take part today in the release of big data sets, from open data projects in public sectors to application programming interfaces (APIs) in internal corporate and industrial processes,[38] and to social and political sentiments as expressed in social networks. This approach, in turn, promises to help develop a better and much finer baseline modeling of the networked nation as a system. These dynamic data models can then be tested against simulated shocks. Here too, exactitude is not as important as agreed-upon, credible, ballpark estimates. However, this development will be an ongoing effort, as cyberspace is consistently evolving.

Understanding thresholds does not resolve the second main informational issue: attribution. The latter will require a specific intelligence, diplomatic, and coercive effort.

A Second Strategy of "Reduction in Asymmetrical Information": Elucidation of Attribution with "Joint Compellence"

Attribution

Because cyberspace consists of three pillars – hardware (calculation, memory, or communication devices), software, and brainware[39] – intelligence work

must investigate and develop hypotheses for each of these three sources. Clues as different as IP traffic patterns, styles of coding, and methods of actions should feed an attribution matrix. It should also include classical human intelligence on hackers themselves and their political sponsors. These investigative activities should adhere to the best practices in elucidation, with emphasis on deductive methods applied to intelligence as suggested by Ben-Israel.[40] As one methodology in the context of general intelligence works suggests,[41] attribution hypotheses could be laid out in different buckets (for example, "Hypothesis #1: Country Y is the aggressor"; "Hypothesis #2: Country Z..."). Then, empirical data refuting each hypothesis could be set against each bucket. Stacking data against attribution hypotheses would be a first step toward identifying which country is most liable to be the originator.[42] This would require advance identification and simulation of the multiple models of necessary preparations required to launch a massive cyber attack for each country. These models of preparation would of course include additional defensive hardening efforts and obfuscation efforts. Ideally, then, deductive A/B tests in the manner of controlled experiments launched against possible culprits could be set to confirm or infirm attribution hypotheses. For example, taking a page from the strategies used by fictional character George Smiley, by simulating unexpected effects of the malware, the true place of origination could inadvertently reveal a surge in unease and embarrassment.[43] The detection of this unease would help with attribution.

Excellence in truth seeking is critical for establishing defense. It is instrumental in convincing allied countries that one is not trying to manipulate them. In return, once genuinely convinced, these countries can then serve as the equivalent of character witnesses toward the greater world audience, and can increase diplomatic acceptance of retaliatory options. Excellence in truth seeking also ensures that the political echelon of the defending country is not making a grave attribution mistake. The government has confidence in its own decision. At this point, the government becomes more at ease than before the elucidation phase to explore non-public, non-retaliatory measures if need be. As in any counter-intelligence work, it is perhaps best to temporarily maintain the illusion for the enemy that his stratagem has not been uncovered.

In cyberspace, truth is power, as it is for any other information domain, such as traditional intelligence.[44] The means and methods of establishing

a quasi-incontrovertible truth are key instruments of power. As such, they can become instruments of influence. One day, the cyber-diplomatic scene could resemble the civilian internet mainstream scene, where some of the largest search engines or reference content providers (such as Wikipedia) are already vying for the highest relevance in terms of content. After all, the most important feature of any information system is the ability to distinguish the right signal.

However, it may be difficult to share the attribution techniques and data described above with a large audience of countries, as is often the case in intelligence sharing. In an increasingly multipolar world, this difficulty could lead to further defense paralysis or diminished deterrence credibility if no method to jointly carry out attribution elucidation is established. However, such a method may exist by way of a large-scale deductive test carried out publicly, especially as deduction is a superior method for truth elucidation in intelligence analysis.[45] In *Cyberwar*, Richard Clarke and Robert Knake highlight the "arsonist principle": the burden of the investigation should be shifted from the investigators to the nation in which the attack was launched.[46] If the suspected nation refuses to cooperate, it would be held responsible. Then an international body − what Clarke and Knake term an "International Cyber Forensics and Compliance Staff" − could suggest cyber sanctions, from shutting down certain ISPs to even blockading the nation from cyberspace.[47]

Building and expanding on this approach, there is actually the possibility to defend against some of the potentially most severe cases of cyber warfare offensive and reestablish cyber-deterrence.

A crucial initial observation is appropriate here: in addition to forcing attribution via the arsonist principle, this approach can actually establish it formally. In diplomatic terms, it can deny the offender the option of plausible deniability. Establishing attribution is as much an intelligence investigation as a diplomatic process. Other nations must be convinced. First, the credibility of the truth is best established when other observers (or testers) can confirm or infirm the attribution hypothesis. This social process is well established, from the two-witness rule governing the trials of treason as early as the Elizabethan era in England,[48] prefiguring Hooper's rule on concurrent testimony[49] to modern statistics where confidence in predictions is increased by the number of observations. To create a public test is to force other nations and their people to become observers. Second,

a diplomatic process ensures higher coordination and thus strengthens the cyber blockade required to pressure suspicious states. The strength of the blockade is vital for the threat to be capable. If it can be significantly evaded, as Western powers managed to do during the Berlin Crisis of 1948 against the Russian blockade, then the threatening country fails.[50] If the blockade cannot be evaded, then the threatened country is forced to decide between escalation and backing down – and if the stakes are too high, it may back down as Russia did during the Cuban Missile Crisis. In addition, carrying out the attribution process first with close allies, then with a wider group of nations, might foster goodwill, rapprochement, and greater understanding toward the defending state. That, in turn, frees up political margins of maneuverability if the defending state is to move toward additional diplomatic, economic, or military sanctions beyond cyberspace and a cyber blockade. It lends further credibility to what is essentially a compellence strategy, as described by Schelling: "a threat intended to make an adversary do something."[51] Suspected states are compelled to collaborate or else they will continue not only to suffer from the cyber blockade, but also to single themselves out. In that new context, countries wanting to prove their goodwill will genuinely cooperate. Perhaps they may even share their own intelligence with regard to attribution, as a further proof of goodwill. Countries that do not cooperate will de facto reveal their true intent.

In addition, cooperation is all the more easily compelled when it means that cooperating countries do not have to lose face. Taking a page from Rattray and Healey's model of public health for cyber security,[52] the metaphor of World Health Organization (WHO) investigation teams at times of pandemics can be used. National governments do not have to be nominally accused – they do not have to be held initially responsible for the pandemics. Officially, the blame is placed on the malware or the nefarious teams of hackers behind it. Using the public lack of attribution for the sake of the compellence action, the coalition of defenders can then request the heads of the suspected states to cooperate. A cyber blockade can still be implemented, analogous to WHO quarantining regions or countries during pandemics. Thus the cost of not cooperating still weighs on the offenders – and it will grow as other states cooperate and the offending state becomes ever more isolated. Conversely, the cost of cooperating is lessened because there is no loss of face. And still, there is a genuine threat,

that is, a cost for having launched the operation in the first place: finally accepting cooperation, the offending capabilities (servers, codes, hackers) will be publicly branded. They will be rendered inoperative. Ongoing cooperation – and the additional intelligence it will provide – will help maintain this calculus. This is the end game. Defecting nations are forced to cooperate again. Their investment in defection capabilities is nullified. But there is not necessarily the audience cost attached to backing down. This makes renewed cooperation acceptable, and thus potentially stable. Additionally, the difficult task of a formal, public attribution, requiring a very high degree of certainty because of its public format, is rendered unnecessary.

Strategies and Requirements for Joint Compellence

To be successful, this strategy must leverage the attribution efforts already mentioned. The quality of intelligence is critical in conducting this compellence approach. Heads of state are at the heart of this strategic conflict. Their methods and manners of communicating threats affect the credibility of their retaliatory threats. The defending head of state, assisted by a coalition of friendly countries, behaves like a police investigator interrogating suspects: "Give us access and information. Cooperate with us – or we keep you locked down." This is bargaining, comparable to an actual police interrogation.[53] The better the intelligence, the better the design of the interrogation and the more efficient the process: "Information power may be the most important source of power" in interrogation.[54] Used as an argument in the interrogation process, it demonstrates the deep knowledge of the interrogator, thereby reaffirming his credibility because he cannot be deceived. The interrogated will then hesitate to misinform; at the same time, the interrogator demonstrates that he can be a knowledgeable partner. A cooperation deal will be solid. Finally, as mentioned above, the interrogator can run tests to check the reaction of suspected states. These tests could simulate unexpected consequences for the defending state. By counter-manipulating, the defending state can instill doubts in the aggressor: cyber weapons are not reliable and could trigger an undesired escalation. The defending state could more easily mobilize external sympathy and support as its vital domestic interests are made more vulnerable to the malware. Solidarity from other countries is all the more extended as the malware has no defined origins: anyone could be its target.

The diplomatic aspect of the compellence process helps turn the strength of the attack against the attacker, as in Judo. The harsher the cyber attack, the stronger the solidarity between the defending state and its ally – and the tighter the cyber blockade against suspected states. Defense retakes the initiative. It can dictate the tempo in escalation control.

This compellence strategy to resolve attribution is feasible because behind a sophisticated attack, there must be a nation-state. Non-state actors are necessarily harbored by advanced developed states. Terrorist organizations based in under-developed, failed states do not currently have the technical capabilities to wage strategic, sophisticated cyber attacks. For example, Stuxnet was a piece of coding developed by very talented IT engineers; it used digital certificates perhaps stolen from two legitimate Taiwanese companies,[55] and it had been tested on a full cyber-physical model that included replicas of the P-1 centrifuges.[56] However, all this requires deep pockets to recruit and retain talent, actual local access to a multidisciplinary pool of talent (especially if cyber-physical models are necessary), and constant training and development as cyberspace is upgrading constantly, not to mention secret services to infiltrate or enable access to privileged software information. These are development capabilities that currently cannot be acquired in tribal areas. In all probability, behind any ad hoc group launching a sophisticated cyber attack, there will be the active sponsorship of an advanced developed nation. Advanced developed nations are to become ever more dependent on access and development in cyberspace for data, instructions, and actual processing. A large portion of business-to-business communication and data processing is shifting to the so-called cloud, that is, servers often situated in foreign locations. In that context, the crippling effects of a cyber blockade may be particularly acute for advanced developed nations that come under suspicion.

This strategy will work if allies of the defending country are also compelled or incentivized to act. Ongoing coordination, agreement on norms, and sharing of processes are prerequisites, before a crisis starts. In practice, cooperation levels might correlate with existing circles, from the closest

allies to the most distant – embracing in cyberspace what is currently the cooperative arrangement at the overall political level.[57] Additionally, in order to give credence to the whole process, there can be a move toward greater cooperation within circles, and greater rapprochement between adjacent circle levels. Gently pointing the way forward has the advantage of solidifying the current level of international cooperation. Even more importantly, the ties that bind these cooperative links should find a credible translation in practical terms. For example, friendly countries can employ additional layers of software used by other friendly countries. Joint use of the same software or standards increases the risks of unexpected consequences for the attacker. It credibly conveys the possibility that to attack one country is to attack all of its allies. Shared use of the same software in cyberspace may play the same role as the US garrison in Berlin during the Cold War[58]: it would create automatic involvement and leave no doubt that the compellence process would be carried out jointly by a coalition of friends.

Finally, defending countries must acquire redundant cyber capabilities to absorb the first shock. Redundant communication and computing capabilities temporarily alleviate bottlenecks. Semantic manipulation could be partly offset by periodically saving critical data in write-only, non-volatile data storage in order to retrieve true pre-attack values. But defensive measures alone are largely insufficient. Without confronting the will of the enemy to learn new attack techniques, the attacker will continue to learn and adapt, mimicking the coevolution (Red Queen) dynamics found in nature.[59] Deterrence will not be achieved. What must be confronted is the attacker's will to learn and not share new offensive techniques: a cost must be imposed on this will to learn and not share. Nevertheless, to absorb the first shock is elemental. Conventional deterrence models posit that short-term weaknesses on the part of the defender can invite attacks[60]: for example, a first blow might be so hard that the defender would not have time to respond properly and mobilize a coalition of allies. Additionally, the attribution process should ideally entail an alternate international team of inspectors. This would ensure that the long "shadow of future"[61] is preserved: whatever happens, the truth will survive. Attribution will be made. Responsibilities will not be evaded.

To summarize, once attribution is made, and once effects can be recognized and evaluated within a defending nation's curve of credibility, informational asymmetries in favor of the offense cease. The idiom of

military action is restored to the benefit of the defender. The defender can make credible retaliatory threats. In particular, after effects are properly recognized, the defender can credibly retaliate in kind by using non-cyber means – diplomatic, economic, kinetic, or strategic. All options are made available anew, thereby giving more weight to the hand of the defender. Non-cyber retaliatory threats may even be superior if proven non-vulnerable to cyber attacks: their resilience will render them highly capable. By setting a limit to the potentially confusing game induced by cyber-only retaliatory means, the defender will signal the translation from cyber attacks to real effects, thus providing a clarity that will force the attacker either to back down or to escalate. In particular, the restrictive environment created by joint compellence will become a difficult situation for the attacker. Again, as the Cuban Missile Crisis demonstrated, in such a situation the non-status-quo power may prefer to back down rather than escalate.

Conclusion: Toward a New Political and Military Doctrine for the Digital Age

The necessity of establishing equivalence between cyber and non-cyber weapons by means of equivalent effects – and the need to switch from cyber to non-cyber retaliatory means – demonstrates the criticality of reframing cyber warfare operations in the context of other weapon systems. Following Edward Luttwak,[62] one-force cyber strategies may at this stage be as confusing and minimally operative as what Luttwak dismissively termed "nonstrategies" – namely, other one-force strategies claiming strategic autonomy such as "naval strategy," "air strategy," and "nuclear strategy."

However, centers of gravity have always shifted as technological disruption changes warfare. The centers of gravity during Cold War fighting were quite different from the ones at the time of Gunderian's blitzkrieg or that of Vauban and its massive fortresses. In the naval domain, strategist Julian Corbett determined that gaining sea control was ensured not by conquering areas of water, which are impossible to hold, but by ensuring the act of passage on the sea.[63] As conflicts move into the digital domain or digital *logos*,[64] centers of gravity are going to shift. The higher criticality of the semantic domain over the physical support reduces the relative importance of communication lines: the internet was built to send information despite the unavailability of hardware. What becomes critical is to ensure that true meaning is protected: Who is attacking? What is being attacked? To know

attribution and to recognize and predict effects become the higher grounds. These are cognitive centers of gravity. In strategic terms, this is knowledge supremacy: to control and to preserve the nation and its sub-systems from information manipulation. To put it differently, in an information domain, truth is the highest ground.

The importance of the digital information domain relative to other components of the networked nation as a system may alter strategic priorities. Additional industrial shifts could further strengthen this new order of priorities. As software continues to "eat the world"[65] and the value of data and data-based applications becomes ever more important, the preserve of the digital *logos* could become as valuable as the physical assets it reflects and partly controls today. In some vital areas, this is already the case: today, wealth is measured and exchanged by means of electronic bits identifying monetary value. So while cyber warfare today is a non-strategy in Luttwak's definition, there is a possibility, small and remote but not nil, that strategy in the digital *logos* claims its autonomy, that it represents both means and ends. Information systems, from DNA to spoken language, are critical to the management of any organism. Therefore such preeminence for the digital *logos* should not be surprising in theory.

This ongoing transformation will mark a profound change in the role of the state defending the nation. The state must maintain the monopoly over large-scale violence, which can be construed as protecting physical assets from corruption by kinetic force. It will also have to protect the reliability of data in use by strategic military and civilian systems, and at a higher level, maintain accuracy of strategic information for the situational awareness of the nation as a system. The state will be the custodian of last resort for the truth.

All these remote possibilities are portended by the ever-increasing acceleration of IT calculation and storage capabilities. As an example, the calculation power of top supercomputers will increase by a factor of at least 10^3 Floating-point Operations per second (FLOPs) over the next ten years.[66] As the scale of calculating power continues to increase, major changes in machine learning and simulation cannot be discarded.[67] The limitations found today in analysis of EBO and the nation as a system may be as temporary as the difficulties in the field of artificial intelligence. For decades, artificial intelligence has been defined as a difficult field of research.[68] Today, it is proving promising again.[69] In this context, advanced

EBO capabilities for further simulation and analysis of effects could also change the calculations regarding national powers.

However, an increase in simulation means further predictability: a longer, more predictable view of the game is then possible. The better the information is regarding each party's true capability, the lesser the risk of war. Additionally, both Zagare[70] and Axelrod[71] demonstrate in their respective works that the longer the perceived game, the higher the chances that cooperative (or status-quo) strategies dominate.[72] Finally, successful enforcement of a joint compellence strategy would also, in the long term, favor the status quo: if the fruits of defection are being denied and the end game of joint compellence is further cooperation, then defection becomes an unnecessary cost. This automatically increases the relative value of the status-quo choice (namely, continued cooperation). As Perfect Deterrence Theory posits, the overall increase in the value of the status-quo choice over any defection strategies is also one of the most important factors to ensure stability.[73]

In this context, the complementary approaches of advanced nation-as-a-system simulations and joint compellence suggest that the accelerated immersion of our human civilization into the digital *logos* could become an additional force for peace and stability. These strategies of reduction in asymmetrical information could serve as key building blocks toward a new doctrinal framework for the societies of the digital *logos*. This doctrinal framework will continue to promote peace and stability and will have to integrate current nuclear and conventional deterrence doctrines. It will also recognize the new preeminence of digital information systems in civilian affairs and therefore in military affairs. Ultimately, it will lead to a refined definition of what is a conflict. The doctrine of mutually assured destruction has transformed wars between global peer-competitors into a futile exercise in conspicuous, immensely negative sum games, thanks in large part to survivable second-strike forces. A doctrine of enforced digital cooperation, supported by the elimination of any asymmetrical information advantages of a challenging country, will further suppress spiraling escalation risks during international crises in our twenty-first-century digital civilization.

Notes

1 Sun Tzu, *The Art of War*, transl. Lionel Giles (1910), ch. 3, http://www.gutenberg.org/cache/epub/132/pg132.html.

2 This article can be viewed as a follow-up to the issues of destabilization in cyberspace discussed in Guy-Philippe Goldstein, "Cyber Weapons and International Stability," *Military and Strategic Affairs* 5, no. 2 (2013): 121-39.
3 See Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge Studies in International Relations, 2000), pp. 296-301.
4 Paul K. Huth, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press, 1988), cited in Zagare and Kilgour, *Perfect Deterrence*, pp. 296-301.
5 For further details on this issue and introductory literature, see for example Goldstein, "Cyber Weapons and International Stability."
6 For further details on this issue and introductory literature, see for example Goldstein, "Cyber Weapons and International Stability."
7 William W. Kaufmann, *The Requirements of Deterrence* (Princeton: Center of International Studies, Princeton University, 1954). See also the discussion in Fred Kaplan, *The Wizards of Armageddon* (Stanford: Stanford University Press, 1983), pp. 193-200.
8 See discussion in Goldstein, "Cyber Weapons and International Stability" with reference to Schelling's definitions of red lines in Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 137.
9 See discussion in Goldstein, "Cyber Weapons and International Stability," with reference to the concept of "curve of credibility" in Carey B. Joynt and Percey E. Corbett, *Theory and Reality in World Politics* (Pittsburgh: University of Pittsburgh Press, 1978), p. 94-95.
10 See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), p. 88: "The international Group of Experts achieved no consensus as to whether non-destructive but severe cyber operations satisfy the intensity criterion." See also pp. 82-83, comments #14 and #15.
11 See Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," in *The Virtual Battlefield: Perspective on Cyber Warfare*, eds. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009) for a discussion of cyber warfare in the context of effect-based warfare. More explicitly, the *Tallinn Manual* states that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (Rule 11) and that "a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Rule 30). The ensuing discussion does highlight that "'acts of violence' should not be understood as limited to activities that release kinetic force. This is well settled in the law of armed conflict. In this regard, note that chemical, biological or radiological attacks do not usually have a kinetic effect on their designated target, but it is universally agreed that they constitute attacks as a matter of law." See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

What matters is the direct effect on civilian populations or on properties, whatever the way – kinetic or not – these direct effects have been caused.

12 Paul M. Carpenter and William F. Andrews, "Effects-based Operations – Combat Proven," *Joint Force Quarterly* 52 (First Quarter, 2009): 78-81.

13 The international group of experts of the *Tallinn Manual* mentions the notion of "scale and effects" posited in the *Nicaragua* judgement of the International Court of Justice, "Case Concerning Military and Paramilitary Activities in and against Nicaragua" (Nicaragua v. United States of America), Judgement, *I.C.J. Reports* (1986), p. 14. See Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 45.

14 Christopher D. Baker, "Tolerance of International Espionage: A Functional Approach," *American University International Law Review* 19, no. 5 (2003): 1091-1113.

15 See for example Thomas C. Wingfield, "Legal Aspects of Offensive Information Operations in Space," *USAF Academy Journal of Legal Studies* 9 (1999): 140: "The lack of an international prohibition of espionage leaves decisionmakers with the usually acceptable liability of merely violating the target nation's domestic espionage law." See also Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: Rand Corporation, 2009), pp. 23-24. In the *Tallinn Manual*, the discussion of Rule 10 ("prohibition of threat or use of force") states that "not all cyber interference automatically violates the international law prohibition on intervention.... As noted by the Court in *Nicaragua*, 'intervention' is wrongful when it uses methods of coercion. It follows that cyber espionage and cyber exploitation lacking a coercive element do not *per se* violate the non-intervention principle." Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

16 See Part I, Chapter 2, Section 2 ("Self-defence") and Rule 32 ("Prohibition on attacking civilians") in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

17 See Charles Tilly, "War Making and State Making as Organized Crime," in *Bringing the State Back*, eds. Peter Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambridge University Press, 1985); see also Antonio Giustozzi, *The Art of Coercion: Armed Force in the Context of State Building* (CSRC Seminar, 2008).

18 See Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between The United States of America and The Union of Soviet Socialist Republics, September 30, 1971, http://www.state.gov/t/isn/4692.htm; Agreement Between The United States of America and The Union of Soviet Socialist Republics on Measures to Improve the U.S.A.-USSR Direct Communications Link, September 30, 1971, http://www.state.gov/t/isn/4787.htm, cited in Laura Grego, *A History of Anti-Satellite Programs* (UCS Global Security Programs, 2012).

19 See Karl Frederick Rauscher and Andrey Korotkov, *The Russia-US Bilateral on Critical Infrastructure Protection: Working Towards Rules for Governing Cyber*

Conflict (New York: East-West Institute, 2011). See also Part II, Chapter 3 ("The law of armed conflict generally"), in particular Rule 20 ("Applicability of the law of armed conflict"), and Chapter 4 ("Conduct of hostilities"), in particular Rule 29 ("Civilians") and Section 3 ("Attacks against persons"), in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

20 Michael S. Lewis-Beck and Mary Stegmaier, "Economic Determinants of Electoral Outcomes," *Annual Review of Political Science* 3 (2000): 183-219.

21 Alan de Bromhead, Barry Eichengreen, and Kevin Hjortshøj O'Rourke, *Right Wing Political Extremism in the Great Depression*, Discussion Papers in Economic and Social History, No. 95 (Oxford: University of Oxford, 2012).

22 The *Tallinn Manual* defines as unlawful a cyber operation against the political independence of any state (Rule 10), Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

23 See Rule 11 in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 51.

24 See Thomas C. Schelling, *Arms and Influence* (Yale University Press, 1966), pp.1-34 & pp.126-189

25 See Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 330.

26 See the *Quirin* case of 1942 on German saboteurs, with particular emphasis on saboteurs not wearing national emblems: "The spy who secretly and without uniform passes the military lines of a belligerent in time of war, seeking to gather military information and communicate it to the enemy, or an enemy combatant who without uniform comes secretly through the lines for the purpose of waging war by destruction of life or property, are familiar examples of belligerents who are generally deemed not to be entitled to the status of prisoners of war, but to be offenders against the law of war subject to trial and punishment by military tribunals." U.S. Supreme Court, *Ex Parte Quirin*, 317 U.S. 1 (1942). Unlawful combatants are nonetheless entitled to "to be treated with humanity and, in case of trial, shall not be deprived of the rights of fair and regular trial prescribed by the present Convention." See Geneva Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949 (GCIV).

27 On "unprivileged belligerents" see comment #17 in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* p. 100.

28 See Ben Smith and Arabella Torp, "The Legal Basis for the Invasion of Afghanistan," *House of Commons, International Affairs and Defence Section*, February 26, 2010, pp. 4-5.

29 See for example Ashton B. Carter, Michael M. May, and William J. Perry, *The Day After – Action in the 24 Hours Following a Nuclear Blast in an American City*, Report based on Workshop (The Preventive Defense Project, Harvard and Stanford Universities, 2007), in particular "6. Retaliation and deterrence," pp. 15-17.

30 See Rule 11 in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.
31 See Rule 13, comment #5, citing the *Nicaragua* judgment, para. 191, in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 55.
32 "All warfare is based on deception" quoted in Sun Tzu, *The Art of War*, transl. Samuel B. Griffith (New York and Oxford: Oxford University Press, 1963), p. 66.
33 Herman Kahn, *On Escalation* (London: Pall Mall Press Ltd., 1965).
34 The observation of effects should be complemented by a technical analysis of the malware itself. However, this could take too much time. For example, Stuxnet was identified by Virusblokada in June 2010 but only significantly analyzed by November 2010. See Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010). Hence the requirement for up-to-date information alerts from all military and civilian activity centers to a cyber intelligence collection point will make it possible to reinterpret cyber incident data points to form a coherent national picture for use by national security institutions.
35 See Rule 30, comment #5, in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 106.
36 See John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (1995).
37 See James N. Mattis, "USJFCOM Commander's Guidance for Effects-based Operations," *Joint Force Quarterly,* no. 51 (2008); see also criticism of USJFCOM decision by USAF officers in Paul M. Carpenter and William F. Andrews, "Effects-based Operations Combat Proven," *Joint Force Quarterly*, no. 52 (2009).
38 On the rise of corporate APIs, see Robin Vasan, "Business Process API-ification: The LEGO Promise Fulfilled," *GigaOm*, October 6, 2012, http://gigaom.com/2012/10/06/business-process-api-ification-the-lego-promise-fulfilled/ and Mark Boyd, "Getting C-Level Buy-In: Demonstrating the Business Value of APIs," *ProgrammableWeb*, September 11, 2013, http://blog.programmableweb.com/2013/09/11/getting-c-level-buy-in-demonstrating-the-business-value-of-apis/.
39 See discussion in Goldstein, "Cyber Weapons and International Stability," for main components of cyberspace.
40 Isaac Ben-Israel, *Philosophie du renseignement* (Paris : Editions de l'Eclat, 2004).
41 Ibid.
42 This example is directly inspired by the 1973 Yom Kippur War post-mortem analysis described in Ben-Israel, *Philosophie du renseignement*.
43 To reveal the identity of "Gerald," the mole working for the USSR, Smiley has a message sent to the head of the "Circus" that forces "Gerald" to seek an emergency meeting with his Soviet handler at an already identified safe

house. This is the test that allows Smiley to identify "Gerald" while breaking into the safe house. In John Le Carré, *Tinker Taylor Soldier Spy* (London: Hodder & Stoughton, 1974).

44 See discussion in Goldstein, "Cyber Weapons and International Stability," for a comparison between the "digital" domain that establishes cyberspace and the "confidential information" domain that establishes the realm of traditional intelligence.

45 See Ben-Israel, *Philosophie du renseignement*.

46 See Richard Clarke and Robert K. Knake, *Cyberwar* (New York City: HarperCollins, 2010), pp. 249-54.

47 Ibid.

48 L. M. Hill, "The Two-Witness Rule in English Treason Trials: Some Comments on the Emergence of Procedural Law," *American Journal of Legal History* 12 (1968): 95-111.

49 See Glenn Shafer, "The Combination of Evidence," *International Journal of Intelligent Systems* I (1986): 155-79.

50 See the game theory analysis of the 1948 Berlin Crisis in Frank C. Zagare, *The Dynamics of Deterrence* (Chicago: University of Chicago Press, 1987), pp. 11-28.

51 See Thomas C. Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1963), p. 69.

52 See Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," in *The Future of American Power in a Multipolar World*, eds. Abraham M. Denmark and James Mulvenon (Washington, D.C.: Center for a New American Security, 2010), pp. 151-72.

53 See Daniel L. Shapiro, "Negotiation Theory and Practice: Exploring Ideas to Aid Information Eduction," in *Educing Information*, eds. Robert A. Fein, Paul Lehner, and Bryan Vossekuil (Washington, D.C.: Intelligence Science Board, National Defense Intelligence College Press, 2006), pp. 267-80.

54 Quote from M.P. Rowe, "Negotiation Theory and Educing Information: Practical Concepts and Tools," in *Educing Information*, eds. Robert A. Fein, Paul Lehner, and Bryan Vossekuil (Washington, D.C.: Intelligence Science Board, National Defense Intelligence College Press, 2006), p. 295.

55 Stuxnet used compromised digital certificates from Taiwanese companies Realtek and JMicron. See Falliere, Murchu, and Chien, *W32. Stuxnet Dossier*.

56 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012.

57 Starting for example with nations from the Technical Cooperation Program ("5 eyes nations") and/or other nations that have a history of cooperating closely in critical programs, in joint cyber operations for example or intelligence-sharing programs, as with the example of nations participating in Base Alliance against al-Qaeda. See Dana Priest, "Help from France Key in Covert Operations," *Washington Post*, July 3, 2005.

58 See Thomas C. Schelling, *Arms and Influence* (Yale University Press, 1966), p. 47.

59 See initial formulation in evolutionary biology, Leigh Van Valen, "A New Evolutionary Law," *Evolutionary Theory* 1 (1973): 1-30; see application to cyber arms race, Rattray, Evans, and Healy, "American Security in the Cyber Commons," the section "Adaptation and counter-adaptation," p. 154; see a first account by a practitioner in Kevin Mandia, "Cyber Threats and Ongoing Efforts to Protect the Nation," Permanent Select Committee on Intelligence, US House of Representatives, October 4, 2011, in particular the lack of deterrence or costs for the attacker.

60 Edward Rhodes, "Conventional Deterrence," *Comparative Strategy* 19, no. 3 (2000): 221-53, in particular 222-23.

61 Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984); see p. 13 for explanation of the "shadow of future" and p. 124 on "enlarging the shadow of the future" to promote cooperation.

62 Edward N. Luttwak, *Strategy: The Logic of War and Peace*, rev. and enlarged ed. (Cambridge: Belknap Press of Harvard University Press, 2001); see Chapter 11, "Nonstrategies," p.168-84.

63 Julian S. Corbett, *Some Principles of Maritime Strategy* (London: Longmans, Green & Co, 1911), p. 90: "Command of the Sea, therefore means nothing but the control of maritime communications, whether for commercial or military purposes."

64 See discussion about digital logos in Goldstein, "Cyber Weapons and International Stability."

65 Marc Andreessen, "Why Software is Eating the World," *Wall Street Journal*, August 20, 2011.

66 In 2010, the fastest supercomputer was the Cray Jaguar, running at 1.8 10^15FLOPS; see top500.org, November 2009-2010. Performances over one exaflop or 10^18 FLOPS could be available by 2020; see Agam Shah, "SGI, Intel Plan to Speed Supercomputers 500 Times by 2018," *Computerworld*, June 20, 2011.

67 Zettaflop capabilities (10^21) could achieve full-weather modelling – the accurate prediction of weather over a two week time span; see Erik P. DeBenedictis, "Reversible Logic for Supercomputing," in *Proceedings of the 2nd Conference on Computing Frontiers*, Sandia National Laboratories (2005), pp. 391-402.

68 Researchers have talked of an "Artificial Intelligence Winter" during at least two periods: in 1974-1980 and 1987-1993. See Jim Howe, "Artificial Intelligence at Edinburgh University: A Perspective," November 1994, School of Informatics, University of Edinburgh; Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach,* 2nd ed. (Upper Saddle River, New Jersey: Prentice Hall, 2003), p. 24.

69 By the mid-2000s, the mood had been reversed on AI and there was talk of a "spring" in AI. See for example John Markoff, "Behind Artificial Intelligence, a Squadron of Bright Real People," *New York Times*, October 14, 2005.
70 See the discussion on rules relaxation and lengthening the game in Zagare, *The Dynamics of Deterrence*, pp. 48-56.
71 See the discussion on the "shadow of the future" in Axelrod, *The Evolution of Cooperation*, p. 13.
72 See Goldstein, "Cyber Weapons and International Stability."
73 Zagare and Kilgour, *Perfect Deterrence*, pp. 293-96.

The INSS Cyber Program

The Institute for National Security Studies (INSS), an independent, non-partisan think tank that is an external institute of Tel Aviv University, deals with issues related to Israel's national security. The Institute holds seminars, forums, and conferences and produces various publications, including monographs, journals, analytical articles, and position papers for decision makers. In 2013, INSS was ranked as Israel's leading think tank and among the leading think tanks in the world in the field of national security. INSS is a public benefit company.

The INSS Cyber Program aims to cultivate knowledge on cyber warfare and broaden the study of its related aspects. It focuses on the conceptualization and creation of a common language regarding cyberspace and national security; development and examination of national policy; and the identification of guidelines for doctrine of cyber warfare for Israel, at both the national and inter-organizational levels. Research aims to contribute to an informed public debate on cyber security and promote strong public policy on the issue.

To this end, the program engages in a variety of research activities in subjects relevant to the field of cyberspace, including: development of a national defense concept for cyberspace; sharing of knowledge and information across organizations and sectors; intelligence and operations in cyberspace; proliferation of malicious codes in the cyber sphere; terrorist and non-state organizations in cyberspace; activities by major states and other actors in cyberspace; and legal and regulatory aspects. In addition, the program publishes a bi-weekly review of cyber intelligence on the basis of open sources. This review, published in English, is distributed by the Cyber Security Forum Initiative (CSFI) as well as through other frameworks.

In order to sharpen the common language and cultivate knowledge, the Cyber Program has established a national professional forum to formulate strategic insights and policy recommendations concerning cyber defense. This forum enables the building of innovative knowledge and connections among the relevant players in both the private and public sector. In addition, it provides decision makers with an important professional resource that researches new issues in the field and publishes position papers.

Forum members include some twenty-five senior figures from three main sectors: government, the defense industry, and research and development in

leading technology companies and academia. The forum holds discussions on a regular basis on a range of subjects, including: conceptualization and creation of a common language in national security contexts; development and examination of a national policy for cyber defense; the interface between the techno-tactical and strategic realms; the interface between the defense sector and the business sector; the boundaries of responsibility between the state and the private sector (organizations and individuals); and knowledge sharing and regulation.

The forum was established in an effort to narrow the gap in the discourse between two realms: the technological, home to many players and where a great deal of knowledge has developed in Israel (and the rest of the world); and the strategic, with an emphasis on Israel, where there is a need for significant improvement in the development of knowledge and policy. Thus a major aspect of the forum's role and its added value in activity and knowledge development in the cyber field in Israel is the connection it forges between the two arenas. Furthermore, the discussion underway in the context of the forum is necessary to achieve the supreme goal: a strong and lasting improvement in Israel's cyber resilience.

In 2013, partly as a result of insights that emerged from the forum's discussions, INSS published recommendations for decision makers concerning the organization of civil defense in cyberspace in Israel. One of the forum's goals during 2014 is to examine the national concept and to make recommendations for decision makers in this field.

INSS Cyber Program Team

Program Director: Dr. Gabi Siboni
Program Coordinator: Daniel Cohen
Cyber Forum Manager: Hadas Klein

Researchers
Prof. Amir Averbuch
Dr. Tal Koren
Dr. Yair Oppenheim
Major M. (IDF – C^{4}I Corps)
Hila Adler
Carmit Valensi

Research Assistants and Interns
Eddo Bar
Roxana Bogdanski
Giorgio Bonadiman
Nir Carmi
Keren Hatkevitz
Sarah Kohne
Sami Kronenfeld
Danielle Levin
Ran Levy
Jeremy Makowski
Amir Steiner
Simon Tsipis
Shlomi Yaas

INSS Memoranda, 2014

No. 145, December 2014, Yoav Zacks and Liran Antebi, eds., *The Use of Unmanned Military Vehicles in 2033: National Policy Recommendations Based on Technology Forecasting – Expert Assessments* [Hebrew].

No. 144, November 2014, Oded Eran, Dan Vardi, Itamar Cohen, *Political Feasibility of Israeli Natural Gas Exports to Turkey.*

No. 143, November 2014, Azriel Bermant, *The Russian and Iranian Missile Threats: Implications for NATO Missile Defense*.

No. 142, September 2014, Emily B. Landau and Anat Kurz, eds., *The Interim Deal on the Iranian Nuclear Program: Toward a Comprehensive Solution?*

No. 141, September 2014, Emily B. Landau and Anat Kurz, eds., *The Interim Deal on the Iranian Nuclear Program: Toward a Comprehensive Solution?* [Hebrew].

No. 140, Oded Eran, Dan Vardi, and Itamar Cohen, *Exporting Israeli Natural Gas to Turkey: Is it Politically Possible?* [Hebrew].

No. 139, July 2014, Arik Rudnitzky, *Arab Citizens of Israel at the Start of the Twenty-First Century* [Hebrew].

No. 138, June 2014, Pnina Sharvit Baruch and Anat Kurz, eds., *Law and National Security: Selected Issues*.

No. 137, May 2014, Emily B. Landau and Azriel Bermant, eds., *The Nuclear Nonproliferation Regime at a Crossroads*.

No. 136, May 2014, Emily B. Landau and Anat Kurz, eds., *Arms Control and National Security: New Horizons* [Hebrew].

No. 135, April 2014, Emily B. Landau and Anat Kurz, eds., *Arms Control and National Security: New Horizons*.

No. 134, March 2014, Yoram Schweitzer and Aviv Oreg, *Al-Qaeda's Odyssey to the Global Jihad*.

No. 133, March 2014, Pnina Sharvit Baruch and Anat Kurz, eds., *Law and National Security: Selected Issues* [Hebrew].

No. 132, January 2014, Yoram Schweitzer and Aviv Oreg, *Al-Qaeda's Odyssey to the Global Jihad* [Hebrew].