Military and Strategic Affairs

Volume 7 | No. 3 | December 2015

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

ISSN 2307-193X (print) • E-ISSN 2307-8634 (online)

Military and Strategic Affairs

Volume 7 | No. 3 | **December 2015**

CONTENTS

Military and
Strategic Affairs

The purpose of *Military and Strategic Affairs* is to stimulate and enrich the public debate on military issues relating to Israel's national security.

Military and Strategic Affairs is a refereed journal published three times a year within the framework of the Military and Strategic Affairs Program at the Institute for National Security Studies. Articles are written by INSS researchers and guest contributors. The views presented here are those of the authors alone.

The Institute for National Security Studies is a public benefit company.

Graphic Design: Michal Semo-Kovetz, Yael Bieber, Tel Aviv University Graphic Design Studio
Printing: Elinir

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 6997556 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

Military and Strategic Affairs is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

ISSN 2307-193X (print) • E-ISSN 2307-8634 (online)

Between Imagined Reality and Real Terrorism

Daniel Cohen

This essay focuses on how the Islamic State and other non-state actors use media and technology to influence individuals and groups by combining Internet activity with activity in the real world. The Islamic State functions in an actual physical and geographical space, in cyberspace, and within the conscious realm. Eachserves the Islamic State's communications, propaganda, psychological warfare, and recruitment, influencing individuals and groups and inducing them to carry out "spontaneous" acts of terrorism. The way the Islamic State uses the Internet in general and social media in particular to shape reality and promote its terrorist objectives differs fundamentally from the ways in which terrorist organizations used technology in the past. Other non-state actors and terrorist organizations are learning to use media and technology, imitating the successful model of the Islamic State.

Keywords: cyber, social networks, terrorism, public perception, al-Qaeda, cyberspace, the Islamic State, Internet

Introduction

The evolution of contemporary terrorism in the form of the Islamic State correlates with the rapid changes that society is undergoing and effectively compresses space and time.[1] The Islamic State functions in three spheres: a geographical and physical space, cyberspace, and in the conscious realm, and applies its capabilities in all three spheres to shape its public image. This is manifested by the use of Salafist ideology, the seizure of territory, and the establishment of the Islamic caliphate. In the geographic and physical space, a proto-state has been created in parts of Syria and Iraq,

Daniel Cohen is a research fellow at the Institute for National Security Studies (INSS).

and Islamic State satellites have been created in battlefields in Libya, Nigeria, Yemen, and Afghanistan. Furthermore, in this space, the Islamic State engages in military activity and terrorist attacks aimed at enemy targets in the different arenas and to promote their political agenda. In cyberspace, the Islamic State has constructed operational infrastructures that it uses systematically in order to promote its objectives. The conscious realm is located between the physical space and cyberspace. The Islamic State employs both physical and virtual actions, such as using historic and religious symbols and markers of sovereignty; erasing other religions and ideologies; and demonstrating extreme, overt brutality in order to shape the public's perception of the Islamic State within the conscious realm. To use a technological metaphor, cyberspace and the physical spaces are the hardware of the Islamic State, while the conscious realm is the software it uses to manipulate the processing of information and symbols.

This essay focuses on how the Islamic State and other non-state actors use media and technology to affect individuals and groups through a combination of online and offline reality, inside and outside the world of the Internet.[2] This essay posits that the Islamic State's use of technology and media to shape its public image and to promote its terrorist objectives differs fundamentally from the ways in which the Internet has been used in the past by other terrorist organizations.

The Islamic State appeals to a wide range of individuals from Muslim communities throughout the world, and presents them with a twisted version of reality by creating and disseminating its own content through campaigns in the media and social networks. Concurrently, the Islamic State is a magnet for recruitment in areas it controls. Non-state actors and terrorist organizations, such as al-Qaeda, Hamas, and Hezbollah, are learning from its various techniques and are seeking more effective tools in the virtual space. Similar to the business world, these players are also expanding their Internet and social media toolbox in ways to facilitate their activities. Their cyber activity supports their actions and terrorism in the real world.

The Internet and the Revolution of the Social Networks

The slow, decentralized mechanical world that came into being in the second industrial revolution included the industrialization of most human activity and the replacement of human and animal labor with machines. In recent years, this world has been replaced by a rapid, electromagnetic, simultaneously unified, and networked one that allows connections across physical and mental borders and blurs the distinction between the two. The appearance of the social media in 2005 heralded a new stage in the development of the Internet. Modern information technology, used by various protest movements throughout the world, has a decisively influential nature; it allows the rapid, transparent transfer of information and serves as a key tool in promoting and changing political and social processes. Even relatively small groups and those lacking a clear hierarchy manage to demonstrate flexibility and sophistication, and quickly reach the masses through the virtual sphere.

An examination of the processes that led to the wave of protests throughout the world in recent years – from the Arab Spring in the Middle East to civil protests on socioeconomic matters all over the globe – points to the decisive importance of the Internet and social media as tools that can change society.[3] Since the Arab Spring, the Internet and social media have facilitated progress and change at the organizational level, while technological accessibility has enabled the development of sites and applications, including the creation of password-protected areas, accessible to close circles of influence; the use of instant, mobile message-sharing applications; and more.[4] This power is now in the hands of billions of people at some level or another, and it has changed the rules of the game from the ground up.[5] Almost two billion people around the world surf the Internet and use social media, and this number is growing and can be expected to increase in the next several years.[6]

Humankind created cyberspace, thereby establishing a global communications network that has significantly reduced the physical dimensions of the human environment. This means that technological and cognitive changes have led to accelerated speeds of human motion and traffic in cyberspace by means of contemporary computer networks. When surfing the Internet, the user's neural responses (i.e., the reactions of nerve cells in the brain to stimuli) and Internet information reach the user's consciousness at the same time.[7] The Internet allows the user to be simultaneously "everywhere and nowhere."[8] The connection between the Internet and the smartphone makes all information and communications available to people at any given moment regardless of their physical environment.

The Influence of the Islamic State on Thought and Practice in Salafist Jihadist Organizations

The appeal of fundamentalist groups to the public at large usually takes place within the framework of invoking general moral principles, injected with a sense of discipline, authenticity, commitment, and security. By compromising these principles, Islamist movements have created new marginal groups who are not only using more radical forms of violence and have expanded the scope of their terrorism, but have also radicalized the dichotomy between Islam and the West.[9] Dr. Abdullah Azzam and his heir, Osama Bin Laden believed that holy war or jihad against the infidel must be steered onto a parallel – sometimes alternative – track of war against "infidel regimes" in the Muslim world. In their view, jihad must embrace the entire world, and it is necessary to attack those who have seized control of areas where Islam prevails (such as Chechnya, the Balkans, and Palestine). Moreover, it is essential to damage the economy of the West, which is the source of the resilience of the "infidel regimes" within the Muslim world. Abdullah Azzam's vision was captivating, especially for the youth who were the first and second generation born in Western Europe to Middle Eastern and North African immigrants, and who failed to overcome the class barrier of their immigrant parents and grandparents. To them, Azzam and Bin Laden's call was like dew falling on parched ground.[10]

The upheavals that shook the Middle East in 2011 and toppled some of the so-called infidel regimes led al-Qaeda to call upon the masses to continue the revolution until all corrupt regimes had been ousted.[11] The Arab Spring allowed al-Qaeda to change its priorities and focus on internal jihad in order to shape new regimes throughout the Middle East and the Maghreb along the Salafist model.[12] A rogue faction of al-Qaeda initially formed in Iraq was quick to act; calling itself the Islamic State of Iraq and al-Sham (ISIS), it exploited the weakness of the sovereign state in Iraq and the collapse of Syria. Jabhat al-Nusra, the Syrian organization identified with al-Qaeda, and Ayman al-Zawahiri, Osama Bin Laden's heir as the leader of al-Qaeda, repudiated this move, thereby creating a rift between ISIS and al-Qaeda. In March 2014, ISIS launched a campaign on Twitter, calling to name the leader of ISIS, Abu Bakr al-Baghdadi as caliph.[13] ISIS's media managers used this campaign to examine how the Salafist jihadist community active on social media perceived the declaration. By the end of June 2014, ISIS spokesman al-Adnani announced Abu Bakr al-Baghdadi as the caliph of the newly established Islamic State in the Iraqi and Syrian territories that the organization had conquered (the words "Iraq and al-Sham" were dropped from the organization's name).[14]

By the second half of 2014, the Islamic State had already spread over vast territories in northeast Syria and northwest Iraq; elicited oaths of allegiance from different Salafist jihadist organizations in Africa, Asia, and the Middle East; and established sleeper cells throughout the Muslim world, including within Muslim communities in the West. The Islamic State uniquely combines Salafist ideology with pragmatic practice, which serves the establishment of a sharia-based state, according to the ideal model of early Islam and the first four caliphs. The organization's practical approach to the establishment of an Islamic state sets it apart from al-Qaeda, its parent body; while al-Qaeda envisions the establishment of a world-encompassing Islamic state at some future date, by contrast, the Islamic State's existence is here and now. The Islamic State managed to realize the long-term goal that al-Qaeda and other proponents of the radical Salafist ideology failed to achieve – of imposing a sharia-based, Islamic regime by establishing facts on the ground and creating mechanisms of sovereignty. The Islamic State's informed use of cyberspace allows it to be omnipresent. It has created a sense of identification and emotional meaning among its supporters and has succeeded in recruiting many young people from all over the world to the battlefields in Syria and Iraq.

The Islamic State's Use of the Internet and its Influence on the Physical Sphere

Since the mid-1960s, the Middle East has seen a steady return to Islam. This trend has been nurtured by many processes and circumstances reflecting the weaknesses of the prevalent secular, nationalistic, and/or socialist ideologies and their inability to meet the challenges of the social and political realities in the Arab countries. Consequently, a supra-state Islamic identity started to take precedence within civil society, especially through its on-the-ground presence in mosques, charities, and community centers, while the state-based framework continued to be the basis of the Muslim and Arab countries, using a wealth of tools, such as education and the media, to shape its citizens.

Salafist movements, led by the Muslim Brotherhood, emphasized preaching and social activity from within the ruling system, cooperated with the rulers and official authorities, and seemingly recognized the necessity of the state's existence as part of the essential process of change.

Salafist jihadism developed out of the ideological foundations of the Salafist movements, but expressed a much more radical ideology,[15] marked by pronounced activism, including violence and militant jihad. As a result, organizations identified with Salafist jihadism were persecuted by state security services and forced underground, while taking care to cover any tracks, including electronic ones, which might lead back to them. Most communication was relayed by computer, in secure jihadist forums using anonymous encrypted communications networks. Al-Qaeda activists, for example, used encrypted chat rooms, including video game chats, as well as single-use SIM cards and satellite phones, to communicate and recruit new members.[16] Osama Bin Laden himself relied upon messengers to transmit information, making it difficult for many years for the US intelligence to locate him.[17]

Peter Singer has claimed that just as the Crimean War was the first telegraph war, and the Vietnam War was the first television war, the current wars – such as those fought in Syria and Iraq – are the first media technology wars. According to Singer, the growth in social media activity by jihadist organizations directly correlates to the increase in the use of cyberspace by the public at large.[18]

In the past, terrorists exploited the inherent advantages of cyberspace to transmit encrypted messages, recruit supporters, acquire targets, gather intelligence, camouflage activity, and so forth. In the networked era, a terrorist organization that seeks to recruit supporters and expand its presence needs to develop capabilities that will allow it to be flexible and change rapidly, and be able to adapt its message to focused target groups or the broader public. Islamic State activists realize that the social media and the various applications for transmitting instant messages are crucial tools for communicating between members and supporters as well as between different devices. Its communications strategy consists mainly of visible Internet activity designed to turn the Islamic caliphate into a focus of attraction and identification for Muslims all over the world. The Islamic State uses the Internet for several purposes, enabling members to communicate with each other while also serving as a platform for disseminating propaganda, engaging in psychological warfare, and recruiting new members. Moreover, through the Internet, the Islamic State is able to influence individuals as well as groups and induce them to carry out terrorist acts. These capabilities provide flexibility and speed, involve only a low signature, serve as a force multiplier, enhance public perception, and make it possible for the Islamic State to be seemingly everywhere when, in fact, they are not.[19] Most importantly, the Islamic State's campaigns to shape public perception and disseminate propaganda through cyberspace quickly branded the Islamic State as the spearhead of global jihad.

An internal document of the US State Department, leaked to the *New York Times* in June 2015, revealed the many challenges the American administration faces in trying to battle the Islamic State in cyberspace.[20] State Department sources estimate that the nations fighting the Islamic State are not doing enough to foil the continued distribution of the organization's messages via the Internet. The document points to the lack of cohesiveness of the counter messages, the dearth of cooperation between the nations, and the slow and complicated pace of the battle. In contrast, the Islamic State is efficient and has a much faster response time in cyberspace than that of technological powerhouses such as the United States, the United Kingdom, and their allies, while it also preserves the cohesiveness of its messages with relative ease.

Aaron Zelin's study indicates that the Islamic State operates more than thirty media centers active in twenty-four provinces under its control.[21] On average, the media centers issue daily at least eighteen messages, including photos, videos, banners, news reports, radio broadcasts, and speeches, in mostly Arabic, followed by English, Russian, Kurdish, French, and Urdu.[22] Most of the media materials issued by the Islamic State in 2013 were produced and distributed by one communications center, al-Furqan Media, with the process having become more decentralized since then. Currently there are five media centers working under the Islamic State's propaganda and communications division, while the rest are provincial centers.[23] After preparing the materials, they are distributed via social media, jihadist forums, blogs and microblogs, video-sharing sites, and content-sharing sites.

In 2014, Twitter was one of the main tools for distributing the organization's materials. According to J.M. Berger and Jonathon Morgan, during the peak activity of the Islamic State on social media in the latter half of 2014, the number of Twitter accounts associated with its supporters reached an impressive 46,000. An inner circle of some 500-2,000 accounts belonged to heavy users, who operated in a coordinated fashion to maximize the organization's exposure and transmit its daily messages.[24] Instant message applications, such as WhatsApp and Snapchat, are other popular distribution tools, enabling users to upload and distribute photos and banners. One of the advantages that the propaganda division of the Islamic State has in working in a decentralized yet synchronized fashion is the use of different Internet platforms as surrogates; maximizing the resources of one social network until the organization's accounts are closed or blocked compels the supporters to find a new social network and repeat the process.[25] Thus, Islamic State supporters have switched from Twitter to KIK and VK, then to Telegram and so on.[26]

All of the Islamic State's distribution methods over social media are supported by traditional news channels that continuously cover the Islamic State and inadvertently disseminate its messages. In most cases, journalists and news editors do not have any access to firsthand information about the situation in the Islamic State-controlled areas, and are forced to make do with messages fed to them by the organization's central and provincial media centers. Even on the rare occasions that they are allowed inside the territories it controls, there is tight supervision of the content, making it impossible for journalists to provide any objective coverage.

The Islamic State operates an internal thought police to suppress and foil attempts by human rights activists and others to disseminate information via the Internet or smuggle out photos, videos, and testimonies of residents depicting reality under the Islamic State.[27] Furthermore, the Islamic State monitors Wi-Fi use in the territories under its control and bans the use of private wireless networks.[28] The Islamic State's messages are presented in black and white terms, good versus evil, and the West versus Islam. In the Islamic State's execution videos, for example, victims are displayed as weak and despicable, and are forced to kneel as if they were guilty for having brought death on themselves, while the executioners are visually portrayed as larger than life. By controlling the flow of information in areas under its control, the Islamic State is able to successfully mold public perception, as it determines the way it is exposed to the rest of the world.

In the past, most communication between members of jihadist terrorist organizations as well as with potential recruits took place by computer, using secure means. Now, the Islamic State and other non-state entities heavily rely upon open communications to recruit followers, distribute propaganda, carry out psychological warfare, and achieve other goals. The Islamic State is able to operate in cyberspace to achieve many different ends, the main ones being:

a. *Encouraging radicalization*: Key messages are transmitted via magazines,[29] videos,[30] posters, and religious chants (*anasheed*).[31] In the areas controlled by the Islamic State, videos made by its propaganda division are screened publicly. The Islamic State has also set up media desks in some major cities where it distributes booklets, discs, and flash drives with content designed to influence children and teens.[32] This aim is supported by activities in mosques and community centers.

b. *Recruitment:* The Internet serves as a magnet for recruiting young Muslims all over the world. The recruitment tactic of the Islamic State consists of projecting a unified, coherent, and simplistic message, which calls on young people to move to the Islamic State or engage in jihad in their countries of origin.[33] Chat platforms provide recruiters with access to many young people attracted to the Islamic State's narrative, and also enable one-on-one recruitments.[34] Islamic State recruiters also respond to people expressing curiosity in public forums and in a Q&A format. The Islamic State is a role model and inspiration for many young Muslims. From June 2014, when the establishment of the Islamic State was declared until March 2015, the number of foreign fighters coming to Syria and Iraq increased by 70 percent, while the pull of the Islamic State is felt in more than half of the world's nations.[35]

c. *Communications among members:* Encrypted software allows Islamic State members to communicate on the Internet securely and anonymously.

d. *Psychological warfare:* The Islamic State employs psychological warfare against the residents living in areas under its control in order to suppress dissent, deter subversive activity, and foil internal espionage. The Islamic State also uses psychological warfare in the videos and publications (magazines, weeklies, banners, and the like) that it shares via social media, intended to lower the morale and fighting spirit of its enemies, and affect their performance on the kinetic battlefield.[36] The videos and publications are also designed to instill fear in the local and international public and deter decision makers in the nations battling the Islamic State.

e. *Intelligence gathering:* The Islamic State gathers intelligence on its opponents, in order to wage psychological warfare against them and deter them. Intelligence is gathered through social media and then distributed as "hit lists," as in the case of the list of American military personnel, which included names, physical addresses, and email addresses. The Islamic State also engages in cyberattacks against the media and other sites identified with its opponents, so that it can leverage the media coverage and turn the media spotlight to the "hit lists." This tactic is done to frighten those appearing on the lists and make them fearful about being a target of a terrorist attack.[37]

f. *Cyber terrorism:* The Islamic State engages in cyber terrorism against sites identified with the opposing governments and against selected communications channels as a means of maximizing its media exposure with a relatively low signature.[38] The Islamic State thus far has only carried out relatively simple cyber terrorist attacks, such as site destruction and denial-of-service attacks.

g. *Use of organized terrorism:* The Internet enables relatively secure communications in order to create terrorist cells and communicate among activists who have left the Islamic State and have returned to their countries of origin. In the series of attacks in Paris in November 2015, the terrorists also used cell phones apps to communicate with one another.[39]

h. *Inducing spontaneous, non-organized terrorist attacks:* Terrorist attacks carried out by "lone wolves" are deeply embedded in Salafist organizations. Salafists perceive the violent struggle against the "enemies of Islam" as a personal obligation both within their countries of origin and elsewhere.[40] Terrorist attacks in the United States, Canada, Australia, Denmark, Kuwait, Tunisia, and France in 2014-2015, which were carried out by Islamic State admirers, reflect the organization's ability to induce individuals and small groups through social media to carry out lone wolf attacks. The common denominator of these perpetrators is that they all surfed the social media where they were influenced by the organization's messages; indeed, most of these attacks have taken place since the Islamic State called upon Muslims to carry out terrorist attacks against the security forces and citizens of Western nations.[41] In a number of cases in which the perpetrators did not accept responsibility in the name of the Islamic State, the Islamic State's influence in motivating the perpetrator to commit the crime is discernable.[42]

The strategy of the Islamic State's media and cyber branches is the same as that of commercial enterprises: it has assimilated the use of cyberspace into its various communications platforms in order to improve its performance in the physical realm. The organization encourages radicalization in mosques and Muslim community centers in tandem with its activity in social media where it disseminates messages designed to create deterrence and wage psychological warfare. Mass recruitment campaigns, such as the one called "One Billion Muslims Support the Islamic State,"[43] reflected the Islamic

State's decision to take overt, focused action via social media in order to attract new recruits while at the same time establishing an infrastructure of recruiters who operate on the ground and help potential recruits access information, resources, and instructions.

The Islamic State has succeeded in controlling the battle over its image by shaping its own experience so that the world sees events in Syria and Iraq through the eyes of the Islamic State, and by not permitting other mechanisms that allow a more objective perspective of reality. As a result, the Islamic State has created a conscious gap between the narrow conceptual meaning of the visuals presented by the Islamic State and the interpretation of "what one sees," which requires broader cognitive processes.

Network-Based Changes within Terrorist Organizations

Terrorist organizations that have pledged their allegiance to the Islamic State, such as Boko Haram in Nigeria and Ansar Bayt al-Maqdis in the Sinai Peninsula, have also started applying various methods of communications, including the production and distribution of videos similar to the Islamic State's execution videos.[44] Other terrorist organizations have studied the Islamic State's methods and have released videos, magazines, and messages as part of their campaigns to shape public perception, disseminate propaganda, and engage in psychological warfare.[45] Hezbollah, for example, has built a communications network specifically for the battle over its perception. It includes more than twenty websites in seven languages delivering news and specialized content. Hezbollah also uses foreign social media and YouTube, but less so than the Islamic State.[46] Hezbollah also restricts media coverage in the areas under its control and persecutes human rights activists and the opposition, who try to provide a more objective picture of reality.

Terrorist organizations identified with al-Qaeda have exploited the wealth of possibilities offered by social media and have increased their Internet presence. For the past several years, al-Qaeda has published online magazines in English, such as *Inspire* (since 2010), to spread propaganda, recruit and instruct supporters, and provide study materials to those interested in joining the organization's ranks.[47] Overall, al-Qaeda is very active on the Internet, and its contents are distributed through sharing sites as well as closed forums.[48] Osama Bin Laden, the organization's founder, was part of the first generation to develop modern jihadist propaganda. Videotapes of his speeches were distributed to new followers, increasing

Bin Laden and al-Qaeda's exposure. The marketing of the organization's powerful image grew increasingly sophisticated when, in addition to the activity of a-Sahab – the organization's production company – members and supporters disseminated and screened propaganda CDs on hundreds of websites.[49] The most prominent figure in the second generation of al-Qaeda was Anwar al-Awlaki who addressed the West in English on YouTube, his personal blog, and his Facebook page.[50] Jabhat al-Nusra, the Syrian branch of al-Qaeda, distributes video clips and engages in other activity on social media, as do the more "moderate" Syrian rebel groups, such as Jish al-Islam (the Islamic Army), which also circulated online an execution video of Islamic State members.[51]

The Islamic State also serves as inspiration for Palestinian terrorist organizations, which are learning to create maximal exposure via the Internet and social media in order to transmit messages and recruit activists and supporters. Palestinian terrorist organizations have even started their own Internet incitement campaigns designed to induce non-organized terrorists (the so-called spontaneous, lone wolf attacks) to act. Hamas and the Palestinian Islamic Jihad both have run social media campaigns, which included videos and photos calling upon Palestinians to stab Jews, especially soldiers.[52] Hamas also controls and monitors the media materials issued in its name in order to maintain its image as leading the struggle against Israel. For example, in January 2015, there was a stabbing on bus number 40 in Tel Aviv. In his interrogation, the terrorist claimed that he embarked on the attack out of frustration with the events in Gaza during Operation Protective Edge and other violent events to which he had been exposed in the Palestinian media and specifically after watching Hamas-produced, Islamic content, replete with praise for those who carried out terrorist acts and thus "reach the Garden of Eden."[53]

Two Palestinian media campaigns, named *Ad'as* ("running over" in Arabic and a pun on "Da'ish," the Arabic acronym for ISIS) and *At'an* ("stabbing" in Arabic), appeared in November and December, 2014. Created by individual Palestinians not affiliated with any organization, the symbol of the *At'an* campaign was a threatening picture of Palestinian youths wielding axes. The two campaigns created psychological terror and undermined the Israeli public's sense of safety, while they invested minimal effort and did not require organizing activists or building an intelligence infrastructure in order to carry out attacks.[54]

Compared to other terrorist organizations, the Islamic State has the most advanced technological and communications capabilities. It has established a well-organized infrastructure for employing social media: it develops applications, posts various instructional materials on JustPaste; distributes audio messages on SoundCloud; shares photos on Instagram and Snapchat; distributes videos on WhatsApp; and uploads *anasheeds* on YouTube. Despite efforts of various countries, media conglomerates, and Internet companies to fight the phenomenon, the Islamic State uses technological tools to bypass restrictions and has remained relevant over time in the media and social media. In that sense, it is light-years ahead of the other terrorist organizations, which have yet to learn to market and distribute materials virally and still lack the resources possessed by the Islamic State.

It can be assumed that the Islamic State segments and focuses its social media presence, using tools for campaign management, constant optimization, and follow-up of performance. Others are inadvertently involved in these cyberspace campaigns and serve as important tools in promoting them. These include social media companies, such as Facebook, and search engine companies, such as Google. These companies examine users' keystrokes and build enormous databases to analyze users' behavior on the Internet. Clients thus become profit-yielding data. All of this takes place through information exchanges with businesses interested in consumer behavior of every kind, including opinions, desires, and ambitions. This information can serve to improve the viral distribution of the Islamic State's campaigns by enabling consumers to choose their preferred content, including videos, songs, content pages, and more, all which are linked to the Islamic State.

Conclusion

The Internet in general and social media in particular have become the most influential factor affecting the behavior of human society in this era. Life online and offline have become part of a seamless fabric. Given that the barriers between the physical and cyber worlds are crumbling, the combination of Internet content and emotions can affect consciousness. Similarly, the activity of terrorist organizations in cyberspace influences terrorist acts in the physical world. In the Internet era, a terrorist organization that wants to achieve political goals and recruit supporters needs to develop capabilities that will allow flexibility and immediate change while adapting its messages to a focused or broad audience.

The Islamic State operates in a geographical and physical space, in cyberspace, and in the conscious realm. It has identified social media as a critical resource that is useful for communication among members, but also as a foundation for its propaganda, psychological warfare, and mobilization of new recruits. The organization also exploits the Internet to influence and induce individuals and groups to carry out terrorist acts. Other terrorist organizations are learning from this successful model and are striving to achieve similar capabilities. As various nations invest more resources to close their borders to Islamic State recruits and block their physical mobilization, the Islamic State likely will redouble its efforts in cyberspace – which is borderless – to recruit hackers and construct strategic cyberattacks in their nations of origin. Greater efforts of intelligence agencies to monitor and identify online activity by Islamic State activists will likely transform the Islamic State's online presence from overt to covert. This would involve a more massive use of dual-purpose commercial encryption technologies and Darknet/TOR networks.

The most significant challenges facing the espionage and intelligence communities are the formulation of new tools for eliciting information, monitoring, and enforcing the use of social media; foiling incitement that leads to terrorism; and engaging in proactive efforts to thwart potential attacks. It is therefore important to conduct a proactive battle, using technological tools, to identify those with the potential to carry out terrorist acts and be on the offense against online incitement. Many nations lack clear directives on how they can act against online terrorist activity, and significant judicial and enforcement mechanisms still need to be implemented, including the formulation of legislation and enforcement codes against online radicalization and incitement. The first stage in formulating policy necessitates establishing the link between online incitement and physical acts, with online incitement being the engine that drives terrorist attacks perpetrated by people who are not necessarily members of any terrorist organization.

The Islamic State has constructed a narrative that draws public and media attention away from the territories under its control. The Islamic State diverts media and public attention away from its oppression of the population, executions, economic woes, starvation, losses on the battlefield, and the like. In order to reduce the Islamic State's global influence and presence, it is critical to find the mechanisms and tools to “decompress” time and space and restore the public perception of the organization to its natural dimension, while forcing the Islamic State to operate in constrained spheres where it will be able to target only very limited audiences, thus causing its influence to wane.

The Islamic State is a global phenomenon and therefore a global threat. As a response, we must broaden our thinking and realize that this is not only a challenge at the intelligence and military levels, but also a multidimensional social and cultural phenomenon that cannot be tackled alone by either cybernetic or kinetic means. While some nations are already active in presenting a counter narrative to confront the Islamic State, this counter narrative is limited and focuses mostly on reducing Western recruitment to the Islamic State and the religious radicalization on the Internet. In the present reality in which the Islamic State determines the way it is perceived, it is imperative for the West to allocate resources to shape and alter this perception. The West needs to engage in a cybernetic battle, and engage in operational activity within the physical territory under Islamic State. This operation could include psychological and information warfare campaigns, but should also focus on training reliable locals opposed to the Islamic State. They would become agents of knowledge and use low-signature, anonymous technological means to gather intelligence, produce objective content, and high-level visual reports to disseminate in a focused manner to target audiences who are susceptible to the Islamic State’s influence.

The formulation of effective tools to fight the Islamic State could bolster the response to other non-state actors and terrorist organizations, which are inspired by the Islamic State, and have adopted similar techniques to further their terrorist activities. The coalition’s bombing campaign has hindered the successes of the Islamic State on the battlefields in Syria and Iraq and has wiped out many of its activists, but it has failed to diminish its overall number of activists because the steady stream of new recruits fills the emptied ranks. To reduce the number of volunteers entering the areas controlled by the Islamic State, it is not enough to close physical borders, which so far has yielded unimpressive results; rather, it is imperative to weaken the motivation of potential recruits in turning to jihad. In order to diminish the Islamic State’s image, it is essential to undermine its narrative and the perverted utopia it presents. To do so, we must wage a proactive cyberwar that incorporates a battle over the regnant narrative.

Notes

[1] For more on the concept of the space-time compression, see David Harvey, *The Condition of Postmodernity* (Cambridge and Oxford; Blackwell, 1989); Avi Rosen, "Compressing Space and Time in Cyberspace Art" (PhD diss., Tel Aviv University, 2009), http://www.sipl.technion.ac.il/~avi/tsc/avi_rosen_TSC.pdf.

[2] The "online-offline" concept in business relates to the combined strategy of marketing and branding both in cyberspace and in the real world. The objective is to create unity in the different spheres, thereby attaining maximal exposure within a defined target audience.

[3] Mahmoud Salem, "You Can't Stop the Signal," *World Policy Journal* (Fall 2014), http://www.worldpolicy.org/journal/fall2014/you-can't-stop-the-signal.

[4] Daniel Cohen and Ran Levi, "The Virtual Umbrella Protest," *Shorty* (blog), Institute for National Security Studies, February 26, 2015, http://heb.inss.org.il/index.aspx?id=5193&Blogid=8860.

[5] Asher Idan, "The Masses Rise," *Odyssey* 16 (July 2012), http://odyssey.org.il/224643.

[6] "Number of Social Network Users Worldwide from 2010 to 2018 (in Billions)," *Statista*, http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

[7] Rosen, "Compressing Space and Time in Cyberspace," p. 16.

[8] Roy Ascott, "From Appearance to Apparition: Communications and Consciousness in the Cybersphere," in *FISEA*, ed. Roman Verostko (Minneapolis: Minneapolis College of Art and Design, 1993), pp. 1-8.

[9] Daniel Cohen, "Between a Religious Islamic State and a Secular National State" (MA thesis, Tel Aviv University, 2012), p. 43.

[10] Emmanuel Sivan, "Clash Within Islam," in *The Battle of the Twenty-First Century: Democracy Fighting Terror*, ed. Haim Fass (Jerusalem: Israel Democracy Institute, 2006), pp. 48-51.

[11] "Al-Qaeda leader to Syrian protesters: Attack Israel," *Walla*, July 28, 2011, http://news.walla.co.il/item/1845055.

[12] Yoram Schweitzer and Aviv Oreg, "Al-Qaeda's Odyssey to the Global Jihad," *Memorandum*, no. 132, Institute for National Security Studies (January 2014): 47, http://www.inss.org.il/uploadImages/systemFiles/memo132f.pdf.

[13] Jessica Stern and J.M. Berger, *ISIS: The State of Terror* (New York: Harper Collins, 2015), p. 157.

[14] English translation of inaugural address given by the Islamic State's leader at https://ia902501.us.archive.org/2/items/hym3_22aw/english.pdf.

[15] Schweitzer and Oreg, *Al-Qaeda's Odyssey to the Global Jihad*, p. 18.

[16] Frank Gardner, "How Do Terrorists Communicate?" *BBC*, November 2, 2013, http://www.bbc.com/news/world-24784756.

[17] Ibid.

18 Mustapha Ajbaili, "How ISIS Conquered Social Media," *Al Arabiya,* June 24, 2014, http://english.alarabiya.net/en/media/digital/2014/06/24/How-has-ISIS-conquered-social-media-.html.

19 Celeste Olalquiaga, *Megalopolis: Contemporary Cultural Sensibilities* (Minneapolis: University of Minnesota Press, 1992), p. 6.

20 Mark Mazzeti and Michael Gordon, "ISIS Is Winning the Social Media War, U.S. Concludes," *New York Times*, June 12, 2015, http://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-us-concludes.html?_r=0.

21 Aaron Y. Zelin, "Picture or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output," *Perspectives on Terrorism* 9, no. 4 (August 2015): 87, https://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20150807-Perspectives.pdf. According to this study, the Islamic State claims to control thirty-three provinces: ten in Iraq, seven in Syria, two on the Syrian-Iraqi border, five in Yemen, three in Libya, two in Saudi Arabia, one each in Algeria, Egypt, Nigeria, and on the Afghani-Pakistani border.

22 Ibid., p. 88.

23 Ibid.

24 J.M. Berger and Jonathon Morgan, "The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter," *Analysis Paper*, no. 20, March 2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

25 Pamela Engel, "ISIS Has Figured out Ways to Get around Restrictions on One of the Main Apps it Uses for Propaganda," *Business Insider*, November 24, 2015, http://www.businessinsider.com/isis-telegram-channels-2015-11.

26 Kik: http://www.kik.com; VK: https://vk.com; and Telegram: https://telegram.org.

27 "ISIS Publically Executes Iraqi Human Rights Activist for Facebook Posts Condemning Terrorists' Destruction: UN," *New York Daily News*, September 25, 2014, http://www.nydailynews.com/news/world/isis-publically-executes-human-rights-activist-article-1.1952281.

28 Pamela Engel, "How ISIS Monitors and Restricts Internet Access in the 'Caliphate,'" *Business Insider,* November 7, 2015, http://www.businessinsider.com/how-isis-governs-its-caliphate-2015-11.

29 Aaron Y. Zelin, "al-Hāyat Media Center Presents a New Issue of the Islamic State's Magazine: 'Dābiq #10,'" *Jihadology*, July 13, 2015, http://jihadology.net/category/dabiq-magazine/.

30 "Videos: How ISIS Recruits around the World," *New York Times*, August 21, 2015, http://www.nytimes.com/interactive/2015/08/21/world/videos-isis-recruits.html?_r=0.

31 M. Shemesh, "Songs of the Islamic Nation: A Tool for Promoting the Caliphate," *MEMRI*, August 13, 2015, http://www.memri.org.il/cgi-webaxy/

sal/sal.pl?lang=he&ID=875141_memri&act=show&dbid=articles&data id=3941.

32 Zelin, "Picture or It Didn't Happen," p. 86.

33 "Canadian ISIS Fighter to Muslims in Canada: You Have a Religious Duty to either Emigrate to the Islamic State, or else Carry Out Attacks in Canada," *MEMRI*, December 8, 2014, http://www.memrijttm.org/canadian-isis-fighter-to-muslims-in-canada-you-have-a-religious-duty-to-either-emigrate-to-the-islamic-state-or-else-carry-out-attacks-in-canada.html.

34 Rukmini Callimachi, "ISIS and the Lonely Young American," *New York Times*, June 27, 2015, http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html.

35 United Nations Security Council, "Analysis and Recommendations with regard to the Global Threat from Foreign Terrorist Fighters," May 19, 2015, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2015/358.

36 Jillian Kay Melchior, "ISIS Tactics Illustrate Social Media's New Place in Modern War," *techCrunch*, October 15, 2014, http://techcrunch.com/2014/10/15/isis-tactics-illustrate-social-medias-new-place-in-modern-war/.

37 Dugald McConnell and Brian Todd, "Purported ISIS militants Post List of 1,400 U.S. 'Targets,'" *CNN*, August 14, 2015, http://edition.cnn.com/2015/08/13/world/isis-militants-american-targets/.

38 Josh Constine, "ISIS 'Cyber Caliphate' Hacks U.S. Military Command Accounts," *techCrunch*, January 12, 2015, http://techcrunch.com/2015/01/12/cyber-caliphate/.

39 "On est Parti on Commence": le SMS Trouvé dans le Téléphone Portable d'un Membre du Commando," *Le Monde,* November 18, 2015, http://www.lemonde.fr/attaques-a-paris/article/2015/11/18/le-telephone-portable-d-un-membre-du-commando-trouve-pres-du-bataclan-a-permis-de-remonter-a-alfortville_4812515_4809495.html.

40 One can learn much about this method and its advantages from an essay penned by Abu Masab al-Suri, one of the most influential figures on the operational methods of al-Qaeda and other global jihad organizations. See https://archive.org/stream/TheGlobalIslamicResistanceCall/The_Global_Islamic_Resistance_Call_-chapter_8_sections_5_to_7_LIST_OF_TARGETS#page/n0/mode/2up.

41 John Hudson, "FBI Director: For Would-Be Terrorists, Twitter is the 'Devil on their Shoulder,'" *Foreign Policy*, July 8, 2015, http://foreignpolicy.com/2015/07/08/fbi-director-for-would-be-terrorists-twitter-is-the-devil-on-their-shoulder/?utm_source=Sailthru&utm_medium=email&utm_term=*Editors%20Picks&utm_campaign=New%20Campaign.

42 "Denmark: Fifteen-year-old Watched an ISIS Incitement Program and Killed her Mother," *Ynet*, September 16, 2015, http://www.ynet.co.il/articles/0,7340,L-4700789,00.html.

[43] This campaign was started by an ISIS supporter on June 19, 2014, using different media shortly after the conquest of the strategic city of Mosul in Iraq and a few days before the declaration of the establishment of the Islamic caliphate. The campaign, which was featured against the backdrop of photographs of various sites, was successful and attracted support from all over the world. See Henri Tartaglia, "German ISIS Supporters Started a Jihadist Social Media Campaign," *VICE News*, June 20, 2014, http://www.vice.com/read/german-jihadi-internet-meme-campaign.

[44] Jay Akbar, "Like Master, like Servant: Nigerian Terror Group Boko Haram Releases First Beheading Video since Pledging Allegiance to ISIS," *Daily Mail*, July 10, 2015, http://www.dailymail.co.uk/news/article-3156551/Like-master-like-servant-Nigerian-terror-group-Boko-Haram-releases-beheading-video-pledging-allegiance-ISIS.html#ixzz3kaEa4HBS.

[45] See, for example, Hamas' video clip that is part of a propaganda and psychological warfare campaign in Yaron Schneider, "Hamas Presents New Documentation of Tunnel Fighters' Unit," *TV2*, August 27, 2015, http://www.mako.co.il/news-military/security-q3_2015/Article-ad8d86659ad6f41004.htm.

[46] "Terrorism and the Internet: The Website Infrastructure of Hezbollah and the Societies Supporting it," Meir Amit Intelligence and Terrorism Information Center, March 4, 2013, http://www.terrorism-info.org.il/he/article/20488.

[47] Elinor Fuchs, "Nails, Sewage Pipe and Pressure Cooker: Al-Qaeda Teaches how to Make Homemade Bombs," *Mako*, April 17, 2013, http://www.mako.co.il/nexter-internet/Article-c04fbab1a771e31006.htm.

[48] See, for example, distribution of videos about communications mechanisms identified with al-Qaeda in "New video by al-Shabab al-Mujahedeen: Documentation of the Attack on the Courthouse and Parliament in Mogadishu," *Online Jihad Exposed*, January 9, 2015, http://www.onlinejihadexposed.com/2015/01/blog-post_9.html.

[49] Schweitzer and Oreg, *Al-Qaeda's Odyssey to the Global Jihad*, p. 25.

[50] Scott Shane and Ben Hubbard, "ISIS Displaying a Deft Command of Varied Media," *New York Times*, August 30, 2014.

[51] "Syria: Jish al-Islam Executes 18 ISIS Members," *Arab Sensor*, July 1, 2015.

[52] Matan Hetzroni, "Why doesn't Nasrallah have Twitter?" *Mako*, January 1, 2015, http://www.mako.co.il/news-military/security-q1_2015/Article-a01a488571aaa41004.htm.

[53] Amir Bohbot and Avi Ashkenazi, "The Terrorist from Tel Aviv: I carried out the Attack because of Operation Protective Edge," *Walla*, January 21, 2015, http://news.walla.co.il/item/2821840.

[54] Udi Dekel, "Terrorism in the Jerusalem Synagogue: From National Struggle to Religious War?" *INSS Insight* no. 633 (November 25, 2014), http://www.inss.org.il/uploadImages/systemFiles/No.%20633%20-%20Udi%20for%20web.pdf.

What Should be the Role and Responsibility of the Government in Defending Private and Commercial Digital Intellectual Property?

Ron Shachar

The rapid development of cyberspace has led to a growing threat of criminally motivated cybertheft of intellectual property in general, and of commercial and private digital trade secrets in particular. This kind of cybercrime could have a critical impact on the international macro-economic system, including potential massive loss of tax revenue and drop in GDP. While most countries have strategic cyber defense doctrines to protect their physical critical infrastructures against politically motivated cyber warfare, they still lack suitable doctrines, legislation, and means of protecting digital intellectual property against criminally motivated cybercrimes. Furthermore, the outdated approach of consequential penalties against cybercrimes is irrelevant, as cyberspace makes it difficult to detect the intellectual property theft in real time. In this article, we will analyze whether the macro-economic implications of the growing cybertheft trends will help render the commercial and private digital intellectual property as critical infrastructure that should be proactively protected by governments against cybertheft.

Keywords: digital intellectual property, cybertheft, critical infrastructure, governmental responsibility, cybercrime, CNE, proactive protection, cyber defense doctrines, macro-economic implications

Ron Shachar is a private Cyber Strategic Consultant, who has served in the IDF as head of the Cyber-Defense Strategic Planning Section and as assistant to the Cyber-Defense Unit's Director.

Introduction

> From now on, our digital infrastructure – the networks and computers we depend on every day – will be treated as they should be: as a strategic national asset.[1]
>
> We are going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century.[2]
>
> President Barack Obama

Commercial and private digital intellectual property in general and trade secrets in particular currently are regarded as important components of the economies of modern countries. Concurrently, cyberspace is rapidly evolving to become a source of both great opportunities and threats through cyber warfare and cybercrime.[3] Some of the criminally motivated cyber threats are aimed directly at stealing commercial and private intellectual property, which could cause loss of massive tax revenue that diminish a country's economic income and GDP (Gross Domestic Product), and could have a severe impact on the international macro-economic systems.[4] While most countries have strategic cyber defense doctrines and statutes for protecting their physical critical infrastructures against politically motivated cyberattacks, they have ignored the need to protect digital intellectual property in cyberspace against criminally motivated campaigns.

The article examines why governments should treat commercial and private intellectual property in general and digital trade secrets in particular as national critical infrastructure, which deserve appropriate governmental proactive protection. We will ask whether the macro-economic implications might help to define the commercial and private digital intellectual property as critical infrastructures that should be protected against cybertheft. Although the scope here neither includes specific measures nor suggests that the governmental defense of private intellectual property should be equivalent to that of the physical critical infrastructure in cyberspace, a general framework for a better balance between the two is recommended.

Definition and Scope of Physical Critical Infrastructures

Cyberattacks are carried out through hacking, mostly from outside the network in order to retain some or full control over the network.[5] That control is used for two purposes: computer network attack (CNA) or computer network exploitation (CNE).[6] Cyberattacks also seek to undermine the computerized network for criminal, political or national security purposes.[7] Governmental agencies, competitive corporations or individuals all might have possible motivations to engage in cybertheft of digital intellectual property.

Governments have a responsibility of providing their people and national assets with protection and security.[8] The degree of fulfilling that responsibility, however, varies between countries in accordance with the particular regime. According to James A. Lewis and Katrina Timlin of the Center for Strategic and International Studies in Washington DC, as the Internet becomes a modern global infrastructure for international commercial businesses and governmental activity, security of cyberspace has become both a national and international concern.[9]

According to Dr. Kristin M. Lord and Travis Sharp, the number of cyberattacks with criminal and political motivations is growing rapidly. There are an estimated 1.8 billion attacks per month with various levels of sophistication solely targeting the US Congress and American federal agencies.[10] Eric Sterner of the American Department of Defense stipulates that the number of cyberattacks is far greater when one includes international attacks on foreign governments and private sectors.[11] Professor Eric Talbot Jensen estimates that thousands of companies around the world are currently under cyberattack, and their intellectual property, specifically their trade secrets, is being compromised.[12] In many cases, the private and commercial companies will be unaware of the attack unless the government and its agencies inform them of the attack.[13] By the time they know about the attack, it is already too late as the company's data and intellectual property have already been stolen.[14]

Of all the possible cyberattacks, the CNE type, which in the private sector manifests mostly as intellectual property theft, is the most troubling one. According to Martin C. Libicki, the CNE cyberattack is of great concern mainly because it focuses on stealing digital data and secrets while operating under the owner's radar and without being exposed, as these methods are difficult to detect.[15] Consequently, the intellectual property theft and

CNE attacks are the greatest threat to keeping and maintaining private and commercial intellectual property as secrets.

The rapid growth in cyberattacks in the international arena and their threat to global security and economic systems have evolved into ongoing cyber warfare and cybercrime, which include both trained military units motivated for political reasons and expert criminals propelled by criminal and commercial interests.[16] The increase in cyberattacks has caused governments from all around the world to establish designated agencies and cyber defense doctrines in order to deal with cyberspace threats. In the United States, the Cyber Command Agency is responsible for removing any politically motivated threats directed at military and critical cyber infrastructures, while other agencies, such as the FBI, deal with criminally motivated cyber threats.[17] This is a result of the growing reliance on networked information systems that control critical infrastructures and communications systems, which are essential to modern life.[18]

In most western countries, the evolving cyber responsibility of the government has focused on defending mainly national interests and infrastructure, while overlooking the need to defend private and commercial intellectual property. France[19] and Germany,[20] have highlighted the cyber threats against national critical infrastructure as a strategic factor prioritized within their defense doctrines. In the United Kingdom, the focus is mainly on governmental assets, activities, national organizations, and critical infrastructure such as the financial system.[21] In Israel, the police is responsible for cybercrime, even though the National Cyber Bureau in the Prime Minister's Office, which is responsible for protecting the state's critical infrastructure, has many more resources and government attention.[22]

Given the similar focus of the various countries, there is a broad consensus to prioritize the physical protection of national critical infrastructures in cyberspace. Some notorious cyberattacks of national critical infrastructures in recent years raised awareness of these sorts of attacks, and may have contributed to this consensus. Following the 2007 massive cyberattack on Estonia[23] and the 2010 Stuxnet attack on the Iranian nuclear program,[24] most countries have prioritized their cyber defense doctrines around the government's physical protection of critical infrastructures. According to Bruce Berkowitz, critical infrastructures and key assets are vital components; if they are cyberattacked, the country under attack will be brought to its knees.[25] As a result of the technological evolvement and the growing dependence of governmental and military processes on cyberspace, the definition of critical infrastructures has expanded. Information systems and digital intellectual property are so vital to governments, civilian society, and modern militaries that they could become the main targets in war.[26] Hence, the definition of "critical infrastructure" needs to be updated to include these digital core components.[27]

Cyber warfare and its direct threat to the stability and vitality of nations has led the international community to establish national cyber defense doctrines. These strategic doctrines have tackled the politically motivated threats through physical protection of critical infrastructures. These defense doctrines, however, are insufficient for criminally motivated intellectual property theft and CNE threats to private and commercial assets. This current situation raises the question whether the macro-economic implications of the increase in cybertheft should motivate governments to consider commercial and private digital intellectual property as part of the critical infrastructure that deserves to be protected proactively against criminally and politically motivated cybertheft.

Private and Commercial Digital Intellectual Property as National Critical Infrastructure

Even though definitions might differ between countries, three criteria must be met in order for intellectual property to legally qualify as a trade secret. First, the data must give a competitive advantage when kept as a secret. Second, it must actually be kept as a secret. The secrecy criterion is an absolute one, as long as the data and information cannot be taken or extracted easily from the published product. Third, the data must be protected by a reasonable secrecy defense mechanism,[28] (including cyber defense technologies) to keep away any intruders. Some courts recognize also a fourth criterion of liability, as they demand that the secret information be continuously used in the company's business.

As mentioned earlier, many companies do not know that their data has been stolen through cyberspace and when they do find out they are often reluctant to report the loss, as they fear the potential commercial damage to their reputation.[29] Cybertheft of commercial and private intellectual property might be politically motivated – known as economic espionage (state-driven)[30] – or criminally motivated to gain private or commercial market advantage, known as industrial espionage.[31] Regardless of the initial motivations or purposes, the potential macro-economic implications for the company are vast and destructive. Companies that have been robbed of their intellectual property use different methods to estimate their financial losses. Some companies base their estimations on the actual costs of developing the stolen secret data, while others project the loss of future gross income.[32]

In addition to the damages inflicted upon an individual company, the question arises whether the theft of individual trade secrets can have a macro-economic impact on the nation's resilience. The cybertheft of digital intellectual property damages the ability of the national financial sector to generate new revenues and jobs or develop and research new innovations,[33] causing loss of tax revenue that diminishes the country's economic income and GDP (Gross Domestic Product).[34] Consequently, a vast and large-scale cybertheft of commercial and private intellectual properties translates into serious macro-economic loss, estimated in the billions and reflected in a drop in the Gross National Product.[35] For example, an elaborate and orchestrated cybertheft of private and commercial digital trade secrets, regardless of the actual motive of the attack, might result in the sudden bankruptcy of a country as a result of a loss of massive tax revenue and income. Economic analysis, depending on the various calculation methods, estimates that the losses caused by cybertheft of trade secrets range from $2 billion to $400 billion or more per year in the United States alone.[36]

Thus, the initial motivation for the cybertheft, whether criminal or political, is insignificant when considering the cyber defense approaches as there is no connection between the purpose of the attack and the destructive macro-economic implications and the holistic preventive cyber defense solutions (technological and doctrinal). Either way, the economic impact of cybertheft on national resilience is a major one.

In the last century, the pace of innovation, and research and development (R&D) in the private and commercial sectors increased the growth of trade secrets and the number of patents issued in the United States by 40.6 percent, showcasing the powerful role of trade secrets in the global economy.[37] According to Technet, a US national coalition of CEOs in the high-tech sector, more than six million jobs and more than a third of the fifteen-trillion dollar US economy is based on innovation and consequently, on trade secrets and intellectual property.[38] General Keith Alexander, former director of the US National Security Agency and Cyber Command, has estimated the losses to the American GDP at about $250 billion a year as a result of cybertheft of trade secrets, calling it "the greatest transfer of wealth in history."[39] An example is the 2007 cybertheft of Lockheed-Martin's F-35 stealth fighter program, allegedly by a Chinese company, which had been working on a similar aircraft at the time (the J20).[40] Although this cybertheft was politically motivated, the economic impact is the same.

A good understanding of the macro-economic value of the trade secrets – and accordingly, the potential national loss of income – can be obtained by reviewing the private and commercial sector's investments in R&D. Although there are a lot of valuable and important trade secrets not related to R&D (for example, sales figures, client lists, marketing strategies, and so forth), R&D represents investment in cutting-edge technologies, ideas, and inventions, all critical components of many trade secrets.[41] R&D investments in the United States has surpassed 2.7 percent of the GDP, which stands at roughly $447 billion a year. Similarly, R&D investments are 2.9 percent in Germany, 2.0 percent in China, 1.8 percent in the United Kingdom, and 1.5 percent in Russia.[42] It is important to emphasize that any R&D investment generates other forms of new trade secrets (one dollar of R&D investment generates up to sixty-nine dollars over the following decade), and accordingly, the economic value of trade secrets is even greater than the R&D's figures.[43]

In a reality where the most valuable assets and infrastructures are digital, intangible, and easy to transfer over networks, cybertheft of intellectual property has taken on a new critical importance.[44] A 2001 report, representing fourteen US intelligence agencies, stated that cybertheft will become a "growing and persistent threat,"[45] as well as a concrete threat that the head of the US intelligence community ranks higher than terrorism.[46] According to a report issued by the Ponemon Institute, intellectual property theft in cyberspace has increased, with some companies experiencing more than seventy-two attacks per week.[47]

As intellectual property becomes more dominant and crucial in the modern economy, as evident from the above-mentioned statistics, its theft or damage will inflict enormous financial losses to the country that harbors it. National economies, therefore, are at tremendous economic risk should something happen to their commercial and private digital intellectual property. As stated in the US congressional report on industrial espionage, the theft of intellectual property from commercial and private companies undermines the private sector's ability to generate revenues, create new jobs, foster innovation, and lay the economic foundation for future growth and national security.[48] The growing importance of digital intellectual property to the modern economy, along with the potential destructive damage to a nation's economy if stolen, renders cybertheft of intellectual property as extremely dangerous to a country's economic resiliency.

Consequently, governments should apply the same concerns and engage in a proactive defensive approach regarding cyberattacks of critical infrastructure of their commercial and private intellectual property. The rise in cybertheft attacks targeting digital intellectual property, along with the potential massive macro-economic losses, places the private and commercial digital intellectual property within the consensual definition of national critical infrastructures that should be protected by the state.

As the protection of commercial and private intellectual property against cybertheft is critical to corporate profitability and growth,[49] it should automatically be regarded as having national importance, as these commercial intellectual properties affect the national economy through taxes, additional indirect incomes, and the national GDP altogether. Thus, any wide-scale cybertheft of commercial intellectual properties might damage the nation's economic resiliency and cause a vast chain reaction that might surpass any possible cyberattack of an individual critical infrastructure. Consequently, governments should take responsibility for protecting private and commercial intellectual property and adopt a more involved and proactive approach towards their defense. This raises a dilemma, however; even though the digital intellectual property has macro-economic importance to the national resiliency, it is also a privately-owned entity that does not belong to the government.

National Copyright Models

Having characterized the current problem and the failure of governments to take responsibility for providing cyber protection of commercial and private intellectual property, we shall define and recommend a solution based on existing national copyrights models. Although copyrights are a specific type of intellectual property, some of the components of their protection may be relevant in defining the optimal governmental responsibility for defending the commercial and private digital intellectual property in general and trade secrets in particular.

The Anglo-American model aims at ensuring the public's benefit and welfare by providing economic incentives for the copyright creators, which increase the creation of new products.[50] Respectively, the government's proactive protection of digital intellectual property will encourage commercial entities and private individuals to continue to create new trade secrets.

Although some would say that there is not any empirical evidence that protection of intellectual property will increase their creation,[51] this claim might be more accurate in regard to copyrights in the field of arts and science. The creation of trade secrets in its essence is closely related to economic incentives, as they serve as an important factor in a country's economic growth; a proactive governmental cyber defense of trades secrets will attract new inventors by granting them economic incentives. Hence, there is a strong connection between governmental cyber protection of intellectual property and the double gain of both preventing macro-economic damages on a national scale as caused by cybertheft of commercial intellectual properties, and of encouraging the growth of new commercial intellectual property. These two consequential gains reflect the Anglo-American model, which benefits the public by producing more inventions and by strengthening the nation's economic resilience.

Complementary to the Anglo-American's model, the French model of property rights solidifies the government's role in keeping the intellectual property in the hands of its creator. According to the French model, based on the *droits d'auteur*, the creation cannot be alienated from its creator who possesses the property rights over his work.[52] This aspect of the French model gives the government the responsibility of ensuring that digital intellectual property is protected as the assets of its creator, while preventing alienation from its owners. In other words, the French model ensures that governmental protection of commercial and private digital intellectual property does not lead to the nationalization of privately-owned intellectual property nor to excessive government intervention in the private sector. It helps balance the appropriate degree of governmental cyber defense of commercial and private intellectual property. It also helps to achieve a more resilient national economic status and limits any overbearing intrusion of government in the private sector.

To conclude, the approach of the Anglo-American model will help stimulate the government's responsibility for protecting private and commercial digital intellectual property, as its national macro-economic implications serve the public's benefit. Components of the French model will ensure that the governmental intrusion into the private sector does not revoke the ownership of the protected intellectual property from its owner. This legal synthesis creates a balanced governmental proactive responsibility, without crossing the thin line between the public and the private sectors. Having synthesized the recommended governmental cyber-defense responsibility, we shall examine how governments should execute that responsibility.

Governmental Proactive Role and Responsibility

Based on the above-mentioned principles and models, we will focus on two important components of the proposed governmental cyber responsibility to proactively protect commercial and private digital intellectual property. The first is the creation of dedicated cyber defense statutes, aimed at protecting commercial and private digital intellectual property of all sorts. Some countries have a unified comprehensive law and some use a set of laws in order to create full legal protection. For example, in the United States, two major trade secrets laws of a civil and criminal orientation have been legislated. First, the 1979 Uniform Trade Secrets Act (UTSA) provides an official definition and criteria for trade secrets, definition of their theft, and suitable consequential remedies (such as injunctive relief, economic compensation, attorney's fees, and so forth).[53] Second, since 1996, the Economic Espionage Act (EEA) has transformed the theft of trade secrets and economic espionage into federal crimes with the appropriate penalties.[54] Both statutes focus on the aftermath and consequential implications of theft of digital trade secrets, without proactively trying to prevent the act of cybertheft itself in real time. The legislation of statutes deters, to some degree, any potential cyber attackers and thieves, but alone is insufficient as a preventive countermeasure, since cyberspace provides the attackers with relative anonymity, including low risk of detection and difficulty in assigning any blame to the attackers.[55]

Hence, the second component is crafting a holistic cyber defense doctrine that strategically acknowledges the government's degree of responsibility and the consequential prioritization of protecting commercial and private digital intellectual property. These national cyber defense doctrines are not just declarative, but rather they embody national prioritization in terms of resource allocation (budgets, human resources, implementation of designated technological solutions, and so forth) aimed at protecting these vital digital assets. For example, in France, President François Hollande has issued a general national defense doctrine that addresses the threat of cybertheft. The French doctrine stresses the importance of protecting French scientific and technological assets, and preventing the theft of "French knowledge and know-how" of both public and private nature.[56] Another good example can be found in the United Kingdom's Cyber

Strategic Doctrine that stresses the importance of protecting the country's digital intellectual property, along with other national and military critical infrastructures.[57] In addition, the *Digital Britain Report* outlines the vision for digitalizing the United Kingdom, while emphasizing the importance of cyber defense as part of the national strategic vision.[58]

Even with these two suggested components – statutes and strategic doctrines aimed at prioritizing the protection of commercial and private digital intellectual property – it is still critical for the government to be proactive in order to prevent cybertheft. According to Professor Lawrence Lessig, the government's proactive responsibility for protecting commercial and private assets might be executed without the owner's consent or knowledge.[59] That sort of government activity means violating human rights and especially individual privacy. Furthermore, according to Glenn Greenwald, the growing government involvement in cyberspace will hurt the public's privacy while it will do very little to improve cybersecurity.[60]

The right solution should be a balanced one. The government should proactively protect commercial and private digital intellectual property, while limiting violations of private data and assets that are not classified as intellectual property. For example, governments could deploy cyber protection means throughout public/civil digital spaces such as by protecting public and common networks or national routers, rather than just protecting military networks from any hostile penetration. Hence, the optimal solution for protecting commercial and private intellectual property should be done through legislating the appropriate statutes and by establishing national strategic cyber defense doctrines, which together form the foundations for providing the government with the right tools and legitimacy to proactively defend crucial civil and private digital assets. In addition to governmental cyber protection, private and commercial companies should make efforts, using their own resources and investments, to prevent and detect any breaches inside their networks or any attempt of cybertheft.

Conclusion

> The new Economic Espionage Act will help us crack down on acts like software piracy and copyright infringement that cost American businesses billions of dollars in lost revenues, and it will advance our national security.[61]
>
> President Bill Clinton

A lot has changed since President Bill Clinton's words of hope of eliminating piracy and copyright infringement of trade secrets and other intellectual property. In the last twenty years, cyberspace has rapidly evolved and has given rise to strategic threats of cybertheft of commercial and private digital intellectual property. Simultaneously, commercial and private digital intellectual property in general and trade secrets in particular have become crucial and dominant factors in the contemporary economy.

The outdated approach of aftermath and consequential penalties is almost irrelevant nowadays, as cyberspace makes it difficult to detect cybertheft in real time and effectively assign its malicious motive to any individual, organization or country. Consequently, governments around the world should revise their own role and responsibility by assuming a proactive and preventive approach in their doctrines, legislation, and regulations. Governments should take some responsibility for protecting private and commercial digital intellectual property given their importance to the macro-economic systems, and their potential to cause massive economic fallout if stolen. Given the potential macro-economic losses, the significance of protecting the country's commercial and private intellectual properties through cyberspace should be seen as equivalent to the importance of protecting military and physical critical infrastructures. Using the Anglo-American model, government protection will expand economic incentives for creating new intellectual property. Furthermore, it will solidify the creator's individual right in keeping his developed intellectual property to himself, based on the French model.

Notes

[1] President Barack Obama, "Remarks on Securing Our Nation's Cyber Infrastructure," *Office of the Press Secretary*, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[2] President Barack Obama, "Remarks by the President at the Export-Import Bank's Annual Conference," *Office of the Press Secretary*, March 11, 2010, http://www.whitehouse.gov/the-press-office/remarks-president-export-import-banks-annual-conference.

[3] Cyberspace is a virtual medium consisting of an accumulation of networked computerized devices that are connected to the outside world (the Internet, for example). See Martin C. Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009).

[4] Pamela Passman, Sanjay Subramanian, and George Prokop, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets*

and Mitigate Potential Threats (Washington, DC: The Center for Responsible Enterprise and Trade, 2013), p. 8.

5 Libicki, *Cyber Deterrence and Cyberwar*.

6 CNA (Computer Network Attack) refers to attacking the network and its business processes by disrupting, denying or destroying the information stored in it. CNE (Computer Network Exploitation) refers to extracting the network by stealing its data. See US Department of Defense, *Dictionary of Military and Associated Terms* (Joint Education and Doctrine Division, 2014).

7 Oona A. Hathaway and Rebecca Crotoff, "The Law of Cyber-Attack," *California Law Review* 100, No. 4 (2012): 827.

8 Gareth Evans and Mohamed Shanoun, *The Responsibility to Protect: Report for the International Commission on Intervention and State Sovereignty* (Ottawa: International Development Research Centre, 2001), p.13.

9 James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, DC: Center for Strategic and International Studies, 2011), p. 3.

10 Kristin M. Lord and Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, DC: Center for a New American Security, 2011), p. 7.

11 Eric R. Sterner, "Deterrence in Cyberspace: Yes, No, Maybe?" In *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, ed. Robert Butterworth (Arlington, VA: George C. Marshall Institute, 2011), pp. 28-35.

12 Eric Talbot Jensen, "Cyber Warfare and Precautions Against the Effects of Attacks," *Texas Law Review* 88 (2010): 1536.

13 Kim Zetter, "Report Details Hacks Targeting Google, Others," *WIRED*, February 3, 2010, http://www.wired.com/threatlevel/2010/02/apt-hacks/.

14 Ibid.

15 Libicki, *Cyber Deterrence and Cyberwar*, p. 23.

16 Abraham R. Wagner, "Cybersecurity: From Experiment to Infrastructure," *Defense Dossier* 4 (2012): 17.

17 Lewis and Timlin, *Cybersecurity and Cyberwarfare,* p. 22.

18 The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011), p. 9.

19 Lewis and Timlin, *Cybersecurity and Cyberwarfare,* p. 11.

20 Federal Ministry of the Interior*, Cyber Security Strategy for Germany* (Berlin: Federal Minister of the Interior, 2011).

21 UK Office of Cyber Security and UK Cyber Security Operations Centre, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (London, 2009), p. 9.

22 Israel's Prime Minister's Office, *Advancing National Cyber Space Capabilities-Decision Number 3611* (August 7, 2011).

23 Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* 56 (2011): 569.

24 Thomas M. Chen, "Stuxnet, the Real Start of Cyber Warfare?" *IEEE Network* 24, no. 6 (2010): 3.

25 Bruce D. Berkowitz, "Warfare in the Information Age," In *In Athena's Camp: Preparing for Conflict in the Information Age*, eds. John Arquilla, and David Ronfeldt (Santa Monica: RAND National Security Research Division, 1997), p. 181.

26 Ibid., pp. 177, 181.

27 Myriam A. Dunn, "Securing the Information Age: The Challenges of complexity for Critical Infrastructure Protection and IR Theory," *International Relations and Security in the Digital Age* (ETH Zurich: Center for Security Studies, 2007), p. 11.

28 Robert G. Bone, "A New Look at Trade Secret Law: Doctrine in Search of Justification," *California Law Review* 86 (1998): 248-249.

29 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* (2011), http://www.ncix.gov/publications/reports/fecie_all/ Foreign_Economic_Collection_2011.pdf.

30 Ibid., p. 7.

31 Ibid., p. 8.

32 Ibid., p. 2.

33 Ibid., p. 3.

34 Passman, Subramanian, and Prokop, *Economic Impact of Trade Secret Theft,* p. 8.

35 Shahar Argaman and Gabi Siboni, "Commercial and Industrial Cyber Espionage in Israel," *Military and Strategic Affairs* 6 (2014): 51, http://media.wix.com/ugd/d48d94_a62f01468dc8448ebe635f8d962c410f.pdf.

36 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets,* p. 4.

37 Passman, Subramanian, and Prokop, *Economic Impact of Trade Secret Theft,* p. 7.

38 Dennis C. Blair and Jon M. Huntsman, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (n.p.: The National Bureau of Asian Research, 2013), p. 23.

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

40 *Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China: Hearing on the Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology, Before the Oversight and Investigations Subcommittee of the Foreign Affairs Committee of the U.S. House of Representatives* (2011) (statement of Richard D. Fisher, Jr., Senior Fellow, International Assessment and Strategy Center, p. 5).

41 Passman, Subramanian, and Prokop, *Economic Impact of Trade Secret Theft,* p. 8.

42 Ibid.

43 Ibid.

44 Blair and Huntsman, *The IP Commission Report,* p. 43.

45 Siobhan Gorman, "China Singled Out for Cyber Spying," *Wall Street Journal*, November 4, 2011, http://allthingsd.com/20111104/china-singled-out-for-cyberspying/.

46 Argaman and Siboni, "Commercial and Industrial Cyber Espionage in Israel," 54.

47 Ponemon Institute, *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies* (Ponemon Institute, 2011).

48 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets,* p. 3.

49 Ibid, p. A-2.

50 Neil Netanel, "Copyright Alienability Restrictions and the Enhancement of Author Autonomy: A Normative Evaluation," *Rutgers Law Journal* 24 (1993): 9.

51 Richard Watt, "An Empirical Analysis of the Economics of Copyright: How Valid are the Results of Studies in Developed Countries for Developing?" in *The Economics of Intellectual Property* (n.p.: WIPO, 2006), p. 68.

52 Netanel, "Copyright Alienability Restrictions," 15.

53 Uniform Trade Secrets Act §§ 1-12 (amended 1985).

54 The Economic Espionage Act, 18 U.S.C.§§ 1831−1839 (1996).

55 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets* p. 1.

56 President of the French Republic's Office, *French White Paper: Defense and National Security* (2013), p. 102.

57 United Kingdom's Prime Minister's Office, *Cyber Security Strategy: Safety, Security and Resilience in Cyber Space* (2009), p. 9.

58 The United Kingdom's Department of Culture, Media and Sport & the Department for Business, Innovation and Skills, *Digital Britain: Final Report* (2009), pp. 189-207.

59 Lawrence Lessig, "The Law of the Horse: What Cyber Law Might Teach," *Harvard Law Review* 113 (1999): 5.

60 Glenn Greenwald and Ewen MacAskill, "Obama Orders US to Draw Up Overseas Target List for Cyber-attacks," *Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

61 President Bill Clinton, "Statement on Signing the Economic Espionage Act of 1996," October 11, 1996, in Weekly Compilation of Presidential Documents, 32, no. 41 (October 14, 1996), http://www.gpo.gov/fdsys/pkg/WCPD-1996-10-14/html/WCPD-1996-10-14-Pg2040.htm.

Cyberspace Espionage and its Effect on Commercial Considerations

Gabi Siboni and David Israel

Cyberspace is becoming the primary and most effective tool for commercial espionage and the theft of information and intellectual property. It allows the attacker a technological shortcut, giving him the competitive edge over the market in general and the defender in particular. This essay examines whether the need to confront cyberspace threats in general and, more specifically, organizational information security affects the considerations of decision makers in commercial enterprises. Decisions relating to the feasibility of starting development, the costs of protecting the information, the product's life expectancy, and the commercial worth of exploring new fields may all be influenced. This essay also includes some suggestions for helping these fields at the national level.

Keywords: cyberspace, espionage, commercial espionage, intellectual property, cybercrime, cyber theft, technology, information

Background

Commercial espionage is hardly new. It has existed in different incarnations since the dawn of time. Some of the historic industrial revolutions were based on the copying of knowledge. For example, industrial machinery from Great Britain found its way to the United States and helped transform it into an industrial powerhouse at the expense of British patents.[1] In the business world, industrial espionage is usually considered one of the biggest threats to an organization's ability to survive in a competitive market. A fundamental assumption has been that the risk of theft and

Dr. Gabi Siboni is the Director of the Cyber Security Program at the Institute for National Security Studies. David Israel is an information security expert at Motorola Israel and an intern in the Cyber Security Program at the Institute for National Security Studies.

loss of information consisting of intellectual property could result from an internal threat, such as a disgruntled employee, a mole, or even a loyal worker who had been tricked. The threat could also be realized by copying a product through reverse engineering.

Until about a decade ago, protection against industrial espionage focused on physical aspects, such as restricted access areas, entrance checks, and security cameras, in addition to testing the loyalty of employees and others in the development and manufacturing chain, which included security checks, integrity testing, background checks of providers, and so forth. Protection was ensured by denying access to information and intellectual property located within an organization's physical space and by taking steps to prevent this information from being leaked by an internal party or by a foreign party that had breached the physical parameters of protection.

Protection of organizational information and intellectual property relied and continues to rely upon patenting and legal agreements, such as confidentiality agreements between companies and their suppliers, assuming that an organization can sue entities that harm its intellectual property. Sensitive information includes not only intellectual property, but also information that is liable to damage the organization in a myriad of ways, such as contract details, salaries (for headhunting special talents), information about tenders and price proposals, strategic plans, marketing plans, client lists, provider lists, and so forth.

The expanding use of cyberspace for technological development and manufacturing exposes this significant sphere to risks of leakage of sensitive information and intellectual property.[2] In fact, this development has changed the rules of the game in terms of the processes of securing information and intellectual property, making their protection much more complex and resource intensive, while the work processes and the flow of information in the organization has also been affected. Senior management in various organizations understands that the cyber attacker has the edge, and that his chances of success are high compared to the limitations of the organization to defend itself in cyberspace. One study conducted by a large consulting firm claims that some 60 percent of senior managers believe that cyberattacks will increase and become more sophisticated and frequent, exceeding the ability of organizations to defend against them.[3]

As a result, we are now seeing a profound change in decision-making processes affecting research and development and in the considerations of commercial organizations when it comes to investing in R&D. The severity of the threat of information and intellectual property theft requires organizations to take their protection very seriously. Such protection requires the allocation of significant resources, including technological ones, and the application of suitable standards and working procedures. These represent a burden on the human resources and involve high costs, thereby reducing the investment in the product's development. Thus, the organization must ask the following fundamental questions: what are the critical weaknesses in the business process and how should they be protected? What will be the added cost for protecting the information and for the entire security system needed for the R&D process? Will it be possible to construct the required protection system before getting development underway, and does the risk increase because the business enters the market late as a result? Because it is clear that any defense can be breached, it is also important to question the organization's ability to bounce back from damage to the working process during the development stage. What will be the effect of a breach on the overall investment? What delays can be expected during development as a result of limits on information sharing, and what will be the effect of these delays? The whole development process requires partnerships with external entities, even outsourcing. Therefore, one must ask to what extent will it be necessary to invest resources in protection in such situations, or demand that external providers supply additional protection that might increase the cost of their service?

This list of questions is only partial, but it makes it clear that the decision-making process in the era of cyber threats is changing and the investment in security processes is indeed significant. In addition to other business considerations, cyber threats could cause an organization to decide to refrain from engaging in technological development in fields that are particularly attractive to commercial espionage. Especially sensitive in this regard is the startup industry. These companies are usually on a shoestring budget; having investing all their capital into technological development, they will be hard pressed to invest the necessary resources into sufficiently protecting their intellectual property assets. As a result, the innovation industry is most exposed to cyber threats involving the theft of intellectual property. Israel has a diverse technological infrastructure, including many startups that develop innovative products and solutions. It is therefore important to examine Israel's role in helping to secure the intellectual property developed within it, especially as a result of investments financed by the Office of the Chief Scientist at the Ministry of Economy and Industry.

Companies are exposed to damage in cyberspace as a result of commercial espionage, as well as malicious cyberattacks aimed at causing shut-downs and other harm. Companies need to take into consideration these attacks and protect themselves. This essay will focus on the significance of investing in security and protection of information and intellectual property, as well as the R&D processes, and how such security considerations might affect the scope of R&D investments in general. Furthermore, this essay will examine the tools that may help companies meet their protection needs through shared means and initiatives with different commercial companies. Moreover, the essay examines the state's role in creating a security infrastructure that can help companies, both large and small, improve their protection of intellectual property and increase their willingness to confront cyber threats.

The Complexity of Protecting the Processes of Intellectual Property Creation

One of the most sensitive types of information requiring protection is intellectual property, which is the primary asset of tech companies and startups. In order to understand the complexity of protecting the processes of creating intellectual property – i.e., the complexity of securing the business innovation and its critical competitive edge that justifies the business' existence – the life cycle of the information needs to be analyzed. We will refer to this as the product life cycle in a high-tech company.

The development of a technological product is characterized by the following stages: coming up with the idea, characterizing it, developing a prototype, lab testing, and manufacturing. Needless to say, all the stages of the birth and development of an idea until its maturation as a final product and its manufacturing are digital processes based on different information systems that provide support for each stage of development. As a direct consequence, each stage provides the attacker with motivation and invites a possible cyberattack, whether via the Internet or through an internal party operating either intentionally or inadvertently.

In principle, the organization's objective is to identify the sensitive points in the process and determine cyber defenses for each. In practice, a risk assessment based on information flow and its importance in the development process very quickly turns into a multi-tentacle creature, requiring an in-depth security treatment for each tentacle. Neglecting a particular channel or underestimating its importance might be the weak spot of the defensive system in general. Each development process uses varied tools and technologies, involves different working environments, and always requires information-sharing capabilities, complicating the security of each development stage. At each stage, the organization must assess the need to mitigate risks, which involves confidentiality, integrity, and availability of the information assets.

As an example, we will examine the complexity of protecting sensitive information of an organization interested in developing a technology that can be defined as a strategic project and liable to be the target of a cyberattack. Early in the gestational stage, the company creates documents that are classified and restricted to internal access, such as minutes of meetings, presentations, technological analyses, market scenarios, roadmaps, and so on. These are stored digitally, thus requiring protective means that will ensure authorized access only. Implementing systems designed to prevent information leakage[4] are expensive and complicated to operate. The complexity of protecting sensitive information requires the organization to analyze the processes in which it creates its information; map the systems; understand the life cycle; identify the classified information in the database, the file servers, and end computers; and determine an organizational policy for defining classification. All this must be done before the organization selects the technological tools that will ensure the company's protection, requires users' training, and will accompany the project throughout its duration.

Beyond the need to secure intra-organizational information sharing, it is also necessary to manage and secure the information that leaves the organization. Almost every company shares information with outsiders in order to promote the development processes: from the developing engineer sharing information with some external subcontractor who is an expert in a specific and sensitive field, to the lawyers who have to receive and send business contracts to partners, suppliers or potential customers, and to the logistics and manufacturing personnel who receive and send information to service providers as part of managing the supply chain.[5] Protecting sensitive information that leaves the company is one of the most complex challenges to meet, since digital channels for data transfer from the organization are almost endless. An employee is liable to share information externally via the company's email or by personal email, via a portable device such as a USB flash drive or by burning it onto a CD, by using free file sharing cloud services,[6] and – worst of all – by peer-to-peer services in which the user installs software on an organization's computer that connects directly to a file-sharing computer network. Each of these methods represents a significant risk to the company's intellectual property. Each information channel requires technology that will limit, prevent, block, and monitor all of the information that flows through it.

Companies have invested many resources to block external memory-devices, such as flash drives and alike, preventing browsing on file sharing servers, and more. But the business need for efficiency and the ability to quickly share information from within and outside the office forces the company to create and allow secure and controlled information-sharing channels. One option is using cloud technology, which allows organizations to improve efficiency and make the information accessible from anywhere through cell phones, tablets, and home computers. Cloud services are an excellent solution for the organization, although their level of built-in security does not, at least for now, meet the rigorous needs of protecting information and intellectual property.

The results of a study by McKinsey indicate that the concern for cyberattacks results in a reluctance to adopt cloud technology and mobile services.[7] Some 70 percent of respondents reported that they postponed adopting the use of cloud technology by a year or more because of information-security concerns, and 40 percent reported they postponed the use of mobile services by a year or more for the same reason. In the high-tech field, 50 percent of respondents reported that they will have to make changes in their R&D processes. Another fact reflecting the influence of cyberspace defense on organizational functioning is that 50 percent of the senior high-tech managers who participated in the study reported that the topic of cloud services and mobile services was "a sore point," which limited the employee's ability to share information.

It thus emerges that technologies promising greater business efficiency, such as inexpensive, efficient cloud services, information sharing, and mobile technologies are perceived as a high risk, compelling an organization to spend more rather than to take a risk and wait until these systems can promise rock-solid security. Under these circumstances, organizations are liable to ignore cyberspace risks, preferring process efficiency and time-to-market instead of applying controls and accepting the limitations imposed by the security processes.

Another weak spot related to the organization's necessity to analyze and apply an information-security policy is the need to provide outside parties with access to the company's network. In many cases, the organization sees fit to provide an external provider with remote access to its network, thereby exposing the company to risks emanating with the provider and the level of protection that the provider implements.[8] Companies providing information systems remote support services; providers who have access to update internal logistical information systems; sub-contractors and business partners connected remotely to the company's systems all have possible access to the core of the information systems and the company's network. The access of these parties necessitates that the company builds, maintains, and manages a secure, encrypted communications infrastructure, using a secure logon and authentication process for the organization given access. In addition, the company should limit the network access of these parties to only those resources critical for their work, preventing situations in which they can browse freely through the company network and view sensitive information in its servers and databases. All access by outside parties should require a process analysis, that is, the name of the server to which access is needed; what software and protocols the party must operate; the creation of a designated username; the operation of a control and monitoring system for the whole process of connecting to and working on the server; implementation of firewall rules; and, of course, continuous reassessment of the need for external connection and for handling glitches.

It is essential to ensure that the level of information security on the external party's end is adequate, and to diminish the security risk from any possible weakness in the service provider's end station. Among other steps, it is important to ensure that the external party's computer has an updated antivirus protection. Has the party received the latest security updates? Is the party infected with a Trojan horse or other malware? A supplier's computer connecting to the organization's network becomes an integral part of it. In many cases, it is the weakest link in the system through which a hostile party can penetrate the network for the purpose of carrying out a cyberattack. Under these circumstances, it does not matter if the organization is regulated, has an updated security policy, and secures end stations by routine security updates, antivirus protection, and locking-out software; the moment an external party with an inferior security policy has access to the organization's network, that party becomes a clear and present danger.

Another layer than must be addressed from the security perspective is the process of creating the prototype and the lab testing stage. This is a sensitive stage in which for the first time, the company exposes the innovative technology, the product, and the new capabilities that are supposed to facilitate its business breakthrough. This is where the intellectual property turns into a fixed entity. Were a hostile party to get ahold of it, that party could stand to gain a significant advantage. Therefore, in most cases, the security needs dictate the establishment of restricted development areas and labs that have separate networks, which are severed from the Internet, and have applied added infrastructure and security products parallel to those already on the organization's network. Needless to say, the economic costs of building separate networks of this sort are high, and operational difficulties are great when it comes to moving information to and from the classified networks.

One of the most significant security circuits is the system to control and monitor security events. Without a monitoring system, the organization does not have any ability to identify security events in its systems nor to adhere to its security policy and confront potential cyber events, not to mention the ability to respond to such events and move quickly to reduce the threat. Security information event management (SIEMs) are usually expensive and require constant maintenance and updating to adapt them to new threats, new business processes, and new security systems. A SIEM can receive a security alert usually rooted in the logs of events from intra-organizational systems (audit logs and security logs), such as servers, communications equipment, firewall systems, authentication servers, remote access systems, databases, file servers, and more.

In addition to technological tools, the organization also needs skilled employees who understand the meaning of the events noted by the system and who are capable of analyzing the activity and determining a countermove. Moreover, the use of a SIEM allows the incorporation of outside cyber intelligence information, which provides current information about the nature of known cyberattacks, the sources of the attacks, and the tools used by the attackers. This intel is crosschecked with existing information in the organization's network, allowing early identification and rapid response to the event. The importance of using SIEMs in defending against cyberattacks is evident in a study by the Ponemon Institute. According to this study, companies using these systems were more efficient in identifying and containing cyberattacks. Consequently, those companies saved some $250,000 worth of damage compared to companies not using SIEMs.[9]

The most important step in defending against cyber threats is investing in employee education and awareness of cyber risks. Successful cyberattacks penetrate an organization through its weak links – its employees – and from there implement the attack. From this perspective, a study of phishing-type attacks targeting a company's employees is of particular interest.[10] This, however, does not conclude the activities that organizations must carry out in order to defend their intellectual property. It is not enough to define the sensitive points in the process and protect them; organizations must also invest and develop their network defensive capabilities and build monitoring and control systems that require constant acquisitions, adaptation, and maintenance so as to be able to identify security events and cyberattacks in real time.

It is evident that protecting intellectual property is a complex technological, organizational, and managerial process of great significance to the organization. The process and its financial cost have negative business ramifications, as the analysis below will demonstrate.

Negative Economic Ramifications

Cyberattacks and their potential for damage have negative ramifications on the organization's operational efficiency and its attempts to shorten development and manufacturing processes in order to reach the market before its competition does. According to McKinsey's estimates,[11] as long as cyber threats continue to grow and defensive capabilities fail to provide an appropriate response, they will negatively affect the global economy in the next five to seven years, by harming the value production of the companies, worth $9-21 trillion. This means that the costs of protecting against cyber threats and the loss of information and intellectual property resulting from commercial cyber espionage will significantly damage the global economy. The numbers cited above are, of course, affected by the development of the strength of the defense systems. In addition, there is also the economic cost specific to any given company, mostly because of its need to expand its cyber defense budget at the expense of its R&D budget and, consequently, also because of reduced operational profitability.

Beyond the negative impact of cyber risks – manifested by a global slowdown and the corporate need to increase investments in cyber defense – the damage to intellectual property, which has its own economic ramifications, is a significant risk. Damage to intellectual property is liable to affect the balance of global commercial forces, create unfair competition, and economically harm the profitability of companies to the point of their becoming extinct. Many companies whose intellectual property has been damaged have reported losses of sales, licenses and royalties; decreased profits; and harm to the brand and product's reputation.

One prominent example of intellectual property theft is the Chinese J-31 stealth plane, strikingly similar to Lockheed Martin's F-35. In the past, the American company was the victim of a Chinese cyberattack in the course of which the stealth technology was stolen.[12] The F-35 is considered the most advanced plane in the world. Today, the Chinese possess the costly technological knowledge associated with this plane, such as detailed diagrams of the engine, radar and other systems; advanced manufacturing technologies; and so forth. In this particular instance, the intellectual property, in which billions of dollars had been invested, was revealed to a competitor who used it to create the J-31, stunningly similar to the original. Advanced technological information that falls into a competitor's hands gives the competitor a technological boost and makes it an important player in a market, which, previously was controlled by a limited number of companies.

The main problem is that a company may not even be aware that it had been the victim of a cyberattack designed to steal information or intellectual property, since the information continues to exist on its servers and function as usual. However, it no longer controls the information and must deal with a new competitor who has similar or improved technology and therefore an invaluable relative advantage. Studies show that the time it takes a company to discover it has fallen victim to a cyberattack is 230 days on average.[13] This means that during this period, the attacker is free to inhabit the company's systems – long enough to study the information, analyze it in terms of relevance to the attacker's needs, draw conclusions, and even improve the attack process. The information amassed by the attacker allows it to understand the company's network structure, learn the names of the systems in use, identify the file servers and databases, crack the passwords of employees with access to the most classified materials, and penetrate databases of interest. Moreover, the information copied from the company allows the attacker to understand the organizational structure, become familiar with key personnel and decision makers, and continue to carry out targeted attacks to extract the specific information of interest.

As noted, the company under attack has no idea it is under attack or how much time the attacker has roamed its network. Even if the company has its suspicions, it will take a long time to learn the details of the attack, its severity, and the quality of the information stolen. The long time lapse before the attack is identified is one of the most important advantages the attacker has, so that shortening the time of discovery becomes one of the most significant challenges in defending against cyberattacks. The ability to identify a cyberattack and respond to it is directly correlated to the company's investment in advanced identification and early warning systems, defense of end stations and databases, implementation of security standards, and employee awareness.

One must also remember that cyberattacks aimed at stealing information are nothing like denial of service (DoS) cyberattacks. In the case of the latter, a company can apply recovery processes when the attack ends and return to normal operations, while drawing conclusions on how to fix the breaches. By contrast, an attack in which knowledge and intellectual property are stolen requires the victim to undertake a complex process of strategizing about future business activity: how to assess the amount of damage caused to the company; whether or not to continue developing the product which depends on a technology that is no longer controlled by the company; whether or not to continue the business strategy outlined in the original plans or to change it radically, and so forth.

According to assessments from various sources,[14] cyberattacks designed for industrial espionage annually cause billions of dollars damage to the global economy. The effects of theft of information and intellectual property are expressed directly upon the organization and also indirectly upon the country's economic situation. In any case, the ability to assess numerically the economic damage is a challenge in itself, and any estimate is no more than conjecture.

The cumulative economic impact of the theft of information and intellectual property has several features. First and foremost, the attacker has the ability to gain a technological advantage and can offer an identical product at a cheaper price because it did not invest in the product's development; at times, the attacker's manufacturing costs are also cheaper. The results for the victim can include reduced sales of the product and having to lower prices, decreased profits, a loss in the value of its shares, and even the demise of the company. Whatever the outcome may be, the costs to the company to handle the attack and improve its defenses are high. A famous example of a company that ceased to exist because of information theft is that of DigiNotar, a Dutch company that went bankrupt after critical information was stolen from it.[15]

At the national level, cyberattacks aimed at stealing information and intellectual property are liable to result in a lowered GDP and the loss of jobs, especially in a country whose economy is driven by technology and R&D. Investments in advanced technology are liable to be lost, translating into an economic boon for the attacker. Moreover, sensitive technological security information is liable to be leaked to enemies, affecting the balance of power vis-à-vis hostile entities and rivals. A quantitative estimate of such an effect could be based on any number of different economic forecasts, but one thing is clear: the economic effect of a cyberattack, both at the company's level and at the national level, must be given profound strategic attention.

In examining the effects of commercial espionage in cyberspace on company business decisions, we must first look at three basic aspects. The first relates to the decision makers' level of awareness of cyberspace espionage risks; the second relates to the question of whether the various companies have the tools to assess the risks and make informed decisions about them; and the third concerns the way in which the decisions made in response to cyber risks are implemented in practice within the organization. Studies show that most companies find it hard to assess the risks and as a result have a difficult time formulating plans to deter them.[16] The unanimous opinion is that cyber risks and sophisticated attacks will only grow as long as companies do not have effective capabilities of defense.

Leakage of intellectual property is one of the main concerns of high-tech companies and is most severe compared to the leaking of product specifications. In contrast, service companies are worried mostly about the leakage of information that identifies their clients, which could damage the service they provide. A survey of companies' cyber-risk maturity – their ability to analyze cyber risks – indicates that large organizations also suffer from significant gaps in their ability to undertake risk management: 90 percent of companies surveyed reported "developing" or "beginning" risk-management processes, while only 5 percent relayed being in an advanced or "mature" risk-management process.[17]

It is interesting to note that no correlation exists between the financial outlay for risk management and the actual maturity of the risk-management process. There are companies that have invested little in the field, but have carried out an effective risk-management process, while others have invested significantly in the process, but have done so without sophistication, thus leaving much to be desired. Senior financial managers lacking technical knowledge have difficulty incorporating cyber risks in their risk-management processes and making informed decisions, all due to the lack of information. Moreover, despite the preoccupation of large organizations with protecting information and spending a significant amount of money over the years on this issue, the data reflect a large gap between the sophisticated risks in cyberspace and the ability of companies to defend against them.

In fact, one might conclude that the greatest problem in dealing with cyber risks is the ability to assess the risk, and consequentially, the difficulty in providing an appropriate security response. The difficulty in confronting complex cyber risks – and the poor record of success to date – has led to the conclusion that increasing cyber expertise within the organizations themselves is imperative. At present, there is a growing trend in large American companies to hire cyber experts for senior positions.[18] Companies included on the Fortune 500 list have appointed cyber experts who report directly to the CEO, compared to the widespread structure in which the chief information security officer – CISO – reports to the chief information office – the CIO. Moreover, the demands currently made of cyber experts include not only a technical understanding in the field of information security, but also extensive familiarity with business processes and an understanding of risk management.

Although large companies make strategic decision about cyber security and establish bodies with the requisite knowledge and technologies designed to analyze the risks and improve the level of security around the information assets, mid-sized and small companies find it hard to do so on their own. These companies lack the resources needed to apply the range of processes, technologies, and frequent adaptations required in the field of cyber defense. Companies with limited resources face several options. Applying minimal cyber defenses to the best of their understanding and budgetary allowance consequently leaves them at risk of information and intellectual property theft as a determined attacker will, in all probability, be able to penetrate the company's network. Many small, resource-poor companies will appoint a system administrator as the professional in charge of information security. In many cases, that person's work will focus on issues within his or her technical responsibility, such as security of servers and end stations, user management, mail server security, and network infrastructure security. Such a person will not be able to build an information security system that takes into consideration the professional analysis of potential cyber risks facing the organization.

A second option is for the company to increase its cyber defense budget in order to provide an appropriate response to the risks and, accordingly, to risk management. One may assume that this will involve significant investing in a cyber security infrastructure, the acquisition of relevant products, setting up a team of experts, professional training, meeting standards, and so on. Investing in the field will affect the company's profitability and its ability to compete, in the expectation that the investment will pay for itself first and foremost by reducing the probability of cyberattacks while increasing the company's ability to develop business processes in a properly-secured environment.

A third option involves relying on managed security services via outsourcing, although in many cases the providers do not see the whole organizational picture and are not part of the critical processes described above. The primary advantage of relying on outsourced security services is that it enables a company that does not have any knowledge or technological and economic ability to receive professional security services. Moreover, the price tag will be lower because the service provider distributes its costs over a large number of customers. On the other hand, an external entity is not part of the company's day-to-day functioning and is not privy to business processes that change regularly and has limited ability to provide an integrative response that is tailored precisely to the organization's needs. Furthermore, outsourcing usually provides a range of priced, defined, and generic services so that it can appeal to most of its customers, which makes it difficult to receive security services that are both dynamic and specific to the company's needs. Managed security services can be a real improvement for small companies with clear security needs, but only up to the point where the business processes become complex.

It seems that small companies, which are founded entirely on their intellectual property, will find it difficult to protect their information – their chief asset – and their working processes against sophisticated cyberattacks. These companies will settle for a partial security solution on the assumption that they are not a preferred target of sophisticated attacks. This type of solution will then place them at the top of the ladder of companies at high risk of cyberattacks, business espionage, and information and intellectual property theft.

The situation is especially difficult for Israeli startup companies. Israel's R&D industry is widespread. Hundreds of companies rely on the R&D budget of the Office of the Chief Scientist at the Ministry of Economy and Industry and on raising capital from all sorts of funds in order to develop knowledge, technology, and products. The intellectual property is the most important asset in the existence and development of the Israeli startups. These companies will have to choose one of the three alternatives described above. One can assume that, because of budgetary constraints and possibly also because of a lack of awareness, they will opt for minimal cyber security. This means that the most advanced information assets and the largest potential growth engine for the nation's economy will receive the lowest form of cyber defense on the market. This is a disturbing realization, requiring profound attention at the national level.

Supporting the need to formulate a national response and strategy for the cyber defense of Israeli startups is the Office of the Chief Scientist at the Ministry of Economy and Industry. The chief scientist facilitates the establishment of technological hothouses by financing of up to 85 percent of their budgets, for an annual total of ILS 1.5 billion. The government's financing is expected to be returned through royalties paid to the state from any income generated by the product itself or a related product, including services that are ancillary to the product or involved in it. The chief scientist's investment in R&D is thus a highly risky venture because of the exposure of developing technologies to the theft of their intellectual property. The damage might be inestimable as the companies risk their ability to realize the products of their R&D, and, as a consequence, they also risk their ability to pay back the state for having funded the R&D process.

Concluding Insights

Protecting information and intellectual property is a critical need for any private, commercial or national organization. The process of protecting information and intellectual property is complex, both technologically and process-wise, and has significant ramifications for the organization's development budgets. The successful implementation of an effective defensive shield around the information and intellectual property depends mostly on the organization's awareness of the risks and its ability to optimally protect itself. All of this is a direct consequence of the organization's economic capabilities, the maturity of the organizational culture regarding information security, the existence of organizational functions, and the presence of skilled manpower. It seems that the economic ability to realize advanced security solutions is one of the major obstacles that small and mid-sized companies face when trying to confront the risk of information and intellectual property theft. But the existence of economic ability – while certainly a necessary condition – does not alone ensure effective handling of the risk of cyberattacks.

It is clear that organizations find it hard to assess their cyber risks because of the lack of current knowledge, the complexity of the issue, the lack of economic resources, insufficient skills, or an inappropriate organizational structure (such as the lack of a position in charge of cyber defense and risk-management). This situation affects an organization's awareness of cyber risks and its preparedness to operate against them. Even organizations rich in resources and professional manpower do not always succeed in implementing optimal defenses against cyber risks, which can provide an effective response using different means information security. The situation is particularly dire for startups notable for their groundbreaking intellectual property and tremendous economic potential, and, at the same time, for their limited budgets that keep them from effectively defending their valuable intellectual property. Moreover, startups by their very nature are focused on technological development and tend not to set up significant IT and information security entities.

Israel's government security organizations and critical infrastructure companies in the private sector are defined as bodies guided by the National Agency for Information Security and the director of security of the defense establishment. By contrast, Israel's private sector sphere is left without guidance or help at the national level, and is, in fact, expected to conduct itself to the best of its understanding and ability. The National Cyber Bureau may be tasked with determining a comprehensive policy for protecting Israel's computerized systems (the so-called "national cyberspace policy") and with developing a state-wide operational approach that is suitable for routine times.[19] Protecting information and intellectual property in private sector institutions not considered critical infrastructures, however, is not a significant part of the bureau's work.

It is incumbent upon the State of Israel to improve its defense of knowledge that is supported with the state's R&D funds, and to ensure the protection of information and intellectual property in the technological and business sectors, as damage to these two sectors would directly affect the Israeli economy and market competition. Furthermore, the State of Israel needs to establish a consulting body for the protection of knowledge and intellectual property within the private sector in general and technological companies, such as startups, in particular. The National Cyber Bureau might be responsible for this body.

One response, albeit only partial, to the challenges described herein is to demand that the state protect its investments in R&D. Such a demand could cause private sector business initiatives to respond with an appropriate level of expertise and at a reasonable cost for companies financed by the Office of the Chief Scientist. It is therefore advisable that the government assist in constructing a security infrastructure for needy companies. An example would be helping with development capabilities and activity within a secure cloud, applying high-level security standards.

A business enterprise that seeks to provide security solutions and development capabilities in a secure infrastructure will only do so if it assumes it has a profitable business model and enough clients. This will occur if the companies financed by the Office of the Chief Scientist are urged to secure their intellectual property using professionally-determined standards. This necessary action will match the financing body’s demands to operate in a secure environment together with the response of private sector companies that will provide such an environment to a captive market.

The establishment of a secure cloud infrastructure should create a safe space for the needs of technological development companies, including startups. Such an infrastructure would be based on security systems that specialize in protecting information and intellectual property and allow those companies to manage their sensitive information within much tighter security parameters than they could make for themselves. The Office of the Chief Scientist, which budgets millions of shekels to technological hothouses, is accelerating the use of the secure cloud. The Office of the Chief Scientist is also a partner in the Kidma Program to Advance the Cyber Security Industry in Israel,[20] along with the National Cyber Bureau, and gives preferential budgeting to R&D in the field of cyberspace in order to promote and position Israel as a global leader in the field. Getting funds from the Office of the Chief Scientist at present is not conditional upon presenting a plan to protect the information and intellectual property; thus, million-dollar companies that are developing technologies designed to fuel Israel’s economic growth are, in practice, exposing themselves to cyberattacks and potentially tremendous damage.

In a world in which sophisticated cyberattacks focus on the theft of information for the sake of taking technological shortcuts, the establishment of a professional body that consults for private sector technological companies and the development of a designated cloud infrastructure with a high level of security should dramatically improve the survival rate of the startups and ensure the successful protection of their intellectual property. By making such a move, Israel would be able to maintain an obligatory security mechanism and ensure a return on its R&D investments.

Notes

[1] Doron S. Ben-Atar, *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power* (New Haven: Yale University Press, 2004).

[2] In many cases, manufacturing plans for product components (sets, printed circuits, electronics, and so forth) are sent to subcontracted manufacturers via magnetic media, whether physically or through telecommunications.

[3] Tucker Bailey, Andrea Del Miglio, and Wolf Richter, "The rising strategic risks of cyberattacks," *McKinsey Quarterly*, May 2014, http://www.mckinsey.com/insights/business_technology.

[4] Such systems are known as data leakage prevention systems.

[5] The organization's supply chain manages processes of acquisitions, manufacturing, storage, distribution, and shipping, and its function is to connect the manufacturers, suppliers, and end clients. Supply chain management requires great flexibility and coordination capabilities vis-à-vis external entities, and represents an important component in creating the company's value.

[6] Cloud services include DropBox, Google Drive, Jumbo Mail, and the like.

[7] Bailey, Del Miglio, and Richter, "The rising strategic risks of cyberattacks."

[8] The attack on the North American retail chain Target, in which millions of credit card numbers were stolen, started with the theft of access permissions from a maintenance-systems provider that Target had contracted. See Brian Krebs, "Target Hackers Broke in via HVAC Company," *Krebs on Security*, February 14, 2015, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[9] "2013 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2013.

[10] "APT1 Exposing One of China's Cyber Espionage Units," *Mandiant Report*, February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[11] Bailey, Del Miglio, and Richter, "The rising strategic risks of cyberattacks."

[12] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," *Diplomat*, January 27, 2015, http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

13 Mandiant, "Mtrends: Beyond the Breach: Mandiant 2014 Threat Report, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

14 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.

15 See the detailed analysis of this attack in Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare," *Military and Strategic Affairs* 4, no. 3 (December 2012): 77-100, http://www.inss.org.il/uploadImages/systemFiles/MASA%20-%204.3.pdf.

16 Bailey, Del Miglio, and Richter, "The rising strategic risks of cyberattacks."

17 Ibid.

18 Nadia Damouni, "U.S. companies seek cyber experts for top jobs, board seats," *Reuters*, May 30, 2014, http://www.reuters.com/article/2014/05/30/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530.

19 From the homepage of the National Cyber Staff at the website of the Civil Service Commission http://www.csc.gov.il/DataBases/NewsLetters/NewsLetters3/Pages/CyberHeadquarters.aspx.

20 See circular issued by the Office of the Chief Scientist: "The Kidma Program to Advance the Cyber Security Industry in Israel," November 21, 2012.

Has the "Spider Web" Theory Really Collapsed?
Casualty Sensitivity during Operation Protective Edge

Yagil Levy

The public discourse during Operation Protective Edge (2014) reflected a higher degree of willingness to accept military casualties than it had during previous wars or operations, particularly the Second Lebanon War (2006). In this article, I seek to clarify the prevailing argument regarding Israeli society's greater willingness to accept military deaths, and to show that this argument should not be accepted at face value. My argument is that casualty sensitivity exists, but it is more complex than it appears to be and is also affected by changing circumstances. When the military operation is swift, intensive, and perceived as successful – as epitomized by Operation Protective Edge – and the sacrifice made by the more affluent social groups is few and even justified in terms of voluntary choice, military death can be more easily justified and does not arouse substantial opposition.

Keywords: risk transfer, military fatalities, casualty aversion, collective action, casualty sensitivity, bereavement discourse

Introduction

The public discourse during Operation Protective Edge (July-August 2014) reflected a higher degree of willingness within Israeli society to tolerate military casualties than it had during previous wars or operations, particularly in relation to the previous round of violence, the Second Lebanon War (2006), during which dozens of soldiers were killed. Operation Protective

Prof. Yagil Levy is a faculty member at the Open University of Israel.

Edge, which lasted fifty days, was Israel's reaction to the escalating rocket and missile fire from the Gaza Strip into Israel, a spiraling escalation over which neither side could control.[1] During the first ten days of the operation, the IDF bombarded the Gaza Strip from the air, ground, and sea; Hamas fired rockets on Israeli communities and made a number of attempts to infiltrate Israel through tunnels that it had dug. Hamas rejected Egypt's proposal for a ceasefire, upon which Israel launched a ground operation tasked with destroying the tunnels. The ground operation lasted about two and a half more weeks, and a ceasefire was achieved only after another three weeks of IDF shelling from the air, ground, and sea.

Sixty-five soldiers were killed during the operation, but their deaths did not arouse public protest or an outcry of opposition to the continuation of the fighting. Against this backdrop was the claim that the "spider web" theory had collapsed – the theory of weak stamina that Hezbollah's Secretary-General, Hassan Nasrallah had attributed to Israeli society. In this context, Professor Ishay Rosen-Zvi, an expert on Israeli culture, made a particularly keen observation during his lecture at a conference at Tel-Aviv University, saying that, "Soldiers' deaths are no longer creating the same public pressure as in the past. This is a new mechanism that differs from the one that we are familiar with, when coffins evoked feelings of revulsion that triggered criticism and media pressure."[2]

Rosen-Zvi's impression was corroborated by Zipi Israeli and Elisheva Rosman who analyzed the media coverage during Operation Protective Edge. According to their study, the media had indeed covered the casualties throughout the operation, but not in a critical manner as in the past, and even if criticism was levelled at the political echelon about tactical conduct, it did not address the human cost of the fighting. The sacrifice was presented as a necessity, the soldiers who lost their lives were presented as heroes, and the discourse did not return to its former pattern of focusing on mourning.[3] A contrary position was echoed by Breaking the Silence, which documented soldiers' testimonies in this operation. Breaking the Silence concluded that the "guiding military principle of 'minimum risk to our forces, even at the cost of harming innocent civilians,' alongside efforts to deter and intimidate the Palestinians, led to massive and unprecedented harm to the population and the civilian infrastructure in the Gaza Strip."[4]

We thus observed two different approaches that seemingly are not contradictory. Indeed, the Winograd Commission, which conducted an inquiry into the Second Lebanon War, quotes Meir Dagan, the head of the

Mossad at that time, who said during the war that, "In my mind, the trauma of Lebanon [in which Israel was dragged into a deadly war of attrition in the years 1982-2000] exists more in the politicians' minds than those of the public."[5] With this remark, he succinctly elucidated the conventional hypothesis that, in reality, the public may be more tolerant of casualties than the policymakers and senior military officers. However, the leadership's concerns that the public will not tolerate casualties may result in risk aversion and even mission aversion, or, alternatively, an aggressive fire policy, both mitigating the risk to soldiers.[6] That is to say, the belief that the sight of coffins generates opposition reflects the leadership's concerns more than public opinion to which the leaders should have responded; certainly, this sight will not inevitably generate organized, antiwar collective action. Nevertheless, the contradiction presented above about the extent to which the public tolerates casualties warrants clarification to which it is hoped the present article will contribute.

My argument is that the assumption that the public showed a higher degree of willingness to accept military casualties in this operation should not be accepted at face value. Casualty sensitivity exists, but it is more complex than it appears to be and is affected by changing circumstances. When the military operation is swift, intensive, and perceived as successful, and the sacrifice made by the more affluent social groups is minor and even justified in terms of voluntary choice, the military death is easier to justify and does not arouse substantive opposition.

The first part of this article will present the background to the discussion and its theoretical framework. The second part will present a number of assertions that examine various explanations for the non-development of active opposition to the sacrificing of lives during Operation Protective Edge.

Background and Theory

Sensitivity to military casualties developed in Israeli society primarily after the First Lebanon War (1982), following a similar path in other democracies; the bereavement discourse reflected this change. Up until the First Lebanon War, soldiers' deaths were perceived as inevitable, as part of the "silver platter" upon which the state's independence was served. The hegemonic discourse at the time was characterized by the bereaving families' acceptance of their loss. The state bestowed honor and prestige upon them and transformed the fallen into symbols of national commemoration; in exchange, the families accepted and reconciled themselves to their sacrifices.

Criticism or questioning about the circumstances of their children's deaths was not part of the discourse.[7] This attitude began to change during the Yom Kippur War, when many bereaved families entered the political arena and joined those demanding to dismiss the Minister of Defense, Moshe Dayan, who was perceived as being responsible for the "mishap" leading to the war. Nevertheless, substantive public challenges were only first voiced after the First Lebanon War (1982), which shattered the consensus supporting the sacrifice of lives on the battlefield, with the discourse becoming more critical and even subversive.

"The Beaufort Family" – a group of bereaved parents who protested the deaths of their sons during the battle over the Beaufort Castle on the first night of the First Lebanon War – was one of the first groups that questioned the war's justification. These public challenges were echoed by the group "Soldiers against Silence," composed of discharged reservists, which protested the death toll during the war of attrition in Lebanon (1982-1985). The protesters raised placards opposite the residence of Prime Minister Menachem Begin to show him the latest number of casualties. The phenomenon reached a peak with the "Four Mothers" movement, which protested the human cost of the military deployment in southern Lebanon after two military helicopters had collided en route to Lebanon and claimed the lives of seventy-three soldiers. The Four Mothers' protest played a pivotal role in supporting the IDF's unilateral withdrawal in 2000. Similar protest organizations became active after the Second Lebanon War (2006), formed by reservists and bereaved parents. These protested the army's flawed functioning during the war, which they claimed led to fatalities that could have been prevented or, alternatively, justifiable had the war's objectives been achieved.

These protest movements leveraged their sacrifice both as reservists and as parents of soldiers and translated it into a political voice. Both bilateral withdrawals from Lebanon, in 1985 and in 2000, which were influenced by the protest over the sacrificing of soldiers' lives, clearly reflected the change in the bereavement discourse and its impact on IDF deployment.[8]

The intensification of this critical discourse imposed restrictions on the freedom of action of the governments and of IDF commanders to endanger soldiers, which peaked during the Second Lebanon War when the government waited until the last minute to launch a massive ground operation deep into Lebanon. The Winograd Commission determined in this context that, "The IDF conducted itself during the war as if its concern about casualties among its soldiers was a central element in its planning process and operational considerations . . . We note that a fundamental component of Israel's security approach is that the army's role is to protect civilians and ensure they live their routine lives."[9]

IDF commanders also acknowledged that Israeli society tolerates causalities less than in the past and that this sensitivity affects military deployments in combat.[10] Since the year 2000, the concern for casualties has deterred the IDF from initiating ground operations in the Gaza Strip; when they were launched, an aggressive fire policy was implemented that mitigated the risk to soldiers and partially transferred the risk to enemy civilians. A clear correlation has been identified since then between Israeli society's heightened sensitivity to casualties and the tendency to adopt an aggressive fire policy, compelling decision makers to use force only when they could claim legitimacy for implementing such an aggressive policy. When such legitimacy has not been achieved, decision makers have opted for military restraint (like the cease-fire arrangements with Hamas, similar to those reached with Hezbollah in Lebanon) in lieu of limited use of force that would increase the risk to IDF soldiers.[11]

Seemingly, this casualty-sensitivity syndrome was not prevalent during Operation Protective Edge. Even if the IDF adhered to the strategy of transferring the risk from its soldiers to the enemy civilians – out of its internalization of Israeli society's sensitivity to casualties – as members of Breaking the Silence have claimed, there are those who will claim that the government and the IDF could have assumed greater risks, given the change in society to accept a higher number of fatalities among its soldiers. I will endeavor to clarify the degree of sensitivity during Operation Protective Edge later on in this article.

Sensitivity to military losses has increased in democratic societies since the 1960s, playing a key role in limiting the state's freedom of operation in deploying the armed forces for military missions, with the Vietnam War representing the turning point. Subsequently, the concept of a casualty-aversion policy was coined, designed to mitigate the risk to soldiers whether by refraining from risk-intensive missions or by launching them in a manner to bolster the soldiers' protection, including through increased use of technology, or by transferring the risk to the enemy civilians by implementing an aggressive fire policy.[12] This casualty-sensitivity syndrome evolved parallel to the strengthening of the liberal culture and its materialistic foundations, and to the diminishing sense of existential threats, particularly with the demise of the Cold War.[13] This change led to the evolution of a post-heroic culture, in which risk to soldiers constitutes a key constraint when forging military policy.[14] Alongside the sociological explanation, scholars of international relations and political science identified variables that heighten or diminish casualty sensitivity even when a political culture is intolerant of fatalities.

Against this background, I wish to propose a two-tiered theoretical framework for the empirical discussion: the first tier is based on the argument by the American political scientists, Gelpi, Feaver, and Reifler that support for continuing a military operation in the face of mounting combat casualties is a function of the interactive effect of two underlying attitudes: expectations that the military operation will be a success and belief in the initial justification of the decision to use force. So, the ability to achieve the goals rather than the number of casualties determines the level of casualty sensitivity.[15]

This argument is a convincing explanation, particularly if we recall that, in Israeli reality, the number of casualties does not always explain the protest or, alternatively, the consensus that arose with respect to bereavement. Nevertheless, the weakness of this argument is that it relies solely on public opinion surveys. Changes in military policies informed by casualty sensitivity often occur when antiwar movements garner mass support, as demonstrated in the cases of the Vietnam War and the First Lebanon War. Public opinion matters to the extent that it is translated into collective action and thereby impacts policies.[16]

Subversive collective action develops mainly among the networks of the middle-class groups that have the time, resources, qualifications, and the courage to protest in circumstances in which they bear significant burden. Therefore, we can ask which social groups bear the burden of the casualties and as a consequence, are likely to develop critical attitudes towards their sacrifice, translating into subversive bereavement discourse, and then into protest. Studies show a correlation between the level of resistance to war and the social origins of those bearing the burden of sacrifice: subversive responses are more likely to arise when the more privileged groups bear the sacrifice. This finding leads to the conclusion that the transition from conscription to voluntary recruitment weakens the potential for protest in most democracies inasmuch as the troops are increasingly staffed with lower-class groups, even when the number of casualties increases.[17]

There are two advantages to this framework: firstly, it turns the argument of Gelpi and his colleagues that "success matters" into a more complicated one and gives greater significance to the interpretations of various groups – an interpretation influenced by each group's social status – of the question of whether the military operation achieves its objectives and whether the sacrifice is commensurate with the achieved objectives. Secondly, this argument raises the possibility that critical public opinion might not evolve into protest, primarily in circumstances when lower-class groups bear the burden of sacrifice. In this scenario, public opinion will also not affect military deployment by means of applying pressures to cease a military operation.

The combination of these two theoretical arguments, both which incorporate the variables of success, justification, and social composition, leads to the assumption that as long as the military sacrifice is shouldered by non-privileged groups, the justification of the use of force and the expectation of its success will increase society's willingness to accept a high number of casualties. On the other hand, insofar as those who are sacrificed are from a more affluent class, one can expect a more critical reading of the reality; that is, a critical reading of the justification of the use of force and of the degree of success achieved relative to the level of casualties, as well as to other sacrifices, such as the economic costs of war. This critical reading could potentially be translated into active opposition to the military policy.

Following are a number of assertions that illustrate a variety of aspects of sensitivity to casualties during Operation Protective Edge. With these assertions, we will attempt to answer the question of why casualty sensitivity did not develop in Israeli society during this operation.

1. Intensive war did not lead to the development of protest and sensitivity

In the past, antiwar protest emerged only after the fighting stopped. Thus, for example, the Beaufort Family emerged after the initial days of combat in the First Lebanon War, upon the completion of the war's "official" stage. This was also the case during the Second Lebanon War. Unlike what is envisioned in the collective memory, questions about the circumstances of soldiers' deaths during these two wars arose about a week after the fighting stopped, when bereaved parents joined the emerging circle of protest. It follows that coffins did not trigger a critical reaction immediately upon their appearance. In the past, protest developed also under circumstances of a protracted war of attrition. This was the case during the war of attrition in Lebanon (1982-1985), with the emergence of the Four Mothers movement, and with the protest started by the Shuvi movement in 2004 against the loss of soldiers in the Gaza Strip during the Second Intifada.

In contrast, Operation Protective Edge may be classified as an intensive war. The majority of the casualties during this operation occurred during about two weeks only, particularly during the ground operation, which could be perceived as intensive combat, but also limited in time and targets (see below). Under these circumstances, the potential for developing both sensitivity and protest was low. It is reasonable to assume that sensitivity and protest would have increased if the ground operation had become prolonged and the number of fatalities had risen, or that they would have developed after the fighting if the operation had been portrayed as having missed its targets, an issue that we will analyze next.

This assertion partially adopts the classic argument of John Mueller, whereas an increase in the number of cumulative casualties heightens casualty sensitivity and thus weakens public support of the military operation.[18] Nevertheless, as other studies cited here show, and as I will elucidate below, numbers alone do not trigger change, unless they are interpreted within the context of the conduct of the operation, its objectives, and achievements.

2. *Sensitivity that may arouse protest depends upon the nature of the combat and its political interpretation*

Left-wing sensitivity can appear as opposition to sacrifice when the sacrifice seems to lack a political purpose, such as the claim that the First Lebanon War was a "war of choice" – a claim that fueled the left-wing protest. Such sensitivity typified the protests of the Beaufort Family, Four Mothers, Soldiers Against Silence, and Shuvi, although, in fact, even the Four Mothers movement had not condemned Israel's presence in southern Lebanon, but rather, protested only its efficacy, given the death toll. Such protests against the military sacrifice can offer a political alternative or a nonviolent alternative, or one that involves less violence (like the demands of the Four Mothers or Shuvi to defend the state's borders at the Green Line and, by doing so, to also reduce the violence from the Arab side).

Right-wing sensitivity can induce protest about unjustified sacrifice, due to the failure to achieve the highly justified military goals. This is the type of sensitivity that developed after the Second Lebanon War. Bereaved parents also implied that they would have been willing to accept a higher price (mainly by launching a massive ground operation), as long as it was justified in terms of attaining military goals.[19]

Common to both wings, therefore, is the willingness to sacrifice, provided that the sacrifice is valuable and necessary. Consequently, coffins do not automatically evoke a feeling of revulsion; this feeling depends on the circumstances, as Gelpi and his colleagues assert. In other words, the belief that the fighting is politically essential and achieves its targets will increase the willingness to accept casualties, and vice versa. This is what transpired during Operation Protective Edge.

From the outset of Operation Protective Edge, the government and the IDF did not want a ground operation. The concern about loss of life dissuaded the Israeli leadership from launching a ground operation, under the assumption that it would require an aggressive use of fire power in order to mitigate the risk to IDF soldiers, and subsequently would expose Israel to international criticism.[20] In the final analysis, Israel was dragged into a ground operation, due to Hamas' rejection of the Egyptian ceasefire proposal at the end of the first ten days of fighting. The discovery of the tunnels, perceived as a threat, not only provided legitimacy (and even internal pressures) in both Israel and the international arena for the ground operation, but also enabled the military to focus the operation on a threat with a concrete objective.

Unlike during the Second Lebanon War, the goal of the ground operation during Protective Edge was not to stop the firing of rockets and missiles at Israel's southern population centers. A ground operation with this defined purpose would have failed and would have been portrayed as ineffective, certainly during its initial phases, which would have gnawed away at the justification for sacrificing soldiers' lives. On the contrary, the loss of soldiers' lives during Protective Edge was justified by the need to eliminate a more tangible threat – that of the tunnels – which was presented in the public discourse in a demonic way, strumming chords of fear in the average Israeli.[21]

Any operation to silence the firing on the population centers can be measured for success and failure, and therefore, can garner praise and criticism. In contrast, any effort to remove a future threat is an operation whose success cannot be measured. In the context of Operation Protective Edge, the military efforts to destroy the tunnels and the time it took could all be measured quantitatively. This was a measure of input (destroyed tunnels) and not output (improved security) and facilitated the decision makers' ability to shape public opinion about the efficacy of the operation. Therefore, this kind of project is almost assured of success, and legitimizes the sacrifice by its very nature. Indeed, at the conclusion of the ground operation, 92 percent of the Jewish population in Israel concurred that the ground operation had been justified, while about half of those surveyed believed that most of the goals had been achieved.[22] Even if criticism was voiced during the ground operation, it focused on the time taken to destroy the tunnels and the way the tactical aspects of the operation were managed, but not on the principal justification of the operation or the price it exacted.[23] It is reasonable to assume that if the ground operation had become protracted and the number of casualties had risen, sensitivity leading to opposition would have increased, all the more so had the objective of the operation been to stop the rockets that Hamas launched at Israel's towns, instead of destroying the tunnels. The situation is different when at issue is an operation that last two and a half weeks and has achievable objectives.

In this way, the government played a significant role in shaping the public discourse by severing the failed efforts to stop the rocket fire on Israel's population centers from the seemingly successful efforts to destroy the tunnels. Most of the casualties, forty-four soldiers, fell during the ground operation (the others were killed during attacks on military concentrations outside of the Gaza Strip), but their deaths did not raise questions. Therefore, when the operation to destroy the tunnels had accomplished all that it could and politicians had to choose between ending the fighting and a massive ground incursion to reoccupy the Gaza Strip, which would have cost hundreds of soldiers' lives, they opted for the first alternative.[24]

Under these circumstances, the potential for protest was not high, even after the fighting had ended. If we compare this operation to the Second Lebanon War, we find that during the weeks following the end of Protective Edge and the subsequent declaration of the ceasefire, 70 percent of the Jewish population believed that the operation did not have any impact on Israel's national security or that the operation had made it even worse. During the weeks after the Second Lebanon War, a similar percentage of the Jewish public (68 percent) believed that the war had ended with some or considerable weakening of Israel's deterrence vis-à-vis the Arab world. In other words, the intensity of the criticism after the Second Lebanon War exceeded that which followed Operation Protective Edge, as the majority of the public believed that the security situation had deteriorated after the war, while public opinion on this matter was divided after Protective Edge.[25] The difference between the objectives of both wars and the extent to which the objectives were achieved caused this difference in public opinion, even though, in both cases, Israel had failed in its military efforts to stop the rocket fire, achieving it only by means of a ceasefire arrangement.

Furthermore, during the Second Lebanon War, the deaths of soldiers were accompanied by injuries to civilians and heavy property damage by Hezbollah rocket fire. In other words, this ineffective sacrifice could be seen as unworthy. On the other hand, during Operation Protective Edge, the harm to civilians and their property was limited in scope, mainly due to the effective performance of the Iron Dome missile defense system; seven civilians were killed during Operation Protective Edge (including one foreign worker and one soldier on leave) in contrast to forty-four civilians killed during the Second Lebanon War. Thus, the justification of military casualties was even more removed from the degree of success in eliminating the immediate threat to the civilian population. Using the concepts of Gelpi and his colleagues, "success" had been guaranteed and thus had averted the development of sensitivity to military casualties.

An additional factor also helped legitimize the sacrifice of lives. As shown by a study on the American wars, presenting the enemy's losses and, particularly, the ratio between one's own casualties and those of the enemy help to improve public perceptions of the war's success and soften the negative effect of information about one's own casualties by placing the numbers in a larger context.[26] This was also the case during Protective Edge: extensive coverage of the damage and death caused to the Palestinian side played a role in justifying the deaths on the Israeli side, the number of which was far lower than on the Gazan side. "The IDF spokesman," wrote journalist Raviv Drucker, "wants us to see what is happening in Gaza, because it will show what the IDF is doing, and will reduce public pressure on the decision makers to do something, as if they are not doing anything."[27]

In democracies, justifying military death becomes more complicated when soldiers are perceived as having endangered their lives in order to protect the enemy civilians.[28] At issue are fatalities that could have been avoided had a more aggressive fire policy been used. Therefore, indirectly, the presentation of the enemy's losses weakens the potential for criticism, particularly when the public strongly supports the use of force. During Operation Protective Edge, approximately 93 percent of the Jewish public believed that the IDF had made appropriate use of force or even used too little force.[29] Therefore, one can understand how the impact of images of destruction and death from the Gaza Strip was not mitigated by internal criticism, but rather translated into a sense of success.

The situation described above was the backdrop to the IDF's increasing aggressiveness given the risk to soldiers' lives in densely populated areas during the ground operation. Protecting the soldiers even at the expense of Gazan civilians was paramount.[30] The tendency to transfer risk from soldiers to Gazan civilians increased during this operation in comparison to previous rounds of violence.[31] Israeli politicians and the IDF know that the Israeli public's sensitivity to casualties will accelerate the end of war more than international pressure that is inspired by sensitivity to fatalities among the enemy civilians. As in the past, the tendency to transfer the risk constrained the decision makers to use force only when the international arena deemed it legitimate to implement an aggressive fire policy. In this instance, Hamas' rejection of the Egyptian ceasefire proposal gave legitimacy to this policy, as did the goal of the ground operation to eliminate the tunnels, depicted as a threat to civilian communities in southern Israel.

From another perspective, the higher the sense of threat, the lower the sensitivity to casualties, and the stronger the belief that the use of force is designed to eliminate this threat.[32] True, during Operation Protective Edge, most of the Israeli population was under threat of Hamas' missiles, but it was at a tolerable level. On the other hand, during the Second Lebanon War, only a portion of the population had been under threat by Hezbollah, but it had been so intensive that hundreds of thousands temporarily left their homes and sought refuge in the south. Given that it is difficult to differentiate between the significant levels of threat, this cannot be the main variable that explains the differences between the wars with regard to the attitude toward casualties, particularly, the justification of fatalities during Operation Protective Edge versus the criticism of the large number of deaths during the Second Lebanon War. Thus, the significance of portraying the military operations as successful has a stronger explanatory power.

To recall, the concern about casualties dissuaded the Israeli leadership from launching a ground operation in the Gaza Strip during Protective Edge, under the assumption that such an operation would require an aggressive fire policy in order to mitigate the risk to IDF soldiers, and thereby subject Israel to international criticism.[33] In the end, Israel was dragged into the ground operation as a result of Hamas' refusal to stop the warfare after ten days of fighting. However, the Israeli leadership concurrently created the conditions necessary to diminish public opposition to the loss of soldiers by implementing the aggressive fire policy, which, as stated, transferred a portion of the risk from IDF soldiers to Gazan civilians. As noted, this policy was legitimized by Hamas' rejection of the Egyptian proposal for a ceasefire, and given that the ground operation focused on eliminating the perceived threat posed by the tunnels. Therefore, it is possible that the politicians and the military enjoyed more freedom of operation than they had previously estimated.

3. Casualty sensitivity is influenced by the identities of those being sacrificed, and not only by an "objective" reading of the reality

As previous wars have shown, casualties from among the secular, middle-class groups induce a critical reading of the reality. Such a reading is likely to be translated into casualty sensitivity among these groups, leading to protest, to a greater degree than would losses from among marginal, immigrant or religious groups. In other words, the variables that influence the degree of sensitivity to casualties – a sense of threat, an assessment of the success or failure of the military operation, recognition of the war as being justified, and more – are mediated through the social status of the group interpreting them. Thus, the more affluent the sacrificing group, the higher the likelihood that even a military success will be critically interpreted.[34] Moreover, as already mentioned, sensitivity will motivate more affluent groups to take action, while sensitivity among lower-class groups is likely to lead to passive acceptance of their sacrifice. And indeed, expressions of protest informed by casualty sensitivity were heard in the past in Israel among relatively upper-middle class families.

In this light, a social map of the casualties is necessary.[35] To better understand the significance of this mapping, a comparison between Operation Protective Edge and the Second Lebanon War (during which 119 soldiers died) is warranted, due to the similar composition of the combat force and the high number of casualties, which aroused protest during the Second Lebanon War. The comparison shows that the overall drop in the proportion of casualties from secular middle-class groups, reflecting the overall change in the army's social composition, has basically remained the same. The percentage of casualties from these groups – the groups with a potential for developing antiwar protest – was the same during both campaigns, about half of the deaths, but were about 15 percent less than during the first critical week of the First Lebanon War, which triggered unprecedented protest. Therefore, the argument heard in the public discourse that the bloodshed had been more balanced than in the past was not valid. Indeed, more students who had graduated from elite high schools in Tel Aviv were among the casualties of Operation Protective Edge than during the Second Lebanon War, and two who fell during combat were graduates of elitist pre-military academies. Nevertheless, if we differentiate the veteran agricultural sector (kibbutzim and moshavim) from the urban middle-class, we see a 60 percent drop when comparing the two wars. This figure refuted the prevailing public belief that there had been substantial representation of the kibbutz movement among the casualties of Operation Protective Edge. Even within this movement, most of the fatalities were from among those who had moved to kibbutzim, rather than children of veteran kibbutz families. Moreover, the mapping showed a 25 percent rise in casualties from lower-class groups (including those of Ethiopian origin) during the two wars and an increase of about 50 percent from among the religious population, even though they were mainly from communities inside the Green Line and not settlers (so too, most of the casualties who had graduated from religious pre-military academies were residents of communities inside the Green Line).

Even though the rate of casualties from among secular, middle-class groups had been similar during the Second Lebanon War and Operation Protective Edge, the low absolute number of fatalities from these groups during Operation Protective Edge – 34 versus 63 during the Second Lebanon War – made it even more difficult to form a critical mass to initiate a protest, which, as stated, had little potential from the outset in light of the operation's goals. Moreover, the infrastructure for protest was further weakened because of the low percentage of casualties from among reservists (15 percent in Operation Protective Edge, compared to 45 percent during the Second Lebanon War), with reservists having played a key role in past protests.

The potential for protest might have increased had it focused on incidents of fatalities that could have been prevented, such as by protecting the soldiers in various situations (most blatant was the explosion of an armored personnel carrier in the Shuja'iyya neighborhood of Gaza that had not been properly armored). Yet, as argued above, the low number of casualties from among more affluent groups made it difficult for such a protest to develop.

At the same time, the portrayal of the sacrifice as effective lowered the chances that protest would emerge from the networks of the bereaved religious families, the proportion of which rose, as stated, by about 50 percent between the Second Lebanon War and Operation Protective Edge. During the Second Lebanon War, the bereaved religious families were prominent in protesting their disappointment with the functioning of the army and the government.

4. Casualty sensitivity is influenced by the nature of the model of recruitment

Over the last decade, the conscription model in Israel increasingly has been built on selective criteria. Accordingly, conscription formally applies to the entire population, but also exempts a relatively high percentage of the population, whether on a collective basis (such as the ultra-Orthodox Jews or the Palestinian citizens) or on an individual basis, as typifies the pattern of personal negotiations between conscripts from more affluent groups and the IDF.[36] The selectivity applies not only to the actual conscription, but also to assignment to combat units, which in fact, gradually has become a volunteer service.[37]

As the model of mandatory conscription has weakened, the potential for protest informed by casualty sensitivity is weakened as well, including among the more affluent families and their social networks. In the conscription model, it is the state that is responsible for those whom it has coerced to sacrifice, whereas enlistees in a voluntary and even semi-voluntary force like the case of Israel, seemingly have made a free choice. Therefore, with the state's responsibility decreasing, it is less likely that families will channel their sense of loss into allegations against the state.[38] Indeed, prominent during the operation was the phenomenon of the fallen as having been highly motivated to serve in the IDF: the fallen were not described as soldiers who were assigned to combat units out of compulsion, but rather, as soldiers who did so willingly. The media even glorified their personal bravery, isolated from the question of the price that they had paid.[39] Such a sentiment curbs the parents' ability to oppose military fatalities and fosters reconciliation and acceptance of their deaths. To this, we have to add the effective efforts of the IDF and the education system over the last decade to contend with the eroding motivation for military service, mainly among more affluent groups. The IDF-initiated programs to motivate pupils to perform their army service, the widespread campaign in high schools against draft dodging (mainly since 2007), and the strengthening of the secular/mixed pre-military academies project, and more, are reflections of effective military socialization.

5. The number of casualties has an impact, but not a decisive one

American scholars of casualty sensitivity have debated over the question to what extent did the number of casualties constitute a decisive factor in causing public opinion to oppose military sacrifice.[40] My argument is that the number is not decisive. For the sake of comparison, the War of Attrition in the Suez Canal (1969-1970), which was waged far from Israel's population centers, cost the lives of about 600 soldiers within less than two years, yet aroused little protest. In contrast, the war of attrition in Lebanon (1982-1985), waged a few kilometers from civilian communities in the Galilee, cost the lives of a similar number of soldiers and did arouse protest.

Military operations, which had been widely supported, became controversial, not because of an objective change in the goals of the operations or in the threat they were designated to remove, but rather because of the ability of mainly affluent groups to break loose from the shackles of military thought and to challenge military sacrifice. If we address this factor by comparing the Second Lebanon War to Protective Edge, we will again see that the number had no impact. Although the number of casualties reached 119 and 65 respectively during the Second Lebanon War and Operation Protective Edge, this difference cannot explain the wave of protest by bereaved parents in the former versus the silence and acceptance in the latter. It is more of a polar than a spectrum situation. It follows that the other factors presented in this article played a decisive role in explaining the presence or lack of protest.

Conclusions

The cumulative circumstances created the difference in protests between the Second Lebanon War and Operation Protective Edge. It seems that those same factors that led to the outbreak of protest informed by casualty sensitivity following the Second Lebanon War should have also generated protest after Operation Protective Edge: ambiguous and fluid objectives of war, indecisive performance, failure to prevent rocket fire on civilian communities, surprise by the enemy's capabilities, and mainly, operational failures that caused the deaths of soldiers. The different circumstances of both wars, however, led families of the fallen during Operation Protective Edge to read the reality in a submissive way. These circumstances increased the leadership's ability to legitimize the military death, while weakening the potential for sensitivity that may elicit antiwar protest: the military efforts were portrayed as swift, intensive, and effective; the sacrifice among the secular, middle-class groups was not high; and selective conscription reinforced the voluntary nature of military service.

Israeli society's attitude towards military casualties is, therefore, complicated. The level of sensitivity is higher than it had been before the watershed of the First Lebanon War, and so also the likelihood that antiwar protest will emerge from this sensitivity. This argument is valid, whether social groups actually demonstrate sensitivity or whether state and military leaders believe in the existence of such sensitivity, even beyond its real potential. Specific circumstances determine whether this sensitivity will erupt or remain dormant. The conclusion that the "spider webs" have become denser, and that coffins arouse indifference appears, therefore, too sweeping.

Notes

[1] Gabi Siboni, "Operations Cast Lead, Pillar of Defense and Protective Edge: A Comparative Review," in *The Lessons of Operation Protective Edge*, eds. Anat Kurz and Shlomo Brom (Tel-Aviv: Institute for National Security Studies, 2014), p. 30.

[2] Yarden Skoop, "Lecturers at Tel-Aviv University: 'They are Trying to Impose Silence on Us,'" *Haaretz*, August 26, 2014 (Hebrew).

[3] Zipi Israeli and Elisheva Rosman, "Debts of Honor, Costs of War: The Media's Treatment of the Question of Casualties during Operation Protective Edge," *Military and Strategic Affairs* 7, no. 2 (2015): 33-54.

[4] Breaking the Silence, *This is How We Fought in Gaza: Soldiers' Testimonies and Photographs from Operation "Protective Edge" (2014)*. (Jerusalem: Breaking the Silence, 2015), p.16.

[5] Winograd Committee, *Final report,* p. 106 (Hebrew), http://www.vaadatwino.org.il/reports.html.

[6] Christopher Gelpi, Peter D. Feaver, and Jason Reifler, *Paying the Human Costs of War: American Public Opinion and Casualties in Military Conflicts* (Princeton: Princeton University Press, 2009).

[7] Udi Lebel, "Postmortem Politics: Competitive Models of Bereavement for Fallen Soldiers in Israeli Society," *Journal of Modern Jewish Studies* 5, no. 2 (2006): 163-181.

[8] Yagil Levy, *Who Governs the Military? Between Control of the Military and Control of Militarism* (Jerusalem: Magnes, 2010), pp. 134-144 (Hebrew).

[9] Winograd Committee, *Final report,* p. 252.

10 Meital Eran-Yona and Batya Ben-Hador, "On Casualty Sensitivity: Comparative and Local Perceptions of Commanders and Implications for the IDF," in *Sociological and Psychological Perspectives of Military Operations in Civilian Environments*, ed. Meital Eran-Yona (Tel-Aviv: IDF Behavioral Sciences Center, Bemachane Publishing, 2013), pp.126-142 (Hebrew).

11 Yagil Levy, *Israel's Death Hierarchy: Casualty Aversion in a Militarized Democracy* (New York: New York University Press, 2012), pp. 127-145.

12 See, for example, Martin Shaw, "Risk-transfer Militarism, Small Massacres and the Historic Legitimacy of War," *International Relations* 16, no. 3 (2002): 343-360.

13 Hugh Smith, "What Costs Will Democracies Bear? A Review of Popular Theories of Casualty Aversion," *Armed Forces & Society* 31, no. 4 (2005): 487-512.

14 Edward N. Luttwak, "Toward Post-Heroic Warfare," *Foreign Affairs* 74, no. 3 (1995).

15 Gelpi, Feaver, and Reifler, *Paying the Human Costs of War*.

16 Yagil Levy, "How Military Recruitment Affects Collective Action and its Outcomes," *International Studies Quarterly* 57, no. 1 (2013): 28-29.

17 See, for example, Douglas L. Kriner and Francis X. Shen, *The Casualty Gap: The Causes and Consequences of American Wartime Inequalities* (New York: Oxford University Press, 2010); Levy, "How Military Recruitment Affects Collective Action and its Outcomes," pp. 28-40; Joseph Paul Vasquez, "Shouldering the Soldiering: Democracy, Conscription and Military Casualties," *Journal of Conflict Resolution* 49, no. 6 (2005): 849-873.

18 John E. Mueller, *War, Presidents and Public Opinion* (New York: Wiley, 1973).

19 Levy, *Who Governs the Military*, pp. 151-153.

20 Amos Harel, "Seven Takeaways from Seven Days of Operation Protective Edge," *Haaretz*, July 15, 2014.

21 Assaf Sharon, "Failure in Gaza," *New York Review of Books*, September 25, 2014.

22 Ephraim Yaar and Tamar Hermann, "Peace Index: August 2014," http://www.idi.org.il/media/3676239/Peace_Index_August_-2014-Eng.pdf; Yehuda Ben Meir, "Operation Protective Edge: A Public Opinion Roller Coaster," in *The Lessons of Operation Protective Edge*, eds. Anat Kurz and Shlomo Brom (Tel-Aviv: Institute for National Security Studies, 2014), pp. 131-132.

23 Israeli and Rosman, "Debts of Honor, Costs of War," p. 36.

24 Itamar Sharon, "Cabinet told Purging Gaza of Terror Would Take 5 Years, Cost Hundreds of Soldiers' Lives," *Times of Israel*, August 6, 2014.

25 Ephraim Yaar and Tamar Hermann, "Peace Index: July 2006," www.peaceindex.org/files/peaceindex2006_7_1.doc; Ephraim Yaar and Tamar Hermann, "Peace Index: September 2014," http://www.idi.org.il/media/3714878/Peace_Index_September_-2014-Eng.pdf.

26 William A. Boettcher and Michael D. Cobb, "Echoes of Vietnam? Casualty Framing and Public Perceptions of Success and Failure in Iraq," *Journal of Conflict Resolution* 50, no. 6 (2006): 831-854.

27 Raviv Drucker, "The Media and Operation Protective Edge," http://drucker10.net/?p=2310 (Hebrew).

28 Michael W. Reisman, "The Lessons of Qana," *Yale Journal of International Law* 22, no. 2 (1997): 395-396.

29 Yaar and Hermann, "Peace Index: August 2014."

30 Amos Harel, "What Netanyahu and Hamas Stand to Lose from a Cease-fire," *Haaretz*, July 24, 2015.

31 Yagil Levy, "How Israel Shifted Risk from Soldiers to Gazan Civilians," *Washington Post*, August 18, 2015.

32 Bruce W. Jentleson and Rebecca L. Britton, "Still Pretty Prudent: Post-Cold War American Public Opinion on the Use of Military Force," *Journal of Conflict Resolution* 42, no. 4 (1998): 395-417.

33 Harel, "Seven Takeaways from Seven Days of Operation Protective Edge."

34 Levy, *Israel's Death Hierarchy,* pp. 37-125.

35 The mapping is based on the social origin of the casualties, according to their life stories and the families' stories, as published after their deaths in the electronic press.

36 Yagil Levy, "'The 'People Army' Vs. Conscription," *Law and the Army* 21 (a): 309-340 (Hebrew).

37 Amos Harel, *The New Face of the IDF* (Or Yehuda: Kinneret, Zmora-Bitan, 2013), pp. 44-45 (Hebrew).

38 See, for comparison, Levy, "How Military Recruitment Affects Collective Action and its Outcomes," pp. 28-40.

39 Israeli and Rosman, "Debts of Honor, Costs of War," p. 39.

40 See, for example, Christopher Gelpi, "How many Casualties will Americans Tolerate? Misdiagnosis," *Foreign Affairs* 85, no. 1 (2006):139-144.

China's Strategic Nuclear Arms Control: Avoiding the "Thucydides Trap"

Stephen J. Cimbala

The "Thucydides Trap" refers to the propensity in history for rising states to challenge putative hegemons or other leading powers for international position, sometimes resulting in war. China's growing military and economic power in the twenty-first century challenges American and Russian leadership on international security issues, including nuclear arms control and nonproliferation. Yet strategic nuclear arms reductions have still proceeded in a two-sided framework of US-Russian negotiations. Despite obvious difficulties, China should be brought into the process of US-Russian nuclear arms reductions because China is rising as a nuclear power and moving beyond its Cold War minimum deterrence posture.

Keywords: deterrence, arms control, China, nuclear weapons, missile defenses, Thucydides Trap, New START, modernization

Introduction

Whether the United States and China can avoid the "Thucydides Trap" involves many issues.[1] One of these is nuclear arms control. The United States and Russia should not continue to restrict their conversations about strategic nuclear arms limitation to a two-way street. China's current and prospective military modernization entitles Beijing to a seat at the table of future Russian-American nuclear arms talks. Among other indicators, China continues to improve the capability of its nuclear ballistic missile

Stephen J. Cimbala is Distinguished Professor of Political Science at Penn State Brandywine and has contributed to the fields of international security studies, nuclear arms control, and other issues for many years. An award-winning Penn State teacher, Dr. Cimbala recently authored *The New Nuclear Disorder* (Ashgate Publishers, 2015).

submarines (SSBNs) and submarine-launched ballistic missiles (SLBMs). Along with this, China's fleet of nuclear attack submarines supports an ambitious anti-access and area denial (A2/AD) strategy to deter US military intervention on behalf of allied interests in Asia against Chinese wishes.[2] China's diplomacy also creates for its leaders an additional space to maneuver between Russian and American perceptions of their own interests. On the other hand, China may lack the commitment to arms control transparency, which is needed to become a meaningful participant in the multilateral nuclear arms control.

The "Thucydides Trap" refers to the historical tendency in which challenges, posed by rising powers against existing hegemonic or superior powers, turn into warfare. China's rising economic and military power, together with its political influence in Asia and globally, do not necessarily mean that a war between the United States and China is inevitable. In fact, China's growing nuclear strength could create a situation of mutual deterrence in East Asia, in which neither larger-scale conventional nor nuclear war would be politically advantageous or acceptable. Instead, US-Chinese competition could take the form of economic rivalry supported by military power and diplomatic sagacity. But nuclear deterrence stability in Asia also requires that Russia, the United States, and China must all be included in any enduring nucleararms-control regime for the region.

China as Balancer

As Russian arms-control expert Alexei Arbatov has noted, Beijing's "cautious and multi-vectored" policies "have allowed it to assume the role to which Russia has traditionally aspired – that of a balancer between East and West. In fact, it is Russia, with its new policy of 'Eurasianism,' that has become the East."[3] On the other hand, China's political and military objectives in Asia and worldwide differ from those of the United States and Russia, reflecting China's perception of its own interests and of its anticipated role in the emerging world order.[4]

Entering China into the US-Russian nuclear deterrence equation creates considerable analytical challenges for a number of reasons. First, China's military modernization is going to change the distribution of power in Asia, including the distribution of nuclear and missile forces. China's military modernization draws not only on its indigenous military culture, but also on careful analysis of western and other experiences. As David Lai has noted,

> The Chinese way of war places a strong emphasis on the use of strategy, stratagem, and deception. However, the Chinese understand that their approach will not be effective without the backing of hard military power. China's grand strategy is to take the next 30 years to complete China's modernization mission, which is expected to turn China into a true great power by that time.[5]

China's strategic missile force – the People's Liberation Army Second Artillery Force (PLASAF) – is among the beneficiaries of its military modernization. PLASAF made major strides during the Hu Jintao era, beginning in 2002 when Hu became Secretary General of the Chinese Communist Party (CCP) and President of China. PLASAF's main mission is described in its publications as "dual deterrence, dual operations," responsible for nuclear deterrence and nuclear counterstrikes as well as conventional deterrence and conventional precision strikes.[6] Chinese military publications specify a number of campaign-deterrence missions that might be undertaken by PLASAF in peacetime or in conditions of crisis or war, including war prevention, escalation control, use of nuclear deterrence to "backstop" conventional operations, and strategic compellence of enemies by means of deterrent actions.[7]

Chinese military modernization and defense guidance for the use of nuclear and other missile forces hold some important implications for US policy. First, Chinese thinking is apparently quite nuanced about the deterrent and defense uses for nuclear weapons. Despite the accomplishments of modernization thus far, Chinese leaders are aware that they are far from nuclear-strategic parity with the United States or Russia. On the other hand, China may not aspire to this model of nuclear-strategic parity between major nuclear powers as the key to avoiding war by deterrence or other means. China may prefer to see nuclear weapons as one option among a spectrum of choices available to deter or fight wars under exigent conditions as well as to support assertive diplomacy and conventional operations when necessary. Nuclear-strategic parity as measured by quantitative indicators of relative strength may be less important to China than the qualitative use of nuclear and other means as part of broader diplomatic-military strategies.[8]

Second, China is expanding its portfolio of military preparedness not only in platforms and weapons, but also in the realm of C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) and information technology. Having observed the American success in Operation Desert Storm against Iraq in 1991, Chinese military strategists concluded that the informatization of warfare under all conditions would predicate future deterrence and defense operations.[9] China's growing portfolio of smart capabilities and modernized platforms includes, in addition to items previously noted, stealth aircraft, anti-satellite warfare, quiet submarines, "brilliant" torpedo mines, improved cruise missiles, and the potential to disrupt financial markets. As Paul Bracken has noted, the composite effect of China's developments is to make its military more agile – meaning more rapidly adaptive and flexible.[10]

The importance of agility instead of brute force reinforces the traditional emphasis in Chinese military thinking since Sun Tzu on the acme of skill as winning without fighting – and if war is unavoidable – getting in the first and decisive blows. It also follows that one should attack the enemy's strategy and his alliances, making maximum use of deception based on superior intelligence and estimation. The combination of improved platforms, command-control, and information warfare should provide options for the selective use of precision-fire strikes and cyberattacks against priority targets, and avoidance of mass killing and fruitless attacks on enemy strongholds.

A third aspect of the Chinese military modernization important for nuclear deterrence and arms control in Asia is the problem of escalation control. Improving Chinese capabilities for nuclear deterrence and for conventional warfighting increases the confidence of Chinese leaders in their ability to carry out an A2/AD strategy against the United States or another power seeking to block Chinese expansion in Asia. This confidence might be misplaced in the case of the United States. The United States is engaged in a "pivot" in its military-strategic planning and deployment to Asia, and toward that end, is developing its doctrine and supporting force structure for AirSea-Battle countermeasures against Chinese anti-access strategy.[11]

Another aspect of the problem of escalation control is the question of nuclear crisis management between a more muscular China and its Asian neighbors or others. Asia in the Cold War was a nuclear-weapons backwater, since the attention of American and allied NATO policymakers and military strategists was focused on the American-Soviet arms race. The world of the twenty-first century is very different. Europe, notwithstanding recent contretemps in Ukraine, is a relatively pacified security zone compared to the Middle East or to South and East Asia, while post-Cold War Asia is marked by five nuclear weapons states: Russia, China, India, Pakistan, and North Korea. The possibility of nuclear first use, growing out of a conventional war between, say, India and Pakistan, or China and India, is nontrivial, while North Korea poses a continuing uncertainty of two sorts. It might start a conventional war on the Korean peninsula, or the Kim III regime might implode, leaving uncertain the command and control over its armed forces, including nuclear weapons and infrastructure.[12]

The problem of keeping nuclear-armed states below the threshold of first use, or containing escalation afterward, was difficult enough to explain within the more simplified Cold War context. Uncertainties are even more abundant with respect to escalation control in the aftermath of a regional Asian war. Then, too, there is the possibility of a US-Chinese nuclear incident at sea or a clash over Taiwan escalating into conventional conflict, accompanied by political misunderstanding and the readying of nuclear forces as a measure of deterrence. The point is that American and Chinese forces would not actually have to **fire** nuclear weapons to **use** them. Nuclear weapons would be involved in the conflict from the outset, serving as offstage reminders that the two states could stumble into a process of escalation that neither had intended.

There is an important correction or cautionary note that needs to be introduced at this point. Policy makers and strategists sometimes have talked as if nuclear weapons always serve to dampen escalation instead of exacerbate it. This might be a valid theoretical perspective under normal peacetime conditions. On the other hand, once a crisis has begun, and especially after shooting has started, the other face of nuclear danger will appear. Reassurance based on the assumption that nuclear first use is unthinkable may then give way to its becoming very thinkable. As Michael S. Chase has warned, miscalculation in the midst of a crisis is a "particularly troubling possibility" heightened by uncertainty about messages that the sides are sending to one another, and/or by leaders overconfident in their ability to control escalation.[13]

Methodology and Analysis

A. *Context*

China's geostrategic view and its military modernization do not fit easily into existing models of nuclear conflict. Chinese participation in future evolutions of strategic nuclear arms control, however, will require their military planners to prepare some estimates of the outcomes of nuclear force exchanges; yet nuclear war between China and either Russia or the United States is extremely unlikely. Nevertheless, Chinese as well as American and Russian armed forces will have to plan for unexpected as well as more probable wars. In addition, the nuclear balance matters insofar as China prefers to maintain a secure second-strike capability against the United States or Russia, regardless of the pace of their modernization. The debate within China relative to the modernization of its nuclear force undoubtedly includes arguments about "how much is enough" to accomplish this fundamental mission of assured retaliation under all conditions.

In the discussion that follows, we project Chinese strategic nuclear forces along with those of Russia and the United States to circa 2020-25. There is significant uncertainty about this for China, compared to the United States and Russia, because the latter two powers are tied to New START force deployment levels beginning in 2018. In addition, China's requirements for reconnaissance and early warning, command-control, and targeting are complicated by regional as well as global requirements. NATO and Russia also face regional issues, but NATO and Russia have decades of experience – including former Soviet experience – in assessing one another's nuclear capabilities and intentions as well as in negotiating arms pacts.

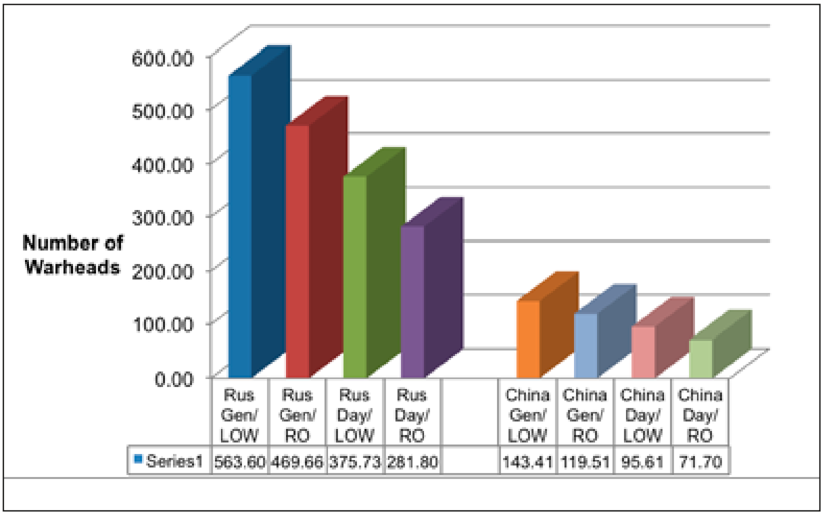
Another asymmetry in this triangle is that Russia and China can inflict "strategic" damage on one another, including attacks on military as well as civilian targets, without necessarily using weapons and launchers of intercontinental range. This recognition is one reason why Russian President Vladimir Putin has put forward the idea of Russian withdrawal from the Intermediate Nuclear Forces (INF) Treaty; only the United States and Russia have denied themselves these weapons, while China and other possible adversaries are free to build and deploy them.[14] Another concern is that China is more opaque about declaring its nuclear capabilities than the United States and Russia and, from China's perspective, it has a number of good reasons for being so.[15]

B. *Analysis*

The analysis that follows necessarily aspires to modesty in creating an analytical structure for a three-sided, strategic nuclear arms competition. For this purpose, we hypothesized: (1) American and Russian New START-compliant strategic nuclear forces, and (2) projected Chinese forces for the same time period, admittedly conjectural, but congruent with expert and government studies.[16] In Chart One, we summarize the results of a nuclear force exchange between Russia and China based on our assumptions about their projected 2020-25 forces. In Chart Two, we provide similar information for a nuclear war between the United States and China. In both cases, the numbers of second-strike surviving and retaliating warheads for each state are summarized under each of four conditions of alertness and launch doctrine: (1) generated alert (Gen) and launch-on-warning (LOW), (2) generated alert, riding out the attack (RO), and then retaliating, (3) day-to-day alert (Day) and launch-on-warning, and (4) day-to-day alert and riding out the attack.

The summaries in Charts One and Two are only illustrative and hypothetical, but nevertheless revealing. China's apparent disinterest in pursuing military-strategic parity with Russia or the United States appears a prudent decision. Although China's prewar projected intercontinental-range nuclear forces are small compared to those of Russia and the United States, they are not negligible. Against New START or similar US and Russian deployment levels, China should be able to guarantee "minimum deterrence" and even more at the end of the decade. Especially important are improvements in China's mobile missile and ballistic missile submarine force, relative to their survivability against surprise attack. Mobile land-based missiles, as seen from the Chinese perspective, increase force survivability and reduce the incentive to launch on warning or preempt, and thereby reinforce deterrence and crisis stability.

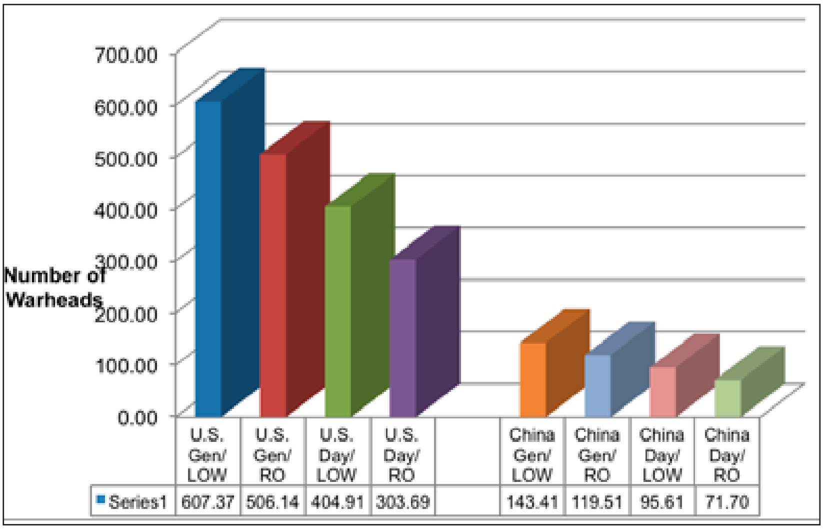
One of the issues that has deadlocked post-New START from Russia's perspective is the NATO plan for deploying missile defenses in Europe, the so-called European Phased Adaptive Approach. China is also concerned about the impact of US global or Asian regional missile defenses on its nuclear deterrent. Therefore, we reanalyzed the outcomes summarized in Charts One and Two above, by calculating the numbers of second-strike surviving and retaliating warheads for each state against opposed missile and air defenses (combined). Since the exact numbers and capabilities of future missile and air defenses are unclear, we established a continuum of possible missile and air defense capabilities, as follows: Phase I, missile and air defenses intercept at least 20 percent of second-strike retaliating warheads; Phase II, at least 40 percent; Phase III, at least 60 percent; and Phase IV, at least 80 percent. Charts Three and Four, immediately below, summarize the offense-defense outcomes for the Russia-China case (Chart Three) and the US-China case (Chart Four).



	Rus Gen/ LOW	Rus Gen/ RO	Rus Day/ LOW	Rus Day/ RO		China Gen/ LOW	China Gen/ RO	China Day/ LOW	China Day/ RO
■ Series1	563.60	469.66	375.73	281.80		143.41	119.51	95.61	71.70

Chart One: Russia-China: Surviving and Retaliating Warheads, circa 2020-25 Deployment Levels

(1) Russian forces at New START agreed levels



	U.S. Gen/ LOW	U.S. Gen/ RO	U.S. Day/ LOW	U.S. Day/ RO		China Gen/ LOW	China Gen/ RO	China Day/ LOW	China Day/ RO
■ Series1	607.37	506.14	404.91	303.69		143.41	119.51	95.61	71.70

Chart Two: US-China: Surviving and Retaliating Warheads, circa 2020-25 Forces

(2) US forces at New START agreed levels

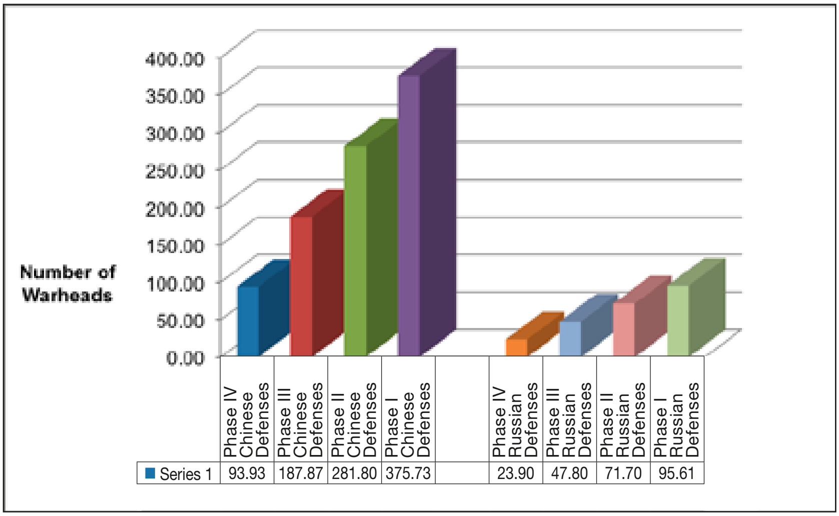


Chart Three: Russia-China: Surviving and Retaliating Warheads vs. Defenses, circa 2020-25 Deployment

Levels (1) Russian forces at New START agreed levels

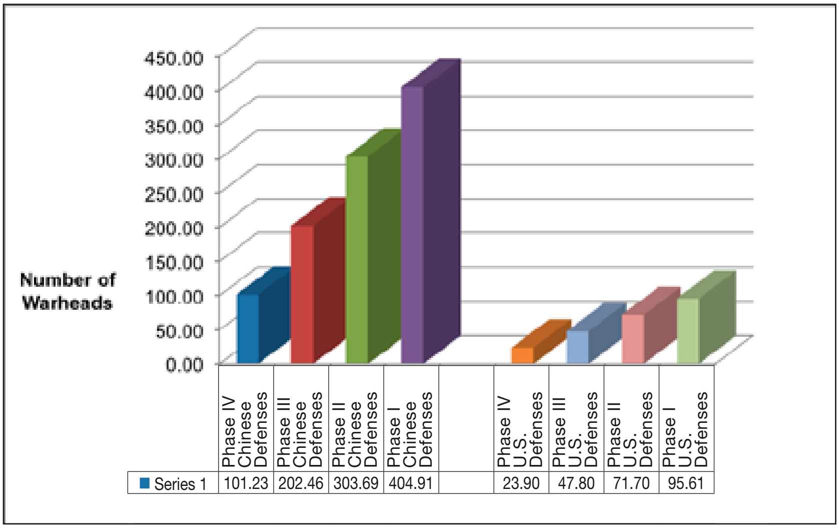


Chart Four: US-China: Surviving and Retaliating Warheads vs. Defenses, circa 2020-25 Forces

(2) US forces at New START agreed levels

The results of the simulations summarized in Charts Three and Four, seen above, are interesting in several respects. First, even with defenses deployed by all three states, the United States and Russia maintain relative nuclear advantage over China with respect to sheer numbers of survivable and deliverable second-strike retaliating warheads. Second, on the other hand, neither the United States nor Russia is able to disarm China in a preemptive nuclear attack without suffering unprecedented and unacceptable retaliation. Third, China's active defenses would be supplemented by passive defenses for retaliatory forces, including systems of tunnels for storing and moving mobile land-based missiles.[17]

Conclusion

China's growing economic power, political ambitions, and conventional and nuclear force modernization suggest that its inclusion in an Asian nuclear arms control regime is overdue. Involving China in multilateral nuclear arms limitation and/or reduction talks is possibly a necessary condition, although admittedly not a sufficient condition for avoiding a "Thucydides Trap" between the United States and China. Indeed, the avoidance of a "triangular Thucydides Trap" in the form of a nuclear arms race in Asia among the United States, Russia, and China is necessary in order to prevent further nuclear proliferation in that region. Toward that end, China is prospectively a meaningful partner for the United States and Russia if they are to go forward with post-New START strategic nuclear arms reductions. China's military modernization and economic capacity create the potential for it to deploy during this decade or soon after a "more than minimum" deterrent sufficient to guarantee unacceptable retaliation against any attack, especially if China's less than intercontinental range forces are taken into account. China's missiles and aircraft of various ranges can inflict damage on Russian state territory and on US-related targets in Asia, including allies and bases. Nevertheless, an open-ended Chinese nuclear modernization in search of nuclear-strategic parity or superiority compared to the United States and Russia is improbable and, from their perspective, pointless. From a broader diplomatic and military perspective, it may be time for a three-cornered, and not a two-sided dialogue on strategic nuclear arms reductions or limitations.

Appendix: Notes on Methodology

Grateful acknowledgment is made to Dr. James J. Tritten, whose forty-four-year career in the US Navy included serving as professor and department head for national security studies at the US Naval Postgraduate School. In that capacity, Dr. Tritten developed a nuclear exchange model based on a spreadsheet that I have since modified, adapted for use as an Excel spreadsheet, and revised the database to account for changes in US and Soviet (and then Russian) forces. A sample output is reproduced below with notional numbers.

The model assists the investigator by calculating formulas and by converting calculations into graphs. The investigator is required to specify the values for force structure, numbers of forces and weapons deployed, estimated performance characteristics of weapons, and other parameters. Dr. Tritten is not responsible for any of the analysis or arguments appearing in this study.

Appendix

Table One: Tritten Model Illustrative Spreadsheet

Russian Forces	Launchers	Warheads @	Total Warheads
SS-11/3	0	1	0
SS-13/2	0	1	0
SS-18	30	10	300
RS-24 silo	0	4	0
SS-19/3	20	6	120
SS-27 silo	60	1	60
sub-total fixed land	110		480
RS-24 mobile	85	4	340
SS-27 mobile	27	1	27
sub-total mobile land	112		367
sub-total land-based	222		847
SS-N-6/3	0	1	0
SS-N-8/2	0	1	0
Delta IV – SS-N-23	64	4	256
Borei-Bulava	64	4	256
Delta III – SS-N-18	0	4	0
sub-total sea-based	128		512

Russian Forces	Launchers	Warheads @	Total Warheads
Bear H6	63	1	63
Bear H 16	0	16	0
Tu-160 Blackjack	13	1	13
sub-total air-breathing	76		76
Total Russian forces	426		1435
US Forces			
Minuteman II	0	1	0
Minuteman III	0	1	0
Minuteman IIIA	400	1	400
Peacekeeper/MX	0	10	0
sub-total land-based	400		400
Trident C-4	0	4	0
Trident D-5/W-76	0	4	0
Trident D-5/W-88	240	4.5	1080
sub-total sea-based	240		1080
B-52G gravity	0	0	0
B-52G gravity	0	0	0
ALCM		0	0
B-52H ALCM	32	1	32
B-2	16	1	16
sub-total air-breathing	48		48
Total US forces	688		1528

Table Two

(Preceding Data in Table One multiplied through matrix of seventeen parameters in order to produce summary descriptors, as below).

Summary descriptors	Numbers
Total Russian deliverable warheads	438.75
Deliverable Russian reserve warheads	175.90
Total US deliverable warheads	583.69
Deliverable US reserve warheads	252.34

Notes

1 For assessments of this concept with pertinent references to the US-China relationship, see Graham Allison, "Just How Likely Is Another World War?" *The Atlantic*, July 2014, http://www.theatlantic.com/international/archive/2014/07/just-how-likely-is-another-world-war/375320/; and James R. Holmes, "Beware the 'Thucydides Trap' Trap: Why the U.S. and China aren't necessarily Athens and Sparta or Britain and Germany before WWI," *The Diplomat*, June 13, 2013, http://thediplomat.com/2013/06/beware-the-thucydides-trap-trap/html.

2 Jeremy Page, "Deep Threat: China's Submarines add Nuclear-Strike Capability, Altering Strategic Balance," *Wall Street Journal*, October 27, 2014, http://online.wsj.com/articles/chinas-submarine-fleet-adds-nuclear-strike-capability-altering-strategic-balance-undersea-1414164738.

3 Alexei Arbatov, "Engaging China in Nuclear Arms Control," Carnegie Moscow Center, October 9, 2014, http://carnegie.ru/publications/?fa=56886.

4 See, for example: Captain Bernard D. Cole, US Navy (Retired), "Island Chains and Naval Classics," *Proceedings of the U.S. Naval Institute* (November, 2014), pp. 68-73.

5 David Lai, "The Agony of Learning: The PLA's Transformation in Military Affairs," in *Learning by Doing: The PLA Trains at Home and Abroad*, eds. Roy Kamphausen, David Lai, and Travis Tanner (Carlisle, PA: Strategic Studies Institute, US Army War College, November 2012), pp. 337-384, citation p. 369.

6 Michael S. Chase, "Second Artillery in the Hu Jintao Era: Doctrine and Capabilities," in *Assessing the People's Liberation Army in the Hu Jintao Era,* eds. Roy Kamphausen, David Lai, and Travis Tanner (Carlisle, PA: Strategic Studies Institute, April 2014), pp. 301-353.

7 Ibid., p. 309.

8 See *Hearing on Developments in China's Cyber and Nuclear* Capabilities *before the U.S.-China Economic and Security Review Commission*, March 26, 2012, (Testimony of Dr. Mark B. Schneider, Senior Analyst, National Institute of Public Policy), http://www.uscc.gov/Hearings/hearing-developments-china%E2%80%99s-cyber-and-nuclear-capabilities.

9 See Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), pp. 39-66; Chase, "Second Artillery in the Hu Jintao Era," p. 331 notes specifically that Second Artillery has benefited from the expansion and improvement in C4ISR capabilities.

10 Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New World Politics* (New York: Henry Holt/Times Books, 2012), p. 206.

11 See Jan Van Tol, Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, *AirSea Battle: A Point-of-Departure Operational Concept* (Washington DC: Center for Strategic and Budgetary Assessments, 2010), http://www.csbaonline.org/publications/2010/05/airsea-battle-concept/.

[12] Kang Seung-woo, "NK could play nuclear option," *Korea Times*, August 12, 2014.

[13] Chase, "Second Artillery in the Hu Jintao Era," p. 340.

[14] Michael R. Gordon, "U.S. Says Russia Tested Cruise Missile, Violating Treaty," *New York Times*, July 28, 2014.

[15] *Hearing on Developments in China's Cyber and Nuclear Capabilities*, p. 2.

[16] For example, see Hans M. Kristensen, Robert S. Norris, and Matthew G. McKinzie, *Chinese Nuclear Forces and U.S. Nuclear War Planning* (Washington, D.C.: Federation of American Scientists and Natural Resources Defense Council, November 2006), esp. pp. 35-46, which includes references to pertinent CIA and DOD assessments; *Hearing on Developments in China's Cyber and Nuclear Capabilities*. For American and Russian forces, see Jon B. Wolfsthal, Jeffrey Lewis, and Marc Quint, *The Trillion Dollar Triad: U.S. Strategic Modernization Over the Next Thirty Years* (Monterey, CA: James Martin Center for Nonproliferation Studies, January 2014); Mark B. Schneider, "The State of Russia's Strategic Forces;" *Defense Dossier* 12 (October 2014):13-18; Hans M. Kristensen and Robert S. Norris, *US Nuclear Forces 2014, Bulletin of the Atomic Scientists*, no. 1, (2014): 85-93; Hans M. Kristensen, "Trimming Nuclear Excess: Options for Further Reductions of U.S. and Russian Nuclear Forces," Special Report No. 5, (Washington, D.C.: Federation of American Scientists, December 2012), http://fas.org/_docs/2012TrimmingNuclearExcess.pdf; Arms Control Association, "U.S. Strategic Nuclear Forces Under New START," July 2013, http://www.armscontrol.org/factsheets/USStratNukeForceNewSTART; Arms Control Association, "Russian Strategic Nuclear Forces Under New START," http://www.armscontrol.org/factsheets/RussiaStratNukeForceNewSTART; Joseph Cirincione, "Strategic Turn: New U.S. and Russian Views on Nuclear Weapons," New America Foundation, June 29, 2011; Pavel Podvig, "New START Treaty in numbers," *Russian strategic nuclear forces* (blog), April 9, 2010, http://russianforces.org/blog/2010/03/new_start_treaty_in_numbers.shtml.

[17] Arbatov, "Engaging China in Nuclear Arms Control." See also Office of the Secretary of Defense, *Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2014* (Washington, DC: US Department of Defense, 2014 and 2013), p. 29.

HUMINT in the Cybernetic Era: Gaming in Two Worlds

Avi Tal and David Siman-Tov

The cyber era has caused enormous changes in intelligence and intelligence gathering. This article discusses whether the profession of human intelligence (HUMINT) is currently still relevant when cyberspace constitutes the main scene for intelligence gathering and action. If so, what missions should it assume, and are new opportunities being created for new operational methods in the cyber era? The article examines the substance of the HUMINT discipline and the challenges that cyberspace poses to this discipline. It also addresses the potential contribution of HUMINT in the cybernetic era, and raises the question whether it constitutes a new intelligence discipline. The first part of this article presents the HUMINT up until the cyber era. The second part discusses HUMINT in the cybernetic era, with an emphasis on its opportunities and risks, its changes, and presents a proposal for a new concept of the HUMINT profession in the cybernetic era.

Keywords: human intelligence, intelligence, intelligence gathering, cyber, intelligence community, cybernetic human intelligence, avatar

Introduction

Cyberspace has transformed the world into a global village. Cyberspace provides instant access to colleagues and rivals, friend and enemies, while transcending borders and languages. Public, open source information, as well as classified and encoded, all pass through cyberspace, which is also a key platform for command and control of systems and weapons. The social networks, blogosphere, and the new media have become the main mass platform for discourse and action in all spheres of life.[1] Almost everyone

David Siman-Tov is an intelligence researcher at the Institute for National Security Studies. Avi Tal is a former senior officer in the Arab Section of the Israel Security Agency.

now has a personal homepage on the Internet, and almost everyone uses the Internet to express their beliefs and desires regarding personal and professional matters. At the same time, cyberspace has led to the creation of threats of cybernetic attacks, which can sometimes have kinetic effects. The social networks have become an important platform for organizational efforts, as we saw with the "Arab Spring," as well as for incitement, as we have seen in the campaign that has led to current wave of knife attacks in Israel. The amount of public information is enormous and continually growing; at the same time, some cybernetic areas are difficult to penetrate.[2]

The cyber era has generated prodigious changes in intelligence and gathering of intelligence. These changes have led to questions about whether human intelligence (HUMINT) is still relevant when cyberspace is an important scene of action, and if so, whether opportunities for new modes of action are being created. The purpose of this article is to consider the nature of HUMINT in the cybernetic era, with an emphasis on the changes that have taken place in its concepts and methods of operation in comparison to the classic profession of HUMINT. The first part of the article presents HUMINT up until the cyber era. The second part discusses HUMINT in the cybernetic era, with an emphasis on its opportunities and risks, and the changes encountered. Finally, we present a proposal for a new concept of the HUMINT profession in the cyber era.

Classic HUMINT

From the dawn of history until the beginning of the twentieth century, intelligence agencies relied exclusively on information from human sources. Sun Tzu, a Chinese general from the sixth century BCE, wrote about spies and their importance in war.[3] Some regard the classic HUMINT profession as an art because it requires its practitioners to have great skills in interpersonal communications, broad general knowledge, familiarity with the psychological-philosophical study of human behavior, as well as the ability to be a jack-of-all-trades, and to be able to persuade, convince, and motivate people.

There are three key stages in the HUMINT profession. The first is locating and selecting the people needed on the basis of personal talents and qualifications, motives (existing and potential), and accessibility (for recruitment and being handled). The second stage is the actual recruitment of the people, for which various and diverse methods can be used: planned recruitment, direct recruitment, indirect recruitment through an undercover collaborator, chance recruitment, and recruitment of volunteers.[4] The third stage is handling and operations. A physical clandestine meeting is very important in creating trust and a personal affinity with the agent, and the related operational aspects of handling the agent (a test of courage, providing weapons, special teaching and training, and so forth).

Classic HUMINT was originally a simple human activity.[5] Recruiting and handling were based mainly on physical meetings, due to an almost complete absence of remote access. The process of locating people relied on limited and relatively inadequate intelligence, while the ability of the recruiters to select good agents was limited. In this physical world, the recruiting and handling required undercover action vis-à-vis the recruit and the surroundings while the system had to completely adapt to the recruit and his environs according to his cover story. These had to meet the physical test: the handler, the support players (including security), the location, lighting, language, and so forth. This situation created many risks for the security of the operation, the agent handlers, and also the agent. Equipping the agent with tools for covert actions increased the risk and constituted an incriminating signature.

The status of HUMINT in the western intelligence community faded from the 1970s onward,[6] as a result of the technological developments and the massive shift by people and armies to using electromagnetic space. This shift caused the rise of technological intelligence gathering; an increase in the contribution of geospatial intelligence through the use of satellites and cyberspace; and an enormous surge in the quantity of open source intelligence (OSINT). The conclusions of the investigatory committees that probed the September 11, 2001 terrorist attacks in the United States and the failure of US intelligence in Iraq were a turning point in the American intelligence community. These conclusions cited a lack of precise information about the al-Qaeda organization – the kind of intimate knowledge that HUMINT is designed to provide. As a result, it was understood that HUMINT had to resume its central role in the US intelligence efforts. One example of an effective and recent contribution by HUMINT to American intelligence gathering was in the hunt for al-Qaeda leader Osama bin Laden. The CIA recruited a Pakistani doctor who administered a vaccination to bin Laden's family members in their compound so that he might be able to obtain a DNA sample from Bin Laden to confirm his presence.

HUMINT in the Cybernetic Era

In the discourse on intelligence gathering in the cybernetic age, one approach is that the intelligence community should not rely only upon cyberspace for intelligence gathering. There is no substitute for HUMINT if the intelligence picture is to be comprehended as a whole, especially for organizations like ISIS and Hamas, which have a low cyber signature; total reliance on technological intelligence in obtaining accurate information about them is inadequate and questionable.[7] One approach holds that only when the extent to which intelligence gathering has penetrated into all aspects of life becomes apparent, then countries and organizations should seek to reduce the level of their intelligence signatures through messengers and work meetings.

In the theoretical discourse on HUMINT in the cybernetic age, some have proposed to broaden the HUMINT concept by combining it with the concept of "social engineering." This would mean creating a false identity for the purpose of recruiting human sources in order to influence them to act in a desired way. The combining of HUMINT and social engineering could fail to achieve HUMINT's existing advantages by channeling it into a single field, that of information security, in addition to losing the inherent potential of offensive cybernetic HUMINT.

The development of cybernetic HUMINT began in the middle of the preceding decade as agents turned to cybernetic tools; first and foremost, they turned to the Internet, and mainly to online forums where they operated under their own names or under aliases. The next stage of cybernetic HUMINT was the creation of fake identities and assumed names, led by a team of people from different disciplines. The team directed these personas to various forums, penetrating areas where existing agents were unlikely to operate. This stage was the result of accelerated technological development in recent years, which has made it possible to create identifies without limitations. In the Israeli context, this method makes it possible to move away from monitoring and foiling "knife terrorism" – currently being practiced and whose effectiveness is questionable – to actively and proactively reducing the incitement that leads to this type of terrorism and influences public opinion.

An internal contradiction exists ostensibly between the classic HUMINT manner of handling agents and that based on handling agents in cyberspace. Classic HUMINT includes holding personal meetings to create trust and personal affinity; developing close, intimate, and long-term relationships;

and hierarchical relations similar to employer-employee relations, including material and non-material remuneration. This is in addition to developing the handling from a long-term perspective, conducting reliability checks, providing training and weapons, and so forth. Cybernetic HUMINT, on the other hand, is based on relations that are not necessarily permanent, with a lower degree of commitment and loyalty, while the connections between the handler and his sources are not deep nor based on direct human connection.

Classic HUMINT involves intimate personal contact facilitating a direct emotional language that creates a connection and closeness beyond shared interests. In cybernetic HUMINT, handling is based on a convergence of interests. As a result, the level of commitment in classic HUMINT is higher, and the agent is more likely to take actions that will endanger him. In cybernetic handling, on the other hand, the level of risk to the agent is much lower. Furthermore, the direct physical meeting with agents is a critical element in creating a personal affinity, important in almost every aspect of handling and operations. The physical contact, the eating and drinking together, and so forth create a special connection that contributes to the agent's motivation. Cyberspace, on the other hand, makes it possible to conduct a virtual meeting that has some similarities to a physical meeting. All that a virtual meeting requires is that it be conducted with minimum risk and without incriminating signatures.

In the cybernetic HUMINT era, the candidates for recruitment are diverse and almost unlimited. Intelligence required for locating them can be obtained quickly, the selection is broad, and access is easy. Furthermore, cyberspace makes it possible to conduct the recruitment and handling stages with relatively little risk, at almost no cost, and with almost no effort, with the help of impersonation or anonymity, including multimedia meetings. Connecting with individuals and groups can be done easily, without any physical danger. Cybernetic HUMINT is groundbreaking and significantly improves the ability of HUMINT personnel to reach remote target audiences that are difficult to recruit. Cyberspace also gives the investigative personnel additional tools to verify the reliability of agents and double check the interrogation of suspects. For example, checking the reliability of a person being interrogated can be done using the information he shared on Facebook. The problem of anonymous sources who are unknown to the handler seems insignificant when the information is intended for research and understanding social currents. On the other hand, this question is acutely significant when the information is needed for counteraction or another operation liable to endanger human life.

The cyber era makes it possible to vanish into the vast sea of information and under assumed identities and roles, thereby substantially ensuring safe communications with agents. Given the varied capabilities for transmitting information through cyberspace and the ability to rapidly transmit large volumes of information, cyberspace has improved the possibilities of communication between agents and collaborators. In the past, agents had to fill cases, luggage, or boxes with material and deliver it to their handlers, at great risk to both parties. Today, a USB drive is enough to enable agents to transfer large amounts of multimedia information of even higher quality. Although cyberspace has reduced the need for face-to-face meetings, thereby diminishing the risk to both parties, at the same time, active intelligence activity in cyberspace has a signature that is liable to constitute a threat in the short or long term. Indirect risks are also increasing as supervision, monitoring, and discovery actions in cyberspace are being stepped up.

Cybernetic HUMINT can penetrate the enemy's cyberspace, such as open or closed forums, and join them passively or actively – in order to extract information. Cybernetic agents can actively exert their influence by recruiting the enemy's agents for the purpose of gathering information; directing agents to act in the physical world; or by affecting public opinion, such as by forging opinions against the delegitimization of Israel (BDS) in relevant forums. Cyberspace can also be utilized to create false rumors about a person in order to attack him – a kind of "cybernetic shaming." In addition, the potential of cybernetic HUMINT for influencing and shaping the enemy's cyberspace is vast, as a result of the open and civilian character of the cyber era. It is important to stress in this context that many intelligence organizations are already operating in the cybernetic sphere, and that the cybernetic personas of these organizations can be located. This makes it possible to engage in cooperative efforts and forge mutual synergy with foreign intelligence organizations that share common interests. At the same time, it should be taken into account that hostile groups or enemies will manipulate cyberspace by using "cybernetic double agents" who will feed false information to intelligence agencies.

In the civilian cyberspace, the "avatar" image – a representation of a user in cyberspace through an imaginary graphic icon, like an actor in a play or a movie, is prevalent. By using avatars, a person could have an unlimited number of identities, and could rapidly create an image and assumed identity for almost any scenario and without complicated operations that require many resources. American intelligence has warned about the use of digital avatars for terrorist purposes, such as Osama Bin Laden's avatar for mass recruitment of terrorists.[8] *Washington Post* reporter Robert O'Harrow wrote about making the spies' battlefield a virtual one, citing as an example a businessman's avatar in the field of games. He notes that intelligence sources understand the potential of the avatar for purposes of terrorism and crime.[9] The handling of avatars of various types and volumes plays a key role in cybernetic HUMINT, including the use of avatars developed in civilian companies, such as an avatar agent for verification testing,[10] a voice-based verification testing device,[11] and polygraph applications[12] used to assist in interrogations and reliability tests.

Actions for Consideration by the Intelligence Community

The field of cybernetic HUMINT integrates the handling characteristics of HUMINT and cyberspace. This combination gives rise to new groundbreaking opportunities that the traditional HUMINT had reserved only for itself. It is too early to tell whether a new discipline has emerged, but the combination of the two, with new concepts and practical features requires an innovative synergy between the clandestine environment and the civilian-commercial environment. This has great potential, both for obtaining intelligence from new communities more quickly and on a larger scale, as well as for influencing the adversaries' social networks and cyberspace.

In the cyber era, HUMINT has experienced substantial changes, led by the introduction of a new sub-profession, which we have referred to as "cybernetic HUMINT." In addition to the need for principles similar to those of traditional HUMINT, cybernetic HUMINT has new features, and does not require direct contact with the sources. This understanding requires organization of all the aspects of building the intelligence force, with an emphasis on training intelligence personnel; in addition to human sensitivity, intelligence personnel need to acquire social sensitivity.

The principles of the HUMINT profession from the period before the cybernetic era form the classic intelligence-gathering profession. The development of this profession in the cyber age emphasizes the change and innovation of this era. The question of the ostensible contradiction between the two types of HUMINT professions – the classic and the cybernetic – was examined, and a number of differences between them can be pointed out:

1. Classic HUMINT requires proximity and direct meeting with the source. In contrast, in cybernetic HUMINT sources can be handled without the handlers knowing their identity, at least up to a certain point.
2. The ability to cross borders is limited in classic HUMINT. In cybernetic HUMINT, borders can be crossed and sources can be handled in remote areas as well.
3. Classic HUMINT focuses on gathering information. In cybernetic HUMINT, the public opinion of the adversary can also be influenced through psychological warfare.
4. In classic HUMINT, the search for agents is limited, and it is difficult to obtain information about the candidates for recruitment. In cybernetic HUMINT, the search for agents is virtually unlimited, with most of those recruited volunteering information and revealing themselves on their own free will.
5. In classic HUMINT, handling incurs great risk for both the handler and the agent being handled. Cybernetic handling, on the other hand, is ostensibly safer, and does not incur risk, although cybernetic handling leaves signatures.
6. In classic handling, the enemy's physical space is given. In cybernetic handling, on the other hand, the enemy's cyberspace can be influenced and shaped.
7. Classic HUMINT is based on human sources and human handlers. In addition to human handling, cybernetic HUMINT is also based on the imaginary personas on both sides, and on computer-generated personas.

In the cyber era, the cooperation between intelligence-gathering disciplines has become stronger. Cyber intelligence and Signals Intelligence (SIGINT) provide intelligence for HUMINT for locating and recruiting, accessing and handling, and gaining operational opportunities, in addition to providing an umbrella of security for its activity. HUMINT provides SIGINT and cyberspace intelligence with leads, which enable them to intercept and monitor intelligence and gain access to information channels, databases, and end-user equipment that is not provided by Internet and by the new type of agents.

It is important for the HUMINT discipline in the intelligence community to monitor the achievements of the civilian industries and companies engaged in cybernetic research, development, and the operational field,[13] and to adapt the HUMINT profession to the challenges of the new era. In addition, the intelligence community should conduct a continuous dialogue with civilian industries and companies in this area as significant HUMINT technologies and capabilities have been created by the private sector from which the defense establishment can and should learn, rather than trying to develop the tools and methods itself. Such a dialogue will significantly augment HUMINT capabilities for coping with the challenges ahead.

Notes

[1] Andrew Shapiro, "Is the Net Democratic? Yes – and No," World Media Forum, Berkman Center for Internet and Society at Harvard University, http://cyber.law.harvard.edu/shapiroworld.html.

[2] Amit Steinhart, "The Future is behind us? The Human Factor in Cyber Intelligence: Interplay between Cyber-HUMINT, Hackers and Social Engineering," *Cyber Guard*, 2014, http://diplomacy.bg./archives/1190?lang=en.

[3] Sun Tzu, *The Art of War*, vol. 13, *The Use of Spies*. Trans. Lionel Giles, http://classics.mit.edu/Tzu/artwar.html.

[4] Volunteers constitute both a risk and an opportunity, because the character is unknown and their intentions have not been verified. They can be swindlers and charlatans, acting out of real and varied motives, or as enemy agents planning to penetrate intelligence ranks as double agents. They can become the best agents, and can also lead us to the brink of disaster. An article by researcher Katherine Herbig analyzes the changes in the methods of espionage in the United States during 1947-2007. See Katherine L. Herbig, *Changes in Espionage by Americans: 1947-2007* (Defense Personnel Security Research Center, March 2008), https://www.fas.org/sgp/library/changes.pdf.

[5] Yehoshafat Harkabi, *The Intelligence as a National Institute (*Tel Aviv: IDF Publishing House and Israel Intelligence Heritage and Commemoration Center, 2015), p. 173, http://www.terrorism-info.org.il/Data/articles/Art_20896/arkabi_1008526679.pdf.

[6] Julien Babanoury, "Where Does HUMINT Fit in with the 21st Century Intelligence Community?" September 8, 2014, http://www.secuinsight.fr/2014/03/03/where-does-humint-fit-in-with-the-21st-century-intelligence-community-by-julien-babanoury-ceis/.

[7] Gabi Siboni, "Cyber Tools are not a Substitute for Human Intelligence," *Haaretz,* July 2, 2014, http://www.haaretz.com/opinion/.premium-1.602413.

[8] Sara Malm, "A Threat for the Digital Age – An Avatar Osama Bin Laden: U.S. Intelligence Warned Terrorists Could Create Virtual Jihadist To Preach and Issue Fatwas for Hundreds of Years," *MailOnline*, January 9, 2014, http://www.dailymail.co.uk/news/article-2536440/A-threat-digital-age-avatar-Osama-bin-Laden-U-S-intelligence-warned-terrorists-create-virtual-jihadist-preach-issue-fatwas-hundreds-years.html; David Kravets, "US Intel: Bin Laden Avatar Could Recruit Terrorists for Hundreds of Years," *Wired*,

January 9, 2014, http://www.wired.co.uk/news/archive/2014-01/09/osama-bin-laden-avatar.

[9] Robert O'Harrow Jr., "Spies' Battleground Turns Virtual," *Washington Post*, February 6, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/05/AR2008020503144.html.

[10] AVATAR – Automated Virtual Agent for Truth Assessments in Real-Time, University of Arizona, 2015, http://borders.arizona.edu/cms/projects/avatar-automated-virtual-agent-truth-assessments-real-time.

[11] Amir Liberman, The LVA (Layered Voice Analysis) Technology, nemesysco, http://www.nemesysco.com/technology-lvavoiceanalysis.html.

[12] Android apk Polygraph Lie Detector Version 1.0 Free Download, 2014, http://appdownload.m5f.net/apk/com.ciberdroix.polygraph.html.

[13] For example, an Israel cyber intelligence company operating an avatar: https://www.sensecy.com.

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for publication in *Military and Strategic Affairs*, a refereed journal published three times a year in English and Hebrew and edited by Gabi Siboni, Director of the Military and Strategic Affairs Program and Cyber Security Program at INSS.

Articles may relate to the following issues:

- Military and strategic thinking
- Lessons learned from military organizations throughout the world
- Military force developments on various subjects, including: human resources, weapon systems, doctrine, training, command, and organization
- Ethical and legal aspects of war and combat
- Military force deployment and operations
- Civil-military relations and decision making processes
- Security/military technology
- Cyber security and critical infrastructure protection
- Defense budgets
- Intelligence
- Terrorism

Submitted articles should not exceed 6000 words (including citations and footnotes), and should include an abstract of 120 words and a list of up to 10 keywords. Only original material that has not appeared in another publication or is under consideration for publication elsewhere may be submitted. Previous issues of the journal may be accessed on the INSS site at: http://www.inss.org.il/.

For further information, please contact:
Hadas Klein
Coordinator
Military & Strategic Affairs Program
Cyber Warfare Program
Tel: +972-54-451-0411
hadask@inss.org.il