Military and Strategic Affairs

Volume 5 | No. 1 | May 2013

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 5 | No. 1 | **May 2013**

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.

Journal Coordinator
Daniel Cohen

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 61398 • 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)

Legal Transparency as a National Security Strategy

Yoni Eshpar

The act of taking initiative is considered the preferred modus operandi within the various spheres that shape and define the concept of Israel's national security: on the battlefield and in diplomacy, as well as on the media front. Conventional wisdom within all these spheres is that one should not be dragged along by the force of events, nor should one ever allow an adversary to define the terms of the battle. The legal realm, however, would appear to be an exception to this rule. Although recognition of its importance has greatly increased in recent years, thinking on the subject remains limited to the defensive and reactive; in other words, thinking is limited to the question of how to furnish the political and operational echelon with professional advice and the proper means of defense against court petitions, lawsuits, commissions of inquiry, and other legal proceedings in Israel and abroad. These are important tasks, but is it the sum total of the law's ability to contribute to security? What about a more comprehensive legal strategy that is more proactive and takes the initiative? What benefit, if any, would it have, and at what price? This article addresses these questions by reviewing the public legal campaign, unprecedented in form and scope, waged by the Obama administration throughout its first term.

This campaign did not include newspaper ads or viral videos on social networks. The message was conveyed in a series of speeches by the most senior legal officials in the administration. One after another – and occasionally more than once – they presented to the public, in a clear and detailed manner, the "legal vision" that guides the administration's

Yoni Eshpar is director of the Public Department at Gisha, an Israeli non-profit organization. The views presented in this article are the author's alone.

national security policies, and in particular the war it is waging against al-Qaeda and its subsidiaries around the world.

This article will not offer a legal analysis of the content of the speeches or presume to take sides in the ongoing debate between the administration and its critics on legal positions regarding military and security issues. The basic assumption of this series of speeches asserted that such a discussion is unavoidable and even essential in any democratic country. The problem is that when it heats up, particularly in wartime, the debate is liable to frame the tension between security and values as an inevitable choice between them. Obama identified this "false choice" as an obstacle and vowed to work toward eliminating it. He did not foment a revolution in the administration's legal positions for this purpose; instead, he redefined the ideological framework in which the public debate on these positions is conducted. The article will analyze this framework and explain why it has proven itself to be an effective means of bolstering security as well as the law and the values that the law represents. In conclusion, it proposes lessons to be learned and outlines directions for thought and action that are relevant for Israel.

Eliminating the False Choice

In January 2008, presidential candidate Barack Obama stated that "ever since 9/11, this administration [the Bush administration] has put forward a false choice between the liberties we cherish and the security we demand." He warned that the winds blowing from the White House for eight years had led the United States into a crisis of legitimacy, both domestically and internationally, which had severely damaged the country's standing and capacity to fight terrorism effectively. Several months after his election to the presidency, Obama presented his alternative in a speech he delivered at the National Archives on May 21, 2009.[1]

At the basis of the credo he presented at length at the National Archives was the assertion that his highest responsibility as president to safeguard the security of the American people does not contradict his obligation to safeguard the democratic values and the universal moral values defined in the US Constitution and American and international law. What is needed, according to Obama, is not a balance between security and values, but determination not to compromise on either of them, with the understanding that in the long run, they reinforce each other and are

essential to one another. He stressed that maintaining these principles is not a luxury, and complying with the law is not a burden, but that "our values have been our best national security asset," especially during wars against an elusive enemy that is not bound by the same laws and values.

Obama provided a number of examples of the manner in which steadfast loyalty to values translates into tangible security benefits. The more the United States maintains its positive moral image, he explained, the closer the cooperation it enjoys with its allies and the easier it is for it to recruit new ones. In such a situation, it is easier to promote American interests in international institutions, it is more difficult to incite public opinion against the United States through anti-American propaganda, and America's enemies have a harder time recruiting fighters and garnering the popular support that is essential to their struggle. American military actions pass muster with the courts and with Congress more easily and trigger less opposition and protest at home and abroad. The President also explained how his unequivocal ban on torture would not only remove a moral stain, but would also encourage enemy fighters to turn themselves in, allow friendly states to turn prisoners over to US authorities for interrogation, and ultimately improve the quality of the intelligence gathered.

The second half of the speech was devoted to another area in which Obama wished to distinguish himself from his predecessor: transparency. The conflict with an enemy like al-Qaeda understandably raises complex ethical questions. The manner in which Obama proposed to deal with these questions was to explain everything that could be explained and to invest time and resources in persuading Americans to have faith in the decision making processes and in the mechanisms designed for oversight of actions taken on behalf of their security. For this reason, the President included in his speech a promise never to hide the truth just because it is inconvenient, and always to inform the public of the reasons underlying his decision to reveal information or to conceal it from the public. Maintaining secrecy more transparently leads to fewer suspicions and conspiracy theories of the type that were rife during the Bush administration, when "Americans often felt like part of the story had been unnecessarily withheld from them." These words echo President John F. Kennedy's speech on freedom of the press in 1961, in which he spoke about the fact that "the dangers of excessive and unwarranted concealment of pertinent facts far outweighed the dangers which are cited to justify it."[2]

In Obama's view, the two major topics in the speech, legality and transparency, play a dual role: they serve as essential checks on those with power and authority, but they are also a source of legitimacy that is no less essential for them. In his view, as long as the public perceives legality and transparency to be antithetical to security, the country will remain in a state in which its democracy is fragile and its freedom of action limited. This is how he described this situation:

> We see that, above all, in the recent debate—how the recent debate has obscured the truth and sends people into opposite and absolutist ends. On the one side of the spectrum, there are those who make little allowance for the unique challenges posed by terrorism, and would almost never put national security over transparency. And on the other end of the spectrum, there are those who embrace a view that can be summarized in two words: "Anything goes." Their arguments suggest that the ends of fighting terrorism can be used to justify any means, and that the President should have blanket authority to do whatever he wants—provided it is a President with whom they agree . . . Both sides may be sincere in their views, but neither side is right. The American people . . . know that we need not sacrifice our security for our values, nor sacrifice our values for our security, so long as we approach difficult questions with honesty and care and a dose of common sense.

However, if the new President had expectations that he would succeed in reframing the debate in one speech, he was most likely disappointed. By the right wing opposition, his statements were seen as confirmation of the claim that his approach to counterterrorism was soft and ineffectual; the response from human rights organizations was no less chilly. In his book *Kill or Capture*, journalist Daniel Klaidman described a meeting Obama held with central figures in the American human rights community one day before the speech, where he set out the main points of his theory. According to the report, the event ended on a discordant note. The attendees, who were also invited to watch the President's speech the following day, elected not to come.[3]

The "Canonical" Speeches

In his Nobel Prize acceptance speech in December 2009, Obama reiterated the benefit of compliance with the law during wartime.[4] However, the conceptual change he was attempting to promote began to be felt only when speeches gradually began to be delivered by other prominent figures from the administration's legal team. They all used the President's speeches as a starting point, quoting them extensively, but each speaker expanded the discussion of the legal and ethical issues pertaining to his area of responsibility, or which were in the headlines at that time.

The first of them was Harold Koh, State Department legal advisor and former dean of Yale Law School, and a well established and respected figure in the human rights community. The detailed speech[5] he delivered in March 2010 at the annual meeting of the American Society of International Law, one of the world's most important forums among experts in international law, was intended to give additional legal content to the framework defined by the President. Koh's main argument was that the administration is unreservedly committed to international law in all its counterterrorism activities. At that time, it had become clear that Obama was dramatically stepping up the use of targeted killings by means of unmanned aerial vehicles (UAVs), even outside the Afghan battlefield, and this was provoking mounting criticism. Koh brought his professional and moral authority to bear, claiming that these actions were not in contravention of international law, and from certain legal perspectives, they were even preferable to other methods.

From Koh's speech onward, a set pattern can be identified. Every time there was a legal or public dispute about actions taken by the administration or by military forces, a senior official publicly presented the administration's legal case. This series of speeches created a platform for the administration's lawyers that allowed them to respond directly to criticism in simple language and within the context of a broad legal framework and an ongoing public process. In this spirit, several months after Koh's speech, Assistant Attorney General David Kris, who worked under Attorney General Eric Holder, explained in a speech[6] to the Brookings Institution the administration's position on another controversial topic: prosecuting foreigners accused of terrorism in federal courts. After Osama Bin Laden was killed, Koh published a post in a leading legal blog in which he explained why the action was lawful.

It was not just legal advisors who took part in the campaign. In order to neutralize the claim of a tradeoff between security and values, it was not enough for respected lawyers to talk about security; it was also necessary for respected security figures to persuade people that the law is not a burden, but rather a security asset. John Brennan, assistant to the President for homeland security and counterterrorism, was the perfect man for this mission. With a long career in the CIA behind him and the look to match, Brennan became one of the main bearers of the message. In September 2011, he delivered a speech[7] at Harvard Law School whose title sums up its contents: "Strengthening our Security by Adhering to our Values and Laws." Shortly thereafter, the microphone returned to the lawyers, when Jeh C. Johnson, general counsel of the Department of Defense, delivered two speeches only four months apart – in October 2011[8] and February 2012.[9]

Johnson reviewed the administration's efforts and its successes in improving the legal framework so that it would furnish the tools with which to confront threats of the kind posed by terrorist groups, and at the same time maintain the necessary separation between the military and the civilian justice system. He addressed such sensitive subjects as prolonged military detentions and the legality of extra-judicial targeted killings of American citizens who have joined al-Qaeda. In the second speech, Johnson addressed the rumors that there were serious differences of opinion between him and Harold Koh, and confirmed the existence of disagreements among the various advisors. He suggested that they be viewed as proof of the complexity of the legal challenge and the seriousness of the attempts to confront it. Whether intentionally or not, these speeches all gave the impression that legal positions on some of the most complex issues, even when they were crystallized and agreed upon, had not been formulated without anguish and misgivings.

The next speaker was Attorney General Eric Holder, who of all the speakers is possibly the closest to Obama personally. In March 2012, he delivered a speech[10] at Northwestern University Law School in which he addressed, inter alia, the criticism of the government's wiretapping program and clarified several of the legal positions mentioned by his predecessors. The surprise in this series of speeches came a month later, when the Central Intelligence Agency also joined the "legal transparency offensive."[11] Stephen W. Preston, general counsel of the CIA, claimed in a detailed public speech[12] – uncharacteristic of the covert agency – that

the CIA's actions are also subject to the same ethical principles and to American and international law.

In late April of that year, following public criticism of the program of targeted killings, President Obama sent Brennan out to speak again.[13] This time, he focused on attempting to convince his listeners that the program operates according to a set of strict standards and procedures and is under the direct oversight of the President in order to ensure the legality of every action and reduce mishaps and errors to a minimum. According to Brennan, "the United States government has never been so open regarding its counterterrorism policies and their legal justification."

At this stage, commentators could no longer ignore the series of "canonical speeches"[14] that began with the address by the President and continued with the speeches by senior legal advisors in the State Department, the Department of Defense, the Department of Justice, the CIA, and of course, the speeches by "Mr. Security," John Brennan. Few people doubted that it was being closely coordinated by the White House. According to one description, it was Avril Haines, legal advisor to the National Security Council, who participated in drafting and coordinating the speeches.[15]

The next speech,[16] delivered in September 2012 by Harold Koh, provided answers to questions on a topic not covered by the previous speeches: cyber warfare. In this speech, Koh explained how the administration views international humanitarian law as valid in the virtual battlefield as well. A cyber attack, according to Koh, can be considered a military attack that triggers the right to self-defense. Likewise, any military action in this area is subject to the principles of the laws of war in international law.

Koh also addressed the question of why the United States should initiate and impose on itself legal restrictions in a new realm that is not covered by the "old laws." "International law," said Koh, "is not purely constraint, it frees us and empowers us to do things we could never do without law's legitimacy. If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we *do* take will earn enhanced legitimacy worldwide for their adherence to the rule of law."

The last in the series thus far was another speech[17] by Jeh Johnson, which was covered in the media relatively widely, both in the United States and abroad. It may be that one of the reasons for this is that the Pentagon's

senior lawyer chose to deliver his address at Oxford University, but it is more likely that the content of the address was the principal reason for the interest it aroused. Johnson chose to devote his last speech as Defense Department general counsel to one of the legal framework's main weak points, which he and the other speakers took the trouble to formulate and present to the public.

According to that framework, much of the authority the United States derives for its war against al-Qaeda stems from the fact that the country has been in a state of war with the organization and its associates worldwide since 2001, in the wake of the September 11 attacks. This argument has led to criticism that in fact, the legal framework was of a war that was not limited in time or space, and it was thus liable to turn the exceptional situation of war, with powers that are reserved for this situation – such as extra-judicial killings, trials in military courts, and unlimited detention – into the new norm. In order to assuage this fear, Johnson attempted to persuade his listeners that in the view of the administration, the war with al-Qaeda has an end. The question is merely how we will know when it has arrived.

The United States, he explained, is involved in an unconventional war against an unconventional enemy, and therefore it should not be expected that the war will end conventionally by means of a truce or surrender. However, it should not be perceived as a permanent war. According to Johnson, if al-Qaeda continues to get weaker and its ranks continue to dwindle, as has happened in recent years, a tipping point will necessarily come when the state of war ends, and along with it, the relevant powers it grants the government.

On International Law

One of the main obstacles to the success of the overall message was the negative attitude toward international law and its institutions during the Bush administration. The new administration promoted a different approach: that the law was basically good and necessary, but that it needed an updated interpretation.

Many of those who gave the speeches stressed that any action taken by security forces in a conflict with al-Qaeda was weighed against four basic principles of the laws of war: (1) Necessity: the action was essential from a security perspective; (2) Distinction: a sufficient effort was made

to differentiate between combatants and civilians not involved in the fighting; (3) Proportionality: any damage that was nevertheless caused to civilians was proportional to the military benefit of the operation; and (4) Humanity: actions were designed so that unnecessary suffering is avoided and human dignity is preserved. When they are presented thus, simply, the laws of war (which are also called international humanitarian law) appear to offer a normative framework with which it is easy to concur. It is also easy to concur that abiding by these laws during asymmetric conflicts is a complex challenge. This is a better starting point for the debate on correctly interpreting the law so that it will fulfill its original purpose in 21st century conflicts as well.

A similar message was also conveyed regarding international legal institutions: they are important, but they need improvement. In his speech, Harold Koh spoke at length about the International Criminal Court and the UN Human Rights Council. The United States has significant differences with both institutions – namely, with respect to the definition of the crime of aggression and the biased approach toward Israel respectively – but, according to Koh, the current administration, in contrast to its predecessor, has decided to work to correct the flaws by means of constructive cooperation.

The essence of the message to the public was that international law and its institutions are not inherently antithetical to the interests of the United States. On the contrary: they have a positive potential that can be realized through initiative and leadership.

Taking Stock

Did the series of speeches succeed in reframing the debate? And if so, did this have positive consequences for security, for values, and for the law? It is still too early to make a definitive assessment, but there are sufficient signs that the answer to these two questions could be affirmative.

At the very least, it can be said that the debate on the administration's counterterrorism policies has become significantly more moderate than during the Bush administration. During the run up to his second electoral victory, President Obama received high marks from the public,[18] and even from his political rivals, on national security. In parallel, criticism of the administration's legal and ethical record by the Congress, the media, and human rights organizations remained limited for most of Obama's first

term. A former senior lawyer in the Bush administration admitted that Obama had succeeded, more than his predecessor, in gaining approval for his policy from the courts and in earning the cooperation of allies.[19] John Bellinger, who served as legal advisor to the State Department under Condoleeza Rice, expressed great appreciation for the Obama legal team's efforts to explain the legality of various actions taken in the name of national security. [20] Other commentators have described the situation toward the end of Obama's first term as a stabilization of the administration's "legal architecture" on issues of national security. [21] Some even spoke in terms of a broad, bipartisan consensus on the legal framework for counterterrorism,[22] a situation hard to imagine until recently.

These analyses are especially interesting given the fact that most of the commentators claim that in terms of pure legal positions, there was more continuity than change between Bush's second term and Obama's first term.[23] In their view, the Obama administration succeeded in gaining greater legitimacy at home and abroad for legal positions and military methods that are not very different from those of the Bush administration. The fact that Obama is a Democrat undoubtedly helped, but in all likelihood, his legal strategy and the public campaign to market it made a significant contribution. The administration translated this legitimacy into an expansion of military operations directed against al-Qaeda and into strengthening its alliances in various regions in the world. It has been reported that in documents seized at the home of Bin Laden after his death, the organization's leader complained that the al-Qaeda brand had become a liability, inter alia, because of changes in the rhetoric emerging from Washington after Obama's election. [24]

Opinion is more divided on the question of Obama's success in promoting the values of which he spoke. Some argue that the speech campaign helped tone down the criticism from the public, the courts, Congress, and the international community. They view with concern the legitimacy given today to actions that in the past provoked strong criticism, such as the broad wiretapping programs approved by the administration, or the continued detention of prisoners at Guantanamo—in certain cases, without trial and indefinitely. In addition, the administration's decision not to disclose documents describing serious instances of torture from the time of the Bush administration and not to prosecute any of those involved

sparked concern that Obama was perpetuating a tradition of immunity from the law.

These concerns were reinforced when a short time after Obama's reelection, in the last days of 2012, he signed two controversial laws: the Foreign Intelligence Surveillance Act (FISA) Amendments Act, which extends the powers given to the National Security Agency to eavesdrop on American citizens, and the National Defense Authorization Act of 2013 (NDAA), which almost completely blocks the chances of moving toward the closure of Guantanamo prison this year.

There is no doubt that the most trenchant criticisms of the Obama administration's legal positions focused on the aerial targeted killings in countries with which, from a legal point of view, the United States is not engaged in a state of war, such as Pakistan, Yemen, and Somalia. Mary O'Connell, a professor of law at the University of Notre Dame who has led the opposition to such operations since the Bush administration initiated them in 2002, is no longer a lone voice. In academic circles, among human rights organizations, and in the media, there are increasing allegations about the vast discrepancy between the genteel words of the speeches and their application in practice.[25] Outside the United States, where the legal campaign had limited resonance, public dissatisfaction with targeted killings is growing, and the question has already been raised as to whether this issue will become "Obama's Guantanamo."[26] Even the commitment to a future tipping point that will end the war with al-Qaeda did not allay these criticisms.[27]

However, the expectations of more radical change might have been excessive. As several of the speakers explained, every administration must maintain a good deal of continuity with the legal positions of its predecessor. Although Obama was limited by a Republican majority in Congress, he succeeded in implementing an impressive series of reforms, in eradicating unacceptable norms such as torture, and in defining new standards of transparency in matters of national security.

This series of speeches did not excite the general public, but it did create a positive impression with influential audiences in the legal, academic, and media world, as well as in international organizations, which in turn had a significant impact on the public debate. The presentation by prominent speakers of complex legal issues in a simple and accessible manner

provided public legitimacy not only for the administration's actions, but also for the justice system and for American and international law.

In 2013, this strategy is expected to face a significant test internationally. In January, Ben Emmerson, the UN special rapporteur on human rights and counterterrorism, declared that a comprehensive investigation would be launched into the legality of aerial targeted killings. It will be interesting to see whether the fact that Obama's first term advisors took the initiative and presented an orderly and well-reasoned set of arguments will help those of his second term to better cope with a legal, media, and diplomatic challenge of this kind.

Yet even an increase in the intensity of the debate over any one type of military action will not necessarily reduce the deep, long term ramifications of Obama's policy. Under his leadership, a political philosophy has been formulated and implemented, significantly increasing the extent to which the president's powers on national security are subordinate to US and international law.[28] With the help of his staff, he demonstrated a model in which the administration became increasingly bound to the law, and, at the same time, freer to act within the boundaries of the law; more exposed to substantive and legitimate criticism, but better protected from hostile criticism.

As noted, the dispute over US counterterrorism policies is alive, but it has changed. It can be said that Obama replaced the "false choice" between security and values with another choice, a real one, between two possible scenarios. In the first one (which he attributed to the previous administration), national security policy is made without adhering closely to the law and without transparency, but it is limited by reduced legitimacy at home and abroad. In the second, proposed by Obama, policy is limited by the strict confines of the law and by high standards of transparency, but enjoys broad legitimacy. In both scenarios, there is a risk of excessive and immoral use of force, and both have the potential for excessively limiting it. Therefore, public, judicial, and parliamentary oversight will always play an important role. Nevertheless, Obama and the other speakers attempted and largely succeeded in persuading their listeners that the second option, *their* option, is the only way in which security and values can be protected without compromising on either of them.

Lessons for Israel

Decision makers in Israel have several good reasons to think carefully before adopting a public legal strategy identical to the one described here. Israel is a small country; the threats to its security are varied and near, its room for error is limited, and its sensitivity to the loss of soldiers and prisoners of war is great. It has neither the ability to lead the free world or head great coalitions nor does it have any pretension to do so. It is much more exposed to diplomatic and legal proceedings in international institutions than the United States, and it has no reason today to expect fair treatment from some of them. Many people in Israel view international law as a weapon used cynically and unfairly by elements hostile to Israel in order to discredit and undermine it. In addition to all this, the complex legal situation beyond the Green Line and the fundamental constitutional questions that are awaiting political decisions could thwart even the most sincere desire to present a full, coherent, and convincing legal vision.

Nonetheless, it is worth noting several similarities. Like the Bush administration, the Israeli government suffers from a serious crisis of legitimacy that constrains its field of action politically and militarily. In Israel, too, the winds blowing from the senior political and military echelons carry with them the implicit notion that the type of conflict in which Israel is involved sometimes requires making a choice between ensuring security and upholding the law (or necessitates changing the law). Israel, like the United States, celebrates an ethical heritage that constitutes a moral compass. Its roots lie deep in Judaism, in the universal values of the Enlightenment, and in the historical role reserved for the Jewish story in the development of international law and recognition of human rights after World War II.

Israel's legal positions on most security-related issues can be found scattered like the pieces of a puzzle in replies to court petitions, Supreme Court rulings, testimonies of witnesses before commissions, newspaper articles, and transcripts of academic panels. When the government appoints a commission to write a more comprehensive legal opinion, such as the commissions headed by Attorney Talia Sasson, retired Judge Yaakov Turkel, and retired Judge Edmond Levy, it grants the commission a narrow mandate, and it does not always adopt its conclusions. Legal ambiguity appears to be the preferred choice not only for diplomatic and security reasons, but also as a political necessity.

The attitude toward international law in statements by government and security officials often ranges from disdain to seeing it as a problem that has to be considered, albeit reluctantly.[29] Professor Eyal Benvenisti recently wrote[30] about the danger in such statements:

> Statements by various IDF spokespeople or consultants showing contempt for international law could affect the decisions of international courts in the future...Such statements are liable to endanger the IDF's freedom of action and reduce it in future combat. Such statements are liable to create the impression that Israel has little regard for international law because the law is neither relevant nor moral.

In the same publication, Col. (ret.) Pnina Sharvit Baruch described[31] how the public attitude toward international law hampers existing efforts to attain legitimacy in the legal arena.

> It is unfortunate when statements are made by [defense establishment] officials, including senior figures, suggesting that "the rules [of international law – Y. E.] are inappropriate and new ones must be formulated." First of all, such statements are incorrect. In addition, such statements are liable to create the impression that Israel has ignored the laws of warfare since it deemed them to be "inappropriate rules." Thus we find ourselves in a situation in which on the one hand we act on the basis of the rules even when this means imposing restrictions on ourselves, and on the other hand we are accused of ignoring them, in part on the basis of such statements.

These are important recommendations, and if we are to judge by the conduct of officials during Operation Pillar of Defense, it appears that they have been internalized, at least partially. The Cabinet decision from the first day of the operation states explicitly that "Israel will act to the best of its ability to avoid harm to civilians while respecting the humanitarian needs of the population, all in accordance with the rules of international law." In addition, a number of reports have appeared in the media about the central role played by the attorney general in authorizing military operations. Minister of Justice Yaakov Ne'eman stated in an interview with Army Radio: "The State of Israel is careful to act in accordance with the law . . . the IDF does everything necessary in order to observe all the

rules of international law. Even though the other side violates all the rules, harming civilians, we observe all the rules of international law."[32]

The above citations reflect a welcome process of learning lessons from the military conflicts of recent years. Nevertheless, in most of these examples, the approach still remains limited to general statements and damage control. It would probably be more beneficial to formulate legal positions into a vision that can be presented to the public, and to explain how within its framework, Israel's security challenges can be met alongside an uncompromising commitment to Israeli and international law.

Imagine that a legal argument that justifies an action or a policy connected to security is explained fully to the public before it is presented to the court; before the petition is submitted and not in response to it; by a senior legal figure and not by an anonymous lawyer; directly to the citizens of Israel and not before commissions of one kind or another; in language that is simple, not tortuous; and as part of a broad, well structured legal framework and not in response to an isolated challenge. Imagine the military advocate general describing, in a public speech, the decision making process that takes place before an air strike is approved or a checkpoint is set up, or the Shin Bet's legal advisor explaining to law students what the criteria are for approving administrative detention, and what the mechanism of oversight is for such decisions. Imagine a YouTube video of a speech by the Foreign Ministry's legal advisor about the legal framework within which Israel conducts its policies regarding the West Bank and the Gaza Strip. Imagine a press conference in which the defense minister announces his decision to strike a new balance between the need to conceal operational information from the enemy and the need to reveal to the public, in so far as is possible, the standards on the basis of which actions are taken in its name and for its security. Finally, imagine that this entire initiative were led and coordinated by the Prime Minister's Office. Would such an initiative harm or strengthen Israel's security?

There is no doubt that such a change would require leadership and a joint effort by various government offices. Perhaps it is no coincidence that the campaign described here was led by a US administration in which the President is a professor of constitutional law[33] and is surrounded by lawyers. In his first term, the President's national security advisor, the Vice President, the Vice President's national security advisor, the Secretary of

State, the Secretary of Defense, and the Secretary of Homeland Security were all trained as lawyers.

However, with or without help from above, the power to promote a reframing of the public debate is in the hands of anyone who takes part in it. Military officials and security experts have the power to convey the fact that obeying the law and maintaining values are first-rate strategic assets. They can also contribute to shaping improved norms of transparency in the security establishment. Legal counsels have the power to push for the publication of the state's legal arguments in an orderly and accessible fashion – even, or especially, on controversial issues. Human rights organizations have the power to prove that an uncompromising commitment to the law and to values can go hand in hand with a serious approach to security concerns and to the operational and ethical complexities of asymmetric conflicts. Research institutes and academic institutions have the power to reinforce the connection between research on national security and research on issues of law and human rights. For the vast majority of them, this means expressing a truth in which they already believe: in the long run, it is not possible to maintain security without values, or values without security.

Notes

1 Remarks by the President on National Security, National Archives, Washington, D.C., May 21, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-national-security-5-21-09.

2 "The President and the Press," Address before the American Newspaper Publishers' Association, April 27, 1961, http://millercenter.org/president/speeches/detail/3677.

3 Daniel Klaidman, *Kill or Capture: The War on Terror and the Soul of the Obama Administration* (Houghton Mifflin Harcourt: Boston and New York, 2012).

4 See http://www.nobelprize.org/nobel_prizes/peace/laureates/2009/obama-lecture_en.html.

5 Harold Hongju Koh, "The Obama Administration and International Law," Washington, D.C., March 25, 2010, http://www.state.gov/s/l/releases/remarks/139119.htm.

6 Remarks as Prepared for Delivery by Assistant Attorney General David Kris at the Brookings Institution, Washington, D.C., June 11, 2010, http://www.brookings.edu/~/media/events/2010/6/11%20law%20enforcement/0611_law_enforcement_kris_remarks.pdf.

7 Remarks of John O. Brennan, "Strengthening our Security by Adhering to our Values and Laws," Cambridge, Massachusetts, September 16, 2011.

8 Jeh C. Johnson's Speech to the Heritage Foundation, October 18, 2011, http://www.lawfareblog.com/wp-content/uploads/2011/10/20111018_Jeh-Johnson-Heritage-Speech.pdf.

9 Jeh C.Johnson's Speech on "National Security Law, Lawyers and Lawyering in the Obama Administration," Yale Law School, New Haven, Connecticut, February 22, 2012, http://www.cfr.org/national-security-and-defense/jeh-johnsons-speech-national-security-law-lawyers-lawyering-obama-administration/p27448.

10 Attorney General Eric Holder Speaks at Northwestern University School of Law, Chicago, March 5, 2012, http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html.

11 This expression was coined by John B. Bellinger in "More on the Obama Administration's National Security Speeches," *Lawfare Blog*, April 20, 2012, http://www.lawfareblog.com/2012/04/more-on-the-obama-administrations-national-security-speeches/.

12 CIA General Counsel Stephen Preston's Remarks on the Rule of Law, Harvard Law School, Cambridge, Massachusetts, April 10, 2012, http://www.cfr.org/rule-of-law/cia-general-counsel-stephen-prestons-remarks-rule-law-april-2012/p27912.

13 Remarks of John O. Brennan, "The Ethics and Efficacy of the President's Counterterrorism Strategy," Woodrow Wilson International Center for Scholars, Washington, D.C., April 30, 2012, http://www.lawfareblog.com/2012/04/brennanspeech/.

14 This is the name given to these speeches on the *Lawfare Blog*. See, for example, the post by Professor Kenneth Anderson from April 19, 2012: "What Should the Administration Say? The Canonical National Security Law Speeches of the Obama Administration Senior Officials and General Counsels."

15 See note 11.

16 Harold Koh, "International Law in Cyberspace," U.S. Cyber Command Inter-Agency Legal Conference, Fort Meade, Maryland, September 18, 2012, http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/.

17 Jeh C.Johnson, "The Conflict against Al Qaeda and Its Affiliates: How Will It End?" OxfordUniversity, November 30, 2012, http://www.lawfareblog.com/2012/11/jeh-johnson-speech-at-the-oxford-union/.

18 See "Obama Security Record Gives GOP Few Openings," *Fox News*, June 19, 2012, http://www.foxnews.com/us/2012/06/19/obama-security-record-gives-gop-few-openings/.

19 Jack Goldsmith, "Obama's Weak Spots on Counterterrorism are Open to Romney," *Washington Post*, April 27, 2012, http://www.washingtonpost.com/opinions/obamas-weak-spots-on-counterterrorism-are-open-to-romney/2012/04/26/gIQAJ42zjT_story_1.html.

20 See note 11.

21 Robert Chesney, "Beyond the Battlefield, beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism," *Michigan Law Review* (forthcoming), downloaded from SSRN, September 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2138623.

22 Ritika Singh and Benjamin Wittes, "Two Parties, One Policy: Washington's New Consensus on Terrorism," *Commonweal Magazine*, September 14, 2012, http://commonwealmagazine.org/two-parties-one-policy.

23 John B. Bellinger, "More Continuity than Change," *New York Times*, February 14, 2010, http://www.nytimes.com/2010/02/15/opinion/15iht-edbellinger.html?_r=3&&gwh=4E4F52DA963A0D510C0E5C4DAD1DBD84.

24 David Ignatius, "The Bin Laden Plot to Kill President Obama," *Washington Post*, March 16, 2012, http://www.washingtonpost.com/opinions/the-bin-laden-plot-to-kill-president-obama/2012/03/16/gIQAwN5RGS_story_1.html.

25 On aerial targeted killings see, for example, Micah Zenco, "The Seven Deadly Sins of John Brennan: What Obama's High Priest of Targeted Killings Doesn't Want You to Know," *Foreign Policy*, September 18, 2012; Anthony Romero, Executive Director of the American Civil Liberties Union, "When the President Orders a Killing," Letters to the Editor, *New York Times*, May 31, 2012.

26 John B. Bellinger, "Will Drone Strikes Become Obama's Guantanamo?" *Washington Post*, October 3, 2011.

27 Glenn Greenwald, "The 'War on Terror'—by Design—Can Never End," *Guardian*, January 4, 2013, http://www.guardian.co.uk/commentisfree/2013/jan/04/war-on-terror-endless-johnson.

28 Trevor Morrison, "Obama v. Bush on Counterterrorism Policy," *Lawfare Blog*, November 11, 2012.

29 As a positive example of an approach to law in the professional echelons, it is worth noting statements made by Maj. Gen. (ret.) Avihai Mandelblit when he was military advocate general of the IDF, in an interview published in *Haaretz* on September 18, 2009. Mandelblit stated, inter alia, "But the rule was clear to all ranks and on all levels: we act according to the principles of international law all along the way"; "Asymmetric war is not asymmetric only in the sense that one side has fewer weapons and the other more, but that one (Hamas) sees itself as exempt from the rules of international law and the other (Israel) is bound by them"; "Our goal is to win the war, but in accordance with the limitations of the law. This is a professional issue, part of the military profession"; "The directive to the army is to act according to the laws of armed conflict, the test is connected to proportionality and also to a distinction between combatants and civilians. The military advantage that you gain from any attack must exceed the collateral damage that could be caused. That is how the directives have come down to the field."

30 Eyal Benvenisti, "How Challenges of Warfare Influence the Laws of Warfare," *Military and Strategic Affairs* 4, no. 1 (2012): 33-38.

31 Pnina Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," *Military and Strategic Affairs* 4, no. 1 (2012): 39-50.

32 "IDF again Calls on Gaza Residents to Leave Areas where Hamas is Active," Tal Lev-Ram, Army Radio, November 20, 2012.

33 On the connection between Obama's academic background and his security policy, see David Luban, "What Would Augustine Do? The President, Drones, and Just War Theory," *Boston Review*, June 6, 2012.

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

Gil Baram

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

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

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

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

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

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

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

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

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

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

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

The Role of Cyber Warfare Technology in the Israel Security Concept

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

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

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

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

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

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

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

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

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

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

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

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

From Israel's inception until the present day, its security doctrine has rested on the principle that quality is more important than quantity. Cyber

warfare technology is consistent with this principle: the use of cyber tools, which requires the training of expert manpower rather than the exertion of great physical force, facilitates operations that help bolster Israel's deterrent capability, and garners it great prestige in the international arena.

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

Formulating a Regular Strategy for Cyberspace

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

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

The Decision to Establish a National Information Security Authority

Israel does not have a regular publication in which it publishes its policy vis-à-vis dealing with the cyber threat. Most of the existing information is based

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

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

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

The Decision to Establish the Israel National Cyber Bureau

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

The key document in the matter is the Cabinet resolution of August 7, 2011 on the subject of "promoting national capability in cyberspace."[22] This decision provided for the founding of the National Cyber Bureau, and established its goal as "promoting national capability in cyberspace and improved handling of its current and future challenges." One of the Bureau's jobs is "to recommend a national cyber policy to the prime minister and the government, provide guidance for the relevant parties concerning the policy decided... implement this policy, and control its implementation."[23] The decision to establish the bureau, which was announced publicly, indicated significant progress in the government's handling of the cyber threat, and constituted a turning point on the issue.

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

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

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

a. Creating a system-wide perspective on the national level: Cyber defense requires multi-system assessment because public systems and private and business systems are highly interdependent.
b. Pooling of resources, actions, and information: Pooling means consolidating resources from various sources into a single integrative

entity for the sake of handling the threats facing Israel in an optimal manner.

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

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

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

All this activity indicates that Israel has correctly identified the looming threat to its national infrastructures, and has acted to set up a defense apparatus at the national level. Two watershed events were the establishment of a national information security authority in 2002, and the

Cabinet decision in 2011 to "promote national capability in cyberspace" and to establish the National Cyber Bureau. Nevertheless, the Israeli government has not yet disseminated a regular and unified strategy in this matter to the public.

Israel is one of the world's leaders in cyber capabilities. Typically, however, this is not appropriately reflected in the institution of a regular strategy or in a clear statement of an official course of action. It appears that Israel has yet to formulate a strategy in this field,[30] and that most of the information comes from press releases and media reports, rather than from official government sources. The government has taken an official decision in the matter, but has not yet published an orderly strategy.

Allocation of Resources

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

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

The figures show that Israel and its business sector invest considerable amounts in R&D in the technological field. To this can be added the various budgets distributed over the past year for R&D in applied and theoretical topics in the cyber sphere.[32] The total figure means that we can assume that R&D in the cyber field is being budgeted because its growing importance

for the nation's security has been acknowledged. The exact allocations have not been publicly disclosed.

One of the principal items in the 2011-2012 state budget consists of allocations for the "defense and public order category." This category includes the allocation from the general state budget for defense and public order. Funds from this budget are allocated to various defense agencies responsible for the cyber sphere. The budget for this category totaled NIS 61.8 billion in 2011 and NIS 63.4 billion in 2012. From these sums, the highest amount was allocated for spending on activities of the Ministry of Defense, which accounted for 18 percent of the total budget spending.[33] It can be assumed that the Ministry of Defense also invests considerable amounts in the development of cyber warfare by agencies for which it is responsible.

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

The Cyber Bureau Budget

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

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

develop the field, and the budget allocations reflect this. The cyber threat is gathering steam, and a long term program to guarantee its budget is being planned.[37]

A May 2012 Knesset Finance Committee meeting explicitly allocated money for the continuation of the Bureau's activity, in addition to the already allocated budget.[38] The Bureau's request, as submitted for the Committee' approval, included NIS 12 million for two main items. The first was an operating budget, including payment of salaries to Bureau staff, the creation of computer infrastructures, and physical security for the classified agencies required for infrastructures of this type. The second was the initial budget funding for the Bureau's regular activity.[39]

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

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

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

Changes in Force Buildup

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

Developments of this type have had a considerable effect on the principles of warfare and the changes that have occurred in the structure of armies, including the IDF. Upon examining the role of technology in Israel's wars, Prof. Ben-Israel asserted that a more technologically advanced battlefield signifies that flexibility and versatility play a more crucial role in modern warfare. For example, the Yom Kippur War clearly demonstrated that constructing electronic weapon systems against the enemy's known threats was insufficient; it is necessary to construct them so that they will be able to handle changes made by the enemy in the electronic parameters of its systems during the course of the fighting.[44]

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

The National Cyber Bureau

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

The Cyber Bureau is responsible for three main areas:

a. Formulating Israel's official security doctrine in cooperation with the agencies responsible for defense. The doctrine operates on two levels: increasing the general level of security and increasing the level of national security.
b. Developing infrastructures and promoting Israel's leading position in the cyber field, among other things by increasing its human capital and supporting the topic of scholarships for cyber-related research.
c. Taking the lead in national cyber processes, such as by regulating the security market, creating national security infrastructure through legislation and emergency exercises, bolstering relations with various countries, and so on.[46]

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

The National Information Security Authority

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

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

Tsafrir Katz, who until recently headed the ISA Technology Division, provided a rare insight into what goes on there when he said that 20 percent

of ISA personnel were technology specialists. The character of the ISA has changed since the 1980s, when it was not technologically inclined. For several years, it was necessary to develop new forms of employment for younger people. From his perspective, this revolution continued throughout the past decade.[49]

The Israel Defense Forces (IDF)

In 2009, then-Chief of Staff Lieutenant General Gabi Ashkenazi defined cyberspace as "a strategic warfare and operating space for Israel." An IDF cyber bureau was then established to coordinate and guide the IDF's cyber endeavors for the General Staff. This bureau was founded in Unit 8200 of the IDF Intelligence Branch.[50]

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

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

Ministry of Defense

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

Israeli Law, Information, and Technology Authority

The Israeli Law, Information, and Technology Authority (ILITA) was established by the Ministry of Justice of Israel in September 2006 to become Israel's data protection authority. ILITA's mission is to reinforce personal data protection, regulate the use of electronic signatures, and increase the enforcement of privacy- and IT-related offenses.[55] It also acts as a central knowledge base within the government for technology-related legislation and sizable governmental IT projects, such as e-gov (available online government).[56] ILITA is currently investigating the particulars of an event in which a large amount of personal information, including credit card data, was published on the internet by parties identifying themselves as Saudi Arabian hackers.[57]

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

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

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

Conclusion

Israel has been extremely efficient in identifying the features of the cyber threat arising from the development of cyber warfare technologies. It has begun to make the necessary changes, and there appears to be a close connection between how the cyber threat is addressed and national security. The handling of the problem focuses on three aspects: (1) defense organizations, the IDF, the intelligence community, and the defense industry, which as of now are taking independent action to protect their systems without direction from the ISA; (2) critical national infrastructures, which are subject to cyber attack, and which are being directed by the National Information Authority; (3) the private sector, in which civilian companies are exposed to cyber attacks. Although this aspect is partially addressed by ILITA, the bulk of the problem is not addressed at all.[59]

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

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

Notes

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

2 According to a report published in February 2012 by an international defense think tank (Security and Defense Agenda – SDA), in cooperation with the McAfee information security company, "Cyber-Security: The Vexed Question of Global Rules – An Independent Report on Cyber-Preparedness Around the World with the Support of McAfee." The report gave the US a four-star rating, http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf. See also Ehud Keinan, "Report: Israel More Prepared for Online Attacks than the US," *Ynet*, January 31, 2012, http//www.ynet.co.il/articles/0,7340,L-4183126,00.html.

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

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

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

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

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

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

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

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

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

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

13 Reuters News Agency, "Stuxnet Virus Used on Iran Was 1 of 5 Cyberbombs," *Ynet*, November 29, 2011, http://www.ynet.co.il/articles/0,7340,L-4168852,00.html.
14 Efrati and Yafe, "That's How You Build a National Cyber Defense."
15 Lior Tabansky, "Protection of Critical Infrastructure against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (2011): 72.
16 For more information about Tehila, see the final section, which discusses the design of forces.
17 Efrati and Yafe, "That's How You Build a National Cyber Defense."
18 "Protection of Computer-Based Systems," from the National Security Council Counter-Terrorism Bureau website, http://www.nsc.gov.il/NSCWeb/Templates/CounterTerrorismActivities.aspx.
19 Tabansky, "Protection of Critical Infrastructure against Cyber Threats," pp. 72-73.
20 In November 2010, the Prime Minister ordered the formation of a special team to formulate a national plan for placing Israel among the five leading countries in the cyber field. Work on this task, called the National Cyber Initiative, was led by the National Council for Research and Development, headed by Prof. Isaac Ben-Israel. The team, which included members from key agencies involved with the cyber realm in Israel, was composed of a number of sub-committees that examined the essential elements for coping with the cyber threat, and analyzed national welfare from an economic, academic, and national security perspective.
21 "The National Cyber Initiative," from the National Research and Development Council 2010-2011 report, July 2012, pp.10-17, http://knesset.gov.il/committees/heb/material/data/mada2012-10-15.pdf.
22 The decision was taken following comprehensive staff work by a national team headed by National Research and Development Council chairman Prof. Isaac Ben-Israel.
23 "Promoting National Capability in Cyberspace," Cabinet resolution No. 3611, August 7, 2011, from the website of the Office of the Prime Minister, http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx.
24 Efrati and Yafe, "That's How You Build a National Cyber Defense."
25 Yehuda Konfortes, "Wanted: An Iron Dome for Cyber that Will Protect the Home Front," *People and Computers*, February 1, 2012, http://www.pc.co.il/?p=79406.
26 Yossi Hatoni, "Dr. Eviatar Matania: Cyberspace Requires a Business and a National Policy Treatment – Not an Easy Task," from the CyberSec Conference that took place in February 2012, *People and Computers*, February 12, 2012, http://www.pc.co.il/?p=80025.
27 Ibid.
28 Speech by Dr. Eviatar Matania, 2nd International Cyber Conference, Tel Aviv University, June 9, 2012.
29 Efrati and Yafe, "That's How You Build a National Cyber Defense."

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

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

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

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

34 A paper for discussion by the National Council for Research and Development on the subject of the National Cyber Initiative – a proposal to establish a national program for building cyber capabilities that will combine R&D, economic, academic, and industrial aspects with national security needs, Tel Aviv, November 2012, p. 20.

35 "Promoting National Capability in Cyberspace."

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

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

38 Ibid.

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

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

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

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

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

44 Isaac Ben-Israel, "Technology Lessons," *IDF Publishing House*, 332 (1993): 10.
45 As discussed in detail in the section dealing with the formulation of strategy.
46 From an August 23, 2012 interview with Major Tal.
47 From a speech by Prime Minister Benjamin Netanyahu at the 1st International Cyber Conference at Tel Aviv University, June 9, 2011.
48 Amir Rapaport, "A Cyber Attack on National Infrastructure," *Israel Defense*, December 8, 2011, http://www.israeldefense.co.il/?CategoryID=536&ArticleID=1421.
49 Amir Rapaport, "Responding Quickly in Order to be Relevant," *Israel Defense*, April 3, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2153.
50 Amir Oren, "The IDF's New Battlefield is Found in Computer Networks," *Haaretz*, January 1, 2010, http://www.haaretz.co.il/misc/1.1182490.
51 "Computer Professions − A Cyber Defense Course," Communications and Teleprocessing Corps website, http://www.tikshuv.idf.il/site/General.aspx?catId=60698&docId=76101.
52 Hadas Duvdevani, "The first IDF cyber course has been completed. The goal is three classes a year," IDF website, May 3, 2012, http://www.mako.co.il/pzm-soldiers/Article-595ec4bc4611731006.htm&sCh=3d385dd2dd5d4110&pid=1093150966.
53 "Disclosure: A New Cyber Administration," *Israel Defense*, January 12, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1657. No other reports about the administration in the Ministry of Defense have been published; a reasonable assumption is that the information is classified.
54 Amir Rapaport, "Disclosure: Cyber Defense Exercise," *Israel Defense*, January 19, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1706.
55 From a September 5, 2012 interview with ILITA head Adv. Yoram HaCohen in the government compound in Tel Aviv.
56 The Law, Information, and Technology Authority (ILITA) website, http://www.justice.gov.il/MOJHeb/ILITA/.
57 A press release by the Law, Information, and Technology Authority, Ministry of Justice Spokesman's Bureau, http://www.justice.gov.il/NR/rdonlyres/4C39E414-E501-48C2-9C53-8EB533FD8B7D/32913/dover5.pdf.
58 "All About Available Government," Available Government website, http://e.gov.il/AboutUs/Pages/AboutUs.aspx.
59 Yossi Hatoni and Gabi Siboni, "There is an entire layer of organizations that is unprotected against cyber attacks," from the CyberSec Conference at the Institute for National Security Studies on February 12, 2012, *People and Computers*, February 15, 2012, http://www.pc.co.il/?p=80466.
60 Foreign reports attribute Stuxnet, Flame, and other cyber events to Israel.
61 Amir Rapaport, "A Cyber Attack on National Infrastructure."

The Classic Cyber Defense Methods Have Failed – What Comes Next?

Amir Averbuch and Gabi Siboni

Introduction

The classic defense methods employed throughout the world in recent decades are proving unsuccessful in halting modern malware attacks that exploit unknown (and therefore still unsolved) security breaches called "zero-day vulnerabilities." Viruses, worms, backdoor, and Trojan horses (remote management/access tools – RATs) are some examples of these attacks on the computers and communications networks of large enterprises and providers of essential and critical infrastructure and services.

The classic defense methods, which include firewall-based software and hardware tools, signatures and rules, antivirus software, content filters, intruder detection systems (IDS), and the like, have completely failed to defend against unknown threats such as those based on zero-day vulnerabilities or new threats. These sophisticated and stealth threats impersonate reliable and legal information and data in the system, and as a result, the classic defense methods do not provide the necessary defense solution. The current defensive systems usually protect against known attacks, creating heuristic solutions based on known signatures and analysis that are already known attacks,[1] but they are useless against the increasing number of unfamiliar attacks that lack any signature. Solving this problem requires different thinking and solutions. This article proposes an up-to-date approach, based on an analysis of sensitive information that

Prof. Amir Averbuch is a faculty member at the Blavatnik School of Computer Science at Tel Aviv University and a researcher in the INSS Cyber Warfare program sponsored by the Neubauer Foundation.
Dr. Gabi Siboni is the head of the INSS Military and Strategic Affairs Program and head of the INSS Cyber Warfare Program.

must be protected, for the purpose of identifying anomalous behavior.[2] The analyzed information includes an organization's data silos as a means of understanding unusual (anomalous) activity that in most cases indicates the presence of malware in the system. The article further proposes relying on the data to be protected as a source of knowledge for developing the defense system. An analytical analysis of massive data (big data analytics) will make it possible to identify such malware, while constructing a model that will provide a high degree of reliability in identifying and minimizing false positives, which pose a challenge to every defense system.

Development of Threats and the Limitations of the Traditional Defense Systems

The first cyber attacks on computer systems were based on viruses or worms that reproduced themselves and spread rapidly. Antivirus technology, however, completely failed to detect Trojan horses, whose behavior was entirely different than that of viruses. Traditionally, defense systems were developed to protect against known viruses, because it is quite difficult to identify such viruses by their behavior rather than their signatures. In this way, it became possible to create a database of virus signatures, and to compare files and communications reaching computers with these signatures. This approach required manufacturers of defensive software to continually monitor the development of viruses in order to create their signatures and distribute updates to their customers for the purpose of enabling them to update as quickly as possible the systems on which the protective software based on these signatures was installed. The burgeoning development of various forms of viruses and malware and the enormous growth in their number rendered this process virtually impossible, because major investments of resources in the continual updating of signature data for antivirus software were required.

The cyber attack hazards can be roughly divided into the following families: malware, spyware, worms, and Trojan horses (which open "backdoors"[3]). A classification that relates more to the object of an attack includes advanced persistent threats (APTs), which began with countries launching cyber attacks against other countries' military networks and the networks of government agencies, and in recent years developed into an attack by one country directed at another's organizational network of critical civilian infrastructure, and attacks against computer-operated industrial

supervisory control and data acquisition (SCADA) systems – such as the Stuxnet attack. Essential infrastructure systems controlled by industrial control systems in which control is exercised by the SCADA protocol are therefore exposed to attacks that are liable to paralyze the essential services, and could even suffer physical damage. Other possibilities include attacks against wireless systems and mobile broadcasting stations, the use of social networks for the purpose of spreading spyware and malware, and an attack against storage and cloud computing services.

The realm of attack in cyberspace can be divided into two types of attacks that exploit numerous weaknesses, including zero-day vulnerabilities:

a. *Broadcast attacks* are attacks that try to damage computers indiscriminately. They also feature extensive infection of software agents in order to create an entire network of computers (Botnet), with the aim of making these computers execute independent commands at a later stage or retrieve commands from a control server. As noted above, when information about new threats reaches the antivirus companies, they identify the signature or investigate them heuristically. By means of regular updates, the computers can be protected against these attacks. Given the extensive target community, the information about such threats will undoubtedly reach the relevant companies rapidly and be inserted into future versions of their products. In some cases, the goal of an attack of this kind is to reach a large number of computers – for example, employees (in the case of an attack against an organizational network) or customers (in the case of an attack against a financial institution, an attempt to steal credit cards via the internet, and so on). After the computer is infected, a Trojan horse is installed on it, making it possible to steal information or access the computer from a remote location. These attacks include various types of malicious code, even codes that vary from one infection to another in order to render identification through a signature more difficult (polymorphic viruses). There is still no complete defense since Trojan horse developers regularly check whether the antivirus software programs have already identified the hostile code and created the signature or group of heuristic rules to intercept it. In most cases, if the detection systems manage to identify the hostile code, the developers change the way it spreads or the way it operates in order to prevent

its detection. In this way, many Trojan horses consistently succeed in evading detection by the leading defensive software.

b. *Targeted attacks* are planned especially for a specific need, and exploit unknown weaknesses in the operating systems or widely known software packages while independently spotting new weaknesses. The vast majority of antivirus software, which is by nature based on signature defense, is incapable of identifying and preventing this type of attack, and the limited target community enables such attacks to evade the "radar" of antivirus manufacturers. It should be noted that threats are rapidly developing in the direction of focused attacks on high caliber targets.

The volume of data transmitted on a modern communications network is very large, owing to the need to provide many services to various kinds of end stations, including PCs, work stations, servers, switches and communications equipment, and many other diverse units. Such networks have many users, most of whom have no security awareness at all. As a result, APT attacks focus on people as well as on machines – via social networks, for example. The attack on the RSA company, which targeted the people in the organization, succeeded in penetrating the most secure systems.[4]

In recent years, we have seen a dramatic rise in the volume of new, undocumented, sophisticated attacks of a stealth nature. This is reflected both in the group of general attacks and in focused attacks. These attacks are overcoming all the classic standard defenses of the companies currently leading the protection sector. Major investments by countries and organized crime are responsible for the development of these attack methods, and the resulting damage is extensive.[5] The quantity of malware successfully penetrating all the existing defense systems and overcoming all the signature and rule-based classic defenses is increasing by leaps and bounds. The rate of increase has been in the three-digit percentages from 2011 until the present time.[6]

The existing systems are based mainly on preventing and thwarting known threats through the use of signatures and rules that are known in advance. Having no known signature at any given moment, these systems cannot detect zero-day attacks. They also find it difficult to identify Trojan horses and backdoors, and many sophisticated stealth attacks have no known signatures. Because they appear to be legal data and code, and do

not look like malware, they can penetrate almost any computer system. The attacks succeed in penetrating organizational networks and end-user computers despite all the defense systems; this is attributable to the fact that the initial appearance and behavior of the malware appears to be legal and proper. Furthermore, most of today's operating systems are built to handle a certain kind of attack, and are unable to deal with a broad range of attacks with mutations and secondary attacks.

In conventional software, one way of detecting unfamiliar and unsigned attacks is by identifying abnormal behavior of codes residing in the organizational systems, which differs from the way most normal data behave. This different behavior is what betrays hostile codes. The notion of the irregular behavior of a software element attempting to conduct unauthorized activity could serve as a possible basis for identifying and preventing attacks. Software producers worldwide understand the challenge and are taking steps to furnish such identification capabilities. This, however, is where the most significant challenge lies, namely, the difficulty in providing a reliable tool that will not produce false alarms or affect the user experience in an extremely negative manner. False alarms, which constitute one of the most significant challenges in defense systems, are created when the system issues a warning for a legal code with normal behavior and defines it as a hostile or suspicious code. If the load of such false alarms is too heavy, it will significantly harm the working capability of the computer systems, and is liable to cause the user to lose confidence in the defense system.

The second challenge is finding a solution for malicious code that evades the defense system. This phenomenon is called a false negative – when a result is obtained that appears negative, but is actually positive (comparable to a bearer of a serious virus who receives a negative test result from a laboratory when the virus is actually present in his body). These two challenges lie at the heart of defense systems in general, particularly in the use of analysis of the anomalous behavior of hostile code in an information system.

Identifying Anomalies as an Approach to an Operative Solution

This article focuses on the protection-based detection of anomalies in communications networks at various levels. The problem is broader, however, and includes the need to identify anomalies of hostile codes that

have penetrated weak points in software programs and applications. This approach is not discussed in the present article, unless the hostile code is exposed in the organizational communications. Regardless of the above, one can assume that some of the ideas mentioned are also suitable for detecting anomalies in software and applications.

Anomalies first proposed in 1987[7] are deviations from the expected behavior, which is the normal behavior. The basic assumption for any system seeking anomalies posits that malicious data have characteristics that are not found in the normal behavior specified during the learning phase. Since 1987, additional theories and methodologies have been developed, based on machine learning approaches and on the theory of information,[8] such as nervous systems,[9] a support vector machine,[10] genetic algorithms,[11] and many others. There are also numerous approaches that utilize data mining in order to find hostile code.[12] A general review of finding anomalies appears in an article by Chandola and Banerjee,[13] and there is a study of methods for spotting hostile code.[14]

One approach to detecting attacks on data from communications networks entails monitoring anomalies in network activity by finding the deviation from a normal profile learned from benign (proper non-malware) data. This methodology is based on tools retrieved from studies in machine learning,[15] mathematical and stochastic analysis,[16] statistics, data mining, graph theory, information theory, geometry, probability theory and random processes, and so on. Machine learning and data mining tools, combined with the above methodologies, are used successfully in many other fields, such as systems for recommending Amazon products,[17] Netflix,[18] optical character recognition,[19] translation of a natural language,[20] and identifying junk e-mail (spam).[21] Machine learning deals with the development of algorithms that enable a computer to learn, based on examples. Supervised learning of data known in advance, in which the correct significance of the parameters is known ahead of time, namely, labeled data, already exists. In unsupervised learning, the goal of the algorithms is to find a simple representation of the data without labels. Supervised learning is more limited with respect to the data content being learned. On the other hand, the results are more reliable, and it is therefore preferable.

Learning first takes place with a "healthy" group of data, which presumably contains no malware at all. This is called the "training set." It is usually best for the learning method to be able to detect whether part of

the training set contains malware up to a given percentage of all the data. Obviously, if most of the training set contains malware, it will be identified as normal data. As part of the filtering process, a process called "outlier removal" is used, which removes data that appear to be noise or infected from the training set.

The training set is analyzed by a variety of existing mathematical methods combined with innovative methods. The normal characteristics of the examined data can be identified through this process. This type of learning is called "one class." Another method, in which the characteristics are learned through comparison with a training set containing both clean and unclean data (e-mail with and without spam, for example) is called "binary class." The training set is derived from a mass of data accumulated and protected in an organization, together with continually guarded new data. For this purpose, methods of learning the data characteristic of normal behavior have been developed. While understanding the geometry of the learned data is one of the analysis methods, other methods also exist. For example, the following process describes a possible general structure of algorithms used as well as the processors of the training set in order to find the characteristics of normal (proper) behavior:

a. Breaking down each basic unit of communications or event data into characteristics (features, parameters).
b. Quantifying the relationships among the characteristics. There are a number of methods of characterizing such relationships. The kernel method[22] is one of the most common methodologies for defining them. Mathematical distance functions are usually used to define these relationships, which are near/far relationships with a range of characteristics existing between them. After this stage, the relationships between the communications data or events are guarded.
c. Lowering the dimension of the data. The dimension of the data is usually high, and is determined according to the number of characteristics making up a basic communications unit or basic event unit. The dimension of the data[23] is therefore lowered (from ten dimensions to two, for example), while preserving the relationships and coherence among the characteristics that were identified at the preceding stage. This is similar to sampling, in which only a small, reliably representative part of the original data is logically selected. Mathematical, algorithmic, and conceptual innovation is required in order to process data from

a high dimension that will suit a computer and reliably represent the original data. The sampling, which is aimed at reducing the volume of data, can be random, and it can be proved that the coherence of the data is maintained. There are many mathematical methods for achieving this objective. One of the methods for streamlining the computations in order to construct a compact representative of multi-dimensional data is the construction of dictionaries in order to speed up calculations while maintaining the relationships and features identified before the dimension was lowered. Other methods for speeding up computations facilitate sparsification of the data. The goal of these approaches is to specify a normal profile for the data from the training set while overcoming heavy computational problems in processing the training set. The learning action is usually computationally heavy. This action is conducted offline, and need not take place in real time. Common methods include PCE,[24] LLE,[25] ISOMAP,[26] and so forth.

The methods described above make it possible to effectively process the training set, which is "heavy" and liable to make calculations impossible. The goal of processing the training set is to specify the training data's ordinary (normal) behavior, based on an examination of the training set and the relationships defined between the characteristics of the data and the events of the training set. This assumes that the learning and the conclusions derived from it will reflect the normal behavior of all the future new data that are not part of the training set. As the volume of data in the training set increases and its characteristics become more numerous and diverse, the normal behavioral characteristics derived from the training set become more reliable. The calculation is more complicated, however, and it is therefore necessary to invest a great deal of effort in producing algorithms that are computationally effective and can handle large volumes of data.

The process described above specifies a possible learning model that generates a specification of the normative behavior of future data with the help of the training set's normal profile. From there on, the characteristics of all new information arriving, or of a new event, are examined. These characteristics are processed in order to see whether they deviate from the normative profile learned and determined during the learning (an anomaly). Deviations from the normal profile make it necessary to identify the attacks characterized as zero-day attacks. The method described thus

far does not use signatures; it finds behavioral deviations from the normal profile generated by processing the training set.

Figure 1 is a procedural description of the learning process described above. The chart also presents the range of sources from which the information has been retrieved for the purposes of the initial learning.

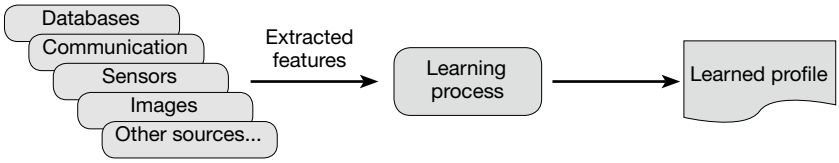

Figure 1. The Learning Process Chart

These methods and their derivatives for finding malware by monitoring the behavior of the data can be used in two different and complementary ways. The common denominator in these two ways consists of offline learning of the communications data from the protocol through which the data reach the organization (for example, port 443 [HTTPS], UDP port 53 [DNS], TCP, and TCP port 80 [HTTP], which are also web protocols) and constructing a profile that describes the normative behavior of the data of a given protocol that must be checked, according to the training set.[27]

a. *Operation in real time*. The algorithm for finding anomalies in communications data (accomplished in software or hardware) is located at the entrance to the organization. After data pass through the ordinary IPS Firewalls and IDS defense tools (signatures and rules allow them to enter), the algorithm checks each communications unit – whether its behavior matches the normal profile learned from the training set. If it proves to be an anomaly, its path into the organization is blocked. Since signatures are not used, the analysis of the substance of the anomaly can be performed either automatically or manually.
b. *Offline operation* – finding malware offline. Communications data that entered the organization through all the defense systems appear to be legal data, and subsequently begin to operate. An example of this is a spyware network absorbed into the environment with the aim of operating in the future. For this purpose, logs and events that occurred previously and are occurring now should be processed. In order to process information from both preserved and newly arrived

logs, security information and event management (SIEM) technology is used. SIEM, an information security monitoring system commonly used in organizational networks, serves as a central location for preserving and decoding logs and events of communications data. SIEM, an archive of all the communications data and events, helps conduct forensic analysis in order to find anomalies.

The above-mentioned methods of finding anomalies can be applied to the data collected by SIEM. Other data mining tools can also be applied to the SIEM data. SIEM contains two functions for security management: security information management (SIM) and security event management (SEM). The method that employs SIEM data should constantly apply the methodology for finding anomalies in order to identify the operation of malware when it is activated at some future date.

Figure 2 describes processes for checking information, given the results of the learning analysis:

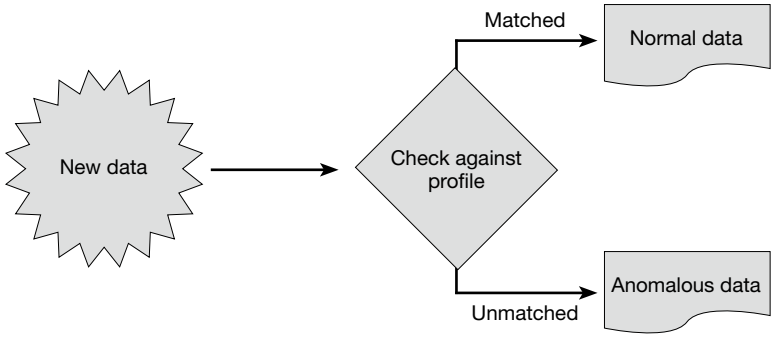

Figure 2. The Identification Process Chart

The Use of Big Data to Find Anomalies: The Data and Events Dictate the Identification Method

As described above, the main idea on which finding anomalies is based is specifying the behavior of the data in the training set and drawing conclusions from it with regard to the behavior of the data that did not participate in the training set, that is, characterizing the newly arrived data. In other words, the data dictate the processing, as reflected in the algorithms whose task was to learn the data as they are, and to adapt to them. This is in contrast to all the existing defenses against malware,

which seek patterns of already familiar malware and are unrelated to the behavior of the data. In the case of communications data, the data from each information unit of the protocol being monitored are analyzed. The relationships between the data are found by using the kernel method, and they are stationed in non-linear fashion in spaces with a lower dimension. The dimension of the data, which is usually high, is lowered in this way, thereby creating an effective way of finding anomalies.

Today, the data in which we look for anomalies are referred to as "big data," that is, a huge volume of data collected from all the information sources available on the organizational network. In many organizations, they are guarded by SIEM methodology. According to former Google CEO Eric Schmidt, the quantity of data created between the dawn of civilization and 2003 was five exabytes.[28] Schmidt asserts that this quantity is now created every two days. The following are a number of examples of the creation of big data every single day: the New York Stock Exchange (NYSE) creates one terabyte of data, Facebook creates 20 terabytes of compressed data, and the CERN particle accelerator in Switzerland creates 40 terabytes of data. According to a published report,[29] the volume of data doubles every year, and at least half of all businesses keep their data for at least three years for analytic purposes. Some of them are legally required to keep these data for a number of years. New sources of enormous quantities of data are constantly emerging in various businesses such as utilities. The bulk (80 percent) of these data is unstructured, which means that the organization is therefore unable to use them effectively. Big data have become a source of data mining that facilitates the identification of malware. Many well known companies such as Facebook, Google, Amazon, LiveJournal, and Wikipedia possess quotidian big data, and this list is far from complete. Today, big data are kept in the cloud. The quantity of data stored in each organization is huge, and is constantly growing. In order to handle large data silos, tools have been developed for processing big data that are unrelated to data mining or finding anomalies, such as Hadoop,[30] MapReduce,[31] and Memcached[32] – enormous parallel databases[33] that facilitate rapid data queries. In addition, many communications "pipelines" are being developed (by the Mellanox company for instance) for high speed transmission of these quantities of data. A great deal of effort is being expended on developing advanced tools for effective processing of big

data. Big data can therefore serve as a source for finding a broad range of sophisticated behavioral anomalies of different varieties of malware.

Conclusion

In order to process big data and effectively identify "high quality" malware, it is necessary to combine all the methods listed above. Tools – most of which are non-linear – were mentioned for reducing the volume of multi-dimensional big data without affecting the coherence of the data, at the same time maintaining the efficiency of the algorithms, for the purpose of handling huge volumes of data. The methods mentioned in this article that should be added are: learning from a small group of data; and using the kernel method on data, thereby determining the relationships (distances) between the sample points and reducing the dimension of the data by means of discrete or random sampling. This thins out the data, thereby obtaining an effective "housing project" of multidimensional big data in a significantly lower dimensional space in which anomalies are identified. Constructing dictionaries and using sophisticated and effective algorithms, together with big data processing tools, create many possibilities for finding malware in any organization by specifying the normative behavior and identifying deviations from it.

The proposed approach is a combination of computationally effective big data analysis and advanced tools for finding anomalies that are malware of zero-day attacks that do not yet have known signatures and behavior patterns. The methodology discussed here requires finding a needle in a haystack of data.[34] The point of departure states that the proposed algorithms adapt themselves and become accustomed to the data themselves. The data dictate how the algorithm operates. The methodology proposed in the article combines an understanding of the data structure by learning from a small group and drawing conclusions about the future behavior of the data that were not included in the learning set. This methodology is capable of detecting both malware whose activity is immediate, and malware, such as Trojan horses, that has entered the organization and will become operational at a later date.

Notes

1 "Heuristically" means through rules that help detect the harmful code.

2 Anomalous behavior of software code or information is unusual (uncharacteristic) behavior that arouses suspicion of malware in a system.

3 A security breach facilitates access to a computer without the need to verify an identity. This can result from a software error, a deliberate breach in the original code, or the installation of special software (such as a Trojan horse).
4 Gabi Siboni and Y. R., "What Lies Behind Chinese Cyber Warfare," *Military and Strategic Affairs* 4, no. 2 (2012): 43-56.
5 Symantec, "Internal Security Threat Report," *2011 Trends* 17, April 2012.
6 "FireEye Advanced Threat Report – 1H," *Source* 2012, http://www2.fireeye.com/advanced-threat-report-1h2012.html.
7 D. E. Denning, "An Intrusion-Detection Model, IEEE Trans," *Software Engl* SE-13, no. 2 (1987): 222-32.
8 W. Lee and D. Xiang, "Information-Theoretic Measures for Anomaly Detection," in *Proc. IEEE Symposium on Security and Privacy* (2001).
9 Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, and J. Ucles, "HIDE: A Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification," in *Proc. IEEE Workshop on Information Assurance and Security* (2001).
10 W. Hu, Y. Liao, and V. R. Vemuri, "Robust Anomaly Detection Using Support Vector Machines," in *Proc. International Conference on Machine Learning* (2003).
11 C. Sinclair, L. Pierce, and S. Matzner, "An Application of Machine Learning to Network Intrusion Detection," in *Proc. Computer Security Applications Conference* (1999).
12 M. A. Siddiqui, *Data Mining Methods for Malware Detection*, PhD dissertation, University of Central Florida (2008).
13 V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys (CSUR)* 41 no. 3, Article 15 (2009).
14 N. Idika and A. P. Mathur, "A Survey of Malware Detection Techniques," Department of Computer Science, Purdue University (2009).
15 R. Sommer and V. Paxon, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proc. IEEE Symposium on Security and Privacy* (May 2010).
16 Stochastic processes are processes whose development over time includes a certain element of randomness at any given moment.
17 G. Linden, B. Smith, and J. York, "Amazon.com Recommendations: Item-to-Item Collaborative Filtering," *IEEE Internet Computing* 7, no. 1 (2003): 76-80.
18 J. Bennet, S. Lanning, and N. Netflix, "The Netflix Prize," in *Proc. KDD Cup and Workshop* (2007).
19 L. Vincent, "Google Book Search: Document Understanding on a Massive Scale," Proc. International Conference on Document Analysis and Recognition, 2007; R. Smith, "An Overview of the Tesseract OCR Engine," in *Proc. International Conference on Document Analysis and Recognition* (2007).
20 F. J. Och and H. Ney, "The Alignment Template Approach to Statistical Machine Translation," *Comput. Linguist* 30, no. 4 (2004): 417-49.

21 P. Graham, "A Plan for Spam," in *Hackers &* Painters: Big Ideas for the Computer Age (O'Reilly, 2004).

22 B. Scholkopf and A. J. Smola, *Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond* (Cambridge: MIT Press, 2002).

23 M. Elad, *Sparse Redundant Representations: From Theory to Applications in Signal and Image Processing* (New York: Springer, 2010).

24 I. T. Jolliffe, *Principal Component Analysis* (New York: Springer, 1986).

25 S. T. Rowels and L. K. Saul, "Nonlinear Dimensionality Reduction by Locally Linear Embedding," *Science* 290, no. 5500 (2000): 2323-26.

26 J. B. Tenenbaum, V. de Silva, and J. C. Langford, "A Global Geometric Framework for Non-Linear Dimensionality Reduction," *Science* 290, no. 5500 (2000): 2319-23.

27 This approach also facilitates performance monitoring, an analysis of users' behavior, an analysis of man-machine relationships, and control of processes.

28 1 exabyte = 1 billion billion bytes.

29 M. G. Siegler, "Eric Schmidt: Every 2 Days We Create as Much Information as We Did up to 2003," *TechCrunch*, August 4, 2010, http://techcrunch.com/2010/08/04/schmidt-data/.

30 Web page: hadoop.apache.org.

31 J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," *OSDI* (2004).

32 L. Gavish, *New Caching Policies for MEMCACHED*, MSc Thesis, Tel Aviv University (2012); B. Fitzpatrick, "Distributed Caching with MEMCACHED," *Linux Journal*. 2004, no. 124 (2004): 5.

33 Hadapt, http://hadapt.com/.

34 M. Baker, D. Turnbull, and G. Kaszuba, "Finding Needles in Haystacks (the Size of Countries Blackhat)," Amsterdam, The Netherlands, March 14-16, 2012.

The Proliferation of Weapons in Cyberspace

Daniel Cohen and Aviv Rotbart

Introduction

Cyberspace is a phenomenon whose fundamental nature is to utilize an electromagnetic field for human purposes by means of technology. This article argues that such technology is a type of weapon. A common dictionary definition of "weapon" is "any instrument used in combat" or "any means employed to get the better of another."[1] A "cyber weapon," therefore, is one that strikes with the purpose of vanquishing another by attacking systems connected to cyberspace. Cyber weapons can be used as non-lethal weapons and have the ability to cause tremendous destruction and serious damage without destroying physical infrastructures or human life. The cyber-strategic environment includes the use of cyber weapons in order to penetrate the enemy's systems for purposes of espionage, psychological warfare, deterrence, and damage to information technology systems or physical targets.

We distinguish between the broad and prolonged capability to attack strategic targets that have a high degree of defensive capability and an attack that is liable to cause local or temporary damage. Currently, offensive capability of the former kind is restricted to a limited number of states, and requires major resources. In contrast, the latter type of capability costs little, and consequently, there are already signs that weapons are being mass produced, are available on the open market, and are used by terrorist and criminal organizations.

Cyber warfare is rapidly becoming one of the popular offensive methods used by states seeking to protect their interests from hostile states

Daniel Cohen is the coordinator of the Military and Strategic Affairs Program at INSS. Aviv Rotbart is a Neubauer research fellow at INSS.

or organizations. This is apparent in the recent cyber attacks covered by the media, such as the attack, attributed to Iran, on oil companies in the Persian Gulf and on American banks; or the attacks on Iran's nuclear facilities, attributed to the United States and Israel.[2] There are a number of reasons for this, including the ability to carry out a targeted attack, the attacker's ability to camouflage itself, and the victim's ability to conceal the incident, thus avoiding the need to strike back. Cyberspace allows states with resources and high level technological capabilities to employ an arsenal of weapons for a cyber attack. Similarly, states lacking resources can also equip themselves with offensive weapons and operate in cyberspace, although on a more limited scale and with less potential for damage.

A unique aspect of cyberspace not found in other arenas of combat is the ability to defend against viruses or other malicious codes[3] that have already been used in the past and discovered by security bodies.[4] Ostensibly, cyber weapons can be used only once, as they become useless the moment they are identified and signed.[5]

That said, do all the man-years invested in developing sophisticated malicious codes go down the drain as soon as an attack is discovered and signed? This article shows that they do not. As cyber attacks increase, cyber tools and capabilities proliferate around the world. One of the main reasons for this is that cyber weapons, for example, malicious code used in one attack, can be used for other attacks as well after they are converted. In a term borrowed from the world of biology, this is called "mutated code." Such code has functional characteristics similar to the original code from which it was created (and can even be totally identical). The difference between the original code and the mutated code is syntactical (structural) only and not semantic, where it is intended to evade the radar of software that identifies attackers.

From this we can conclude that if malicious code falls into the hands of an adversary with motivation and capability, it provides the attacked party with a weapon that, if it arms itself appropriately while executing complex actions such as reverse engineering, can be exploited for repeated use.[6] In addition, an attacker who understands the weapon can use it effectively and change it according to his needs to carry out further attacks.

We are in the throes of a silent cyber war, and while very few details have been leaked to the media, the mystery cannot be maintained forever. Consider, for example, the development of the field of unmanned aerial

vehicles, or drones. In its early days, the field was cloaked in secrecy. Few states had the ability to operate drones for espionage and subsequently for attack, and they made calculated and careful use of the technology in order not to reveal it to their adversaries. With the increasing use of unmanned tools, the wall of mystery has been breached, and today, thanks to the media, detailed descriptions of the countries that use drones, the targets of this type of attack, and drones capabilities and limitations are available. Terrorist organizations too have closely studied the new-old weapons that states use against them, and have developed means of defending themselves.

Another result of the extensive use of drones and the resulting media exposure is that an arms race has commenced, with many countries attempting to join the exclusive club of those in possession of these weapons for espionage and offensive purposes.[7] State supporters of terrorism have also entered the race, and terrorist organizations operating under the sponsorship of these states also enjoy the fruits of the investment. For example, Iran has acquired the ability to operate drones, and it did not take long for this capability to make its way to the Hamas and Hizbollah terrorist organizations.[8]

According to estimates, only a limited number of states currently possess the ability to carry out an attack in cyberspace in order to disrupt industrial control systems and cause physical damage, as with the Stuxnet virus, which damaged the centrifuges in the Iranian nuclear reactors, and many other states have joined the race to achieve this capability. Thus, a new type of combat weapon is being acquired for the purpose of causing damage and destruction from a great distance.

Carrying out an attack that will damage an industrial process is not overly complex, and it can be perpetrated by junior engineers. In contrast, understanding the industrial process that occurs at the target under attack and performing an in-depth analysis of it requires the full intelligence and penetration capabilities of a state.

Non-state actors in cyberspace, particularly criminal and terrorist organizations, can make use of, or already have made use of, variations of existing malicious codes and convert them so as to serve the organization's purposes. This is what happened in 2012 when criminal organizations made their own changes to two existing viruses, Zeus and SpyEye, and

managed to withdraw some 78 million dollars from banks around the world.[9]

The greater the accessibility of existing codes and the greater the ability of individuals or small organizations to perform conversions and modifications, the greater the proliferation of malicious codes for attacks on the financial world and for economic gain for criminal organizations. Furthermore, these codes will also spread to terrorist organizations that wish to accomplish social, ideological, and political goals through intimidation and the disruption of normal civilian life.

Capabilities of Actors in Cyberspace

The transition from the industrial age to the information age has produced a new product in the shape of cyberspace. The development of the information age is connected to the growth of communications, control, and computer technologies, which have deep social and economic significance. The year 2008 has symbolic significance in that it was the year in which, for the first time, the number of home computers (most of them connected to the internet) passed the billion mark. That same year, it was reported that the number of people in the world possessing cell phones exceeded the number of people without cell phones. Every such computer or phone can serve as a gateway to cyberspace and a weapon for a potential attacker (or itself become a target for attack).[10]

The rapid technological developments of the information age create unique characteristics and features in cyberspace that make it possible to work quickly against adversaries located far from the attacker. These developments may also change the face of the modern battlefield, creating theaters of combat in which the non-state actor is the main actor and exerts its influence on the policy of governments and international institutions to a greater extent than in the past. For example, the fighting in Kosovo between 1996 and 1999 was dubbed "the first internet war." State and non-state actors used the internet to disseminate information and propaganda and to demonize their adversaries. Hackers used the internet during the fighting as a tool against both other former Yugoslavia states and NATO, interfering with government computer systems and taking over government websites. Individuals and activists used the web to disseminate messages from the combat zone.[11]

Another example can be found in the attacks in Estonia. Commencing in April 2007, Estonia was attacked for three weeks with a DDoS, or distributed denial of service. The wave of attacks targeted the websites of government institutions, banks, and newspapers. Since it began after a clash with Russia over demonstrations by the Russian minority in Estonia, Estonian and NATO officials hinted that there had been Russian state intervention in carrying out the attacks.[12]

Cyberspace has broad significance with regard to the use of military force, terrorist activity, organized crime, espionage, and intelligence. Concerning the use of force, an attack on computers does not require a state base; it can be carried out by organizations and even individuals. In addition, a cyber attack can also be perpetrated between friendly states competing for diplomatic and economic intelligence.

A unique trait of cyber warfare is the ability of both attacker and victim to conceal almost perfectly the fact that an attack did indeed take place. Because of the nature of cyberspace, the attacker can carry out the offensive action at a great distance from the target and use concealment techniques to prevent exposure almost entirely. The victim, for its part, can always claim that the damage to its systems was the result of a hardware or software problem, thereby avoiding tarnishing its image and responding or threatening to respond.

A direct result of the ability to hide in cyberspace is very limited media exposure of attacks. From the little that is published in the press, however, we can see an increase in the number and sophistication of cyber attacks. All the major powers are already involved in cyber warfare in one way or another, and many other countries are investing in developing attacks and defense capabilities in cyberspace.[13] Cyber warfare is being perfectly integrated into the new "Cold War" that is underway between East and West because it allows the adversary to be threatened or harmed without compelling it to respond. A cyber attack that is not reported and for which no one claims responsibility is an attack to which the victim does not feel obligated to respond; nonetheless, it is totally cognizant of the hint sent by the attacker. This is the essence of a cold war.

On the defensive side, with the expanded use of cyber weapons, there is greater awareness of the dangers of these weapons and the potential damage they can wreak in terms of security, economics, and image. As a result of this awareness, more resources are being invested in developing

software systems that are better protected and more secure, as well as in securing facilities and critical infrastructures in various countries. As in any battle between attackers and defenders, in cyberspace too the attackers had the upper hand when cyber warfare began to develop. Now, however, it appears that the gap is narrowing, as more and more organizations are working to secure their IT infrastructures.

One of the characteristics of cyberspace is the difficulty in identifying the attacker. This contrasts, for example, with the attack on Pearl Harbor by Japanese Imperial Air Force bombers in 1941, which led the United States to declare war on Japan. After the large cyber attack such as that on Aramco in August 2012, the identity of the attacker is still being debated by security experts, even though an accusatory finger is being pointed at a state actor (Iran).[14] The characteristics of cyberspace also make it difficult to distinguish between intentional harm and a glitch, and to attribute an operation to a particular actor, thereby making it problematic for victims to respond to an attack. Some people argue that the characteristics of cyberspace today are still more advantageous for the attacker than for the defender.[15]

Groups that Employ Cyber Attack Tools

There are five main groups that employ cyber attack tools today or have the potential to use them in the future.[16]

States develop offensive and defensive capabilities as part of their exercise of power. Reasonable estimates are that some 40 states are acquiring cyber warfare capabilities or have already acquired them, including the ability to carry out cyber attacks. Most of the national programs are covert, and there is no consensus on the extent to which existing international law, which is valid for an armed conflict, is supposed to apply to this new type of attack.[17]

In the information age, there is increasing state intervention in the economy, civilian infrastructures, national security, civilian security, inter-organizational communication, management of government institutions, education, and so forth. As a result, countries around the world are increasing their investment in the defense of computerized systems, which is reflected in the resources allocated to the issue and to the development of specialized technologies and security concepts.[18] At the same time, defense and intelligence agencies are adopting the tools of cyberspace in order

to achieve their goals. Information technologies are also providing state intelligence services with a wide range of ways and means to perform the task. States have the ability to gain access to closed computer systems by infiltrating or activating an agent and by intervening in the supply system and introducing "infected" components into the enemy target.

The same characteristics of cyberspace that make it difficult to identify the attacker can also provide the attacking state with an advantage by utilizing a proxy to carry out an attack or take responsibility for attacking a state or a business enterprise in a rival country.

For example, in state cyberspace, three new programs that employ malicious code were exposed in 2012: Flame, Gauss, and miniFlame. Flame is an example of complex malware that existed undetected for some time, and collected data and information. At 20 MB, Flame is a large program for a virus, as most viruses rely on their small size to avoid detection. The program includes properties of a Trojan horse, allowing those who activate it to open a "back door" to computer systems in order to collect information and pass it to remote servers around the world. In addition, Flame is capable of recording audio by means of the computer's microphones, of taking screen shots, and of connecting to Bluetooth devices in the area of the attack.

This type of attack, which, because of its complexity is attributed to a state, affects not only government institutions, but also businesses and the infrastructures of business enterprises that have ties with government institutions.[19]

Criminal organizations are driven mainly by criminal and business interests. Organized crime uses hackers for profit: identity theft, fraud, spam, pornography, concealment of criminal activity, money laundering, and the like. Some 80 percent of internet crime is perpetrated by criminal organizations.[20]

Former Interpol president Khoo Boon Hui claimed that banks in the United States are losing 900 million dollars every year as a result of computer crime.[21] During the first quarter of 2012, it was reported that criminal organizations had created variations of SpyEye and Zeus for an attack on banks in Europe and the United States. The attack was first identified in Italy, where the code was tailored specifically to attack different banks. Later, a similar type of attack was identified against German and Dutch banks. The attacks then spread to Latin America and the United States.

The attackers managed to steal at least 78 million dollars in transfers from the accounts of some 60 financial institutions.[22]

According to the assessment of senior analysts, hackers manage to steal about one billion dollars a year from financial institutions. There are those who estimate that three of the major crime gangs operating in this field have succeeded in stealing some 100 million dollars a year by means of computer systems, while according to the FBI, in 2010, only 43 million dollars were stolen from American banks by non-cyber methods.[23]

Business enterprises mainly operate defensively since the scope of cyber attacks in the business context is growing significantly. However, some of them could elect to attack competitors for the purpose of industrial espionage – or have already done so. In addition, business enterprises face technological challenges in cyber defense such as protecting online payments, video broadcasts in real time, smartphone apps, and many others.

Terrorist organizations exploit the advantages of using cyberspace in order to pass coded messages, recruit supporters, acquire targets, gather intelligence, conceal operations, and the like. Out of cost-benefit considerations, terrorist organizations also use cyberspace to carry out cyber attacks, which help them influence public opinion so as to convey political messages and create demoralization and intimidation in order to disrupt citizens' lives. Terrorist organizations focus their offensive cyber operations on symbols of power such as the websites of government and media institutions.

One of the first documented attacks by a terrorist organization against state computer systems was carried out in Sri Lanka by the Tamil Tigers guerrilla fighters in 1998. For two weeks, Sri Lankan embassies around the world were flooded with some 800 e-mails per day saying, "We are the internet Black Tigers and we're doing this to disrupt your communications."[24] Some argue that this message induced fear at the embassies.[25] In Israel in January 2012, a group of pro-Palestinian hackers calling themselves "Nightmare" brought down the websites of the Tel Aviv Stock Exchange and El Al Airlines for a short time, and disrupted activity on the website of the First International Bank of Israel. Referring to this hacking incident, a Hamas spokesman in the Gaza Strip announced that the organization had initiated a new field of resistance against the Israeli occupation.[26]

Finally, *anarchists*, who oppose the existing institutional system, are eager to sabotage it from within or without, and will seek to attack the computer systems that are the basis for running it in order to disrupt and even destroy the social order and the fabric of life in the country. For example, groups of activists or individuals could attack websites in order to plant a political message, or endeavor to breach censorship mechanisms and reveal secrets.

In November 2012, during Operation Pillar of Defense in Gaza, government officials in Israel announced that there had been 100 million attempted cyber attacks against Israeli government internet services.[27] Anonymous, an organization that represents a theoretical concept of a community of hackers and activists, took responsibility for bringing down Israeli websites and leaking the credit card numbers of Israeli citizens during the conflict. Anonymous also published a list of more than 650 Israeli websites that it claimed were taken down or defaced as a result of the attacks by "hacktivists."[28]

A US government official has stated that "a couple dozen talented programmers wearing flip-flops and drinking Red Bull can do a lot of damage."[29] However, the ability to attack strategic targets of an enemy with advanced defensive capabilities differs from the ability to cause local, tactical damage. The various actors are acquiring cyber weapons in accordance with their capabilities and their limitations with regard to setting up a cyber force with offensive capabilities, and this has also been influenced by the interests and needs of each actor.

Table 1 charts cyber weapon capabilities of the various actors. Currently, there is a limited number of states with the capabilities and high level technological resources with the ability to use cyber weapons to attack both physical and cyber strategic targets. However, there is a low threshold of entry, and there are cyber weapons with the ability to cause tactical damage. Such weapons can be mass produced quickly and at a relatively low cost, and some of them are even available on the open market. States exploit cyberspace in order to gain an advantage and to promote their interests by collecting information, achieving the capacity to strike at the capabilities of anyone considered an enemy, and so forth. Non-state actors such as terrorist and criminal organizations can also leverage cyberspace for their purposes, and they benefit because it affords small actors influence that is disproportionate to their size.

Table 1. Basket of Cyber Weapon Capabilities of the Various Actors in Cyberspace

	Use of cyber weapons to attack physical equipment	Use of cyber weapons to attack in cyberspace	Use of cyber weapons for espionage	Denial of service and psychological warfare
States	Because of the large resources required, only a limited number of states today have the ability to carry out a cyber attack that causes physical damage to the defender. (According to reasonable estimates, the United States, Israel, Russia, China, and Britain have this capability.) Many other states are attempting to reach the threshold of physical attack capability or are keen to do so.	Medium-sized resources are required for this, and the number of states with electronic attack capabilities is greater than the number with the ability to attack physical equipment. States can carry out an electronic attack and/or use proxies to carry out such an attack.	The leading states in the field of industrial espionage and espionage for intelligence gathering are Russia and China, and, according to some, the United States and Israel. Since large resources are needed to make use of this capability, only a limited number of states possess it. If we assume that espionage is the second oldest profession in the world and that most states engage in espionage in one way or another, spyware to be used on targets inside and outside the country will become more common as access to technologies that provide cyber espionage capabilities increases.	This capability is relatively simple, and any state is likely to use it during a conflict with another state or by means of proxies.

	Use of cyber weapons to attack physical equipment	Use of cyber weapons to attack in cyberspace	Use of cyber weapons for espionage	Denial of service and psychological warfare
Terrorist organizations	Terrorist organizations today lack the resources required to realize this capability. Nevertheless, there are states that use terrorist organizations to carry out terrorist attacks, and it is therefore not inconceivable that they have been used or will be used to carry out physical cyber attacks as well.	Terrorist organizations lack the resources required to realize this capability, other than those acting as a proxy for a state.	Large resources are required to realize this capability. However, since it is one of the needs of terrorist organizations, they might attempt to acquire it (even though ostensibly, this weapon requires resources that are relatively complicated to acquire).	Used by terrorist organizations in order to disrupt routine life and sow anxiety and panic among civilians.
Criminal organizations		Used by criminal organizations in order to perpetrate financial crimes and extort business organizations and the wealthy.	Carry out the espionage activities necessary to perpetrate other crimes: identity theft, credit cards.	
Business organizations			Today, spyware is used to provide a business with an edge over a competitor.	A capability that can be exploited to harm competitors – for example, by bringing down a competitor's website or service.
Anarchists				A capability used by activists to convey messages by disrupting governmental and civilian systems.

The table shows that the state actor is capable of achieving offensive capabilities in all categories. States have diverse needs such as espionage and damaging industries in an enemy state. States also have restraints such as avoiding harm to innocents and avoiding a great deal of environmental damage. This leads to the development of cyber weapons for cyber attacks rather than physical attacks, or weapons for a psychological attack such as a warning before a bombing that makes it possible to avoid harming civilians.

The other actors in cyberspace have more focused interests and needs: terrorist organizations have more limited capabilities and resources, and are driven by the desire to accomplish political and ideological goals by means of damage to physical systems (even though no such incident has yet taken place), espionage, or psychological warfare. Business organizations, in contrast, are interested mainly in industrial espionage, and sometimes also in disrupting the activities of their competitors. Criminal organizations are interested primarily in obtaining assets and money fraudulently, and therefore focus on attacking cyber systems and on espionage that supports such activity (collecting credit cards and identity-linked information for an attack).

The Threat of the Repeated Use of Cyber Weapons

Every new cyber attack that is revealed brings cyber weapons closer to belonging to the public domain. As the use of cyber warfare tools increases, it is not inconceivable that more sophisticated cyber weapons with the ability to cause strategic damage will become commonplace, with various versions finding their way into the hands of state sponsors of terrorism and terrorist organizations.[30] An example of this is the Stuxnet virus attack on Iranian nuclear facilities. The attack continued in secret for several years, but the moment it was discovered, it led to the in-depth study and analysis of the virus's code and an attempt to understand everything that enabled it to be successful. The results of the analysis could have been used immediately to develop new viruses based on similar principles. The secret was exposed and the weapon disseminated. Theoretically, an analysis of malicious code by security companies and security experts could divulge the virus to various actors, ranging from states to terrorist organizations. Cyber weapons will not always remain the province of the few.

There is a belief that cyber weapons can be used only once, and that this will restrain their use and retard the development of new cyber warfare tools

because it is imperative to innovate constantly and to avoid using weapons that have already been discovered and signed by protection software. This belief has not proven itself; in fact, the opposite is usually the case. In other words, there is widespread repeated use of cyber warfare tools, which undergo changes to allow them to evade the radar of protection software. Cyber attacks depend on successful exploitation of a vulnerability in the system attacked.[31] The vulnerability can reside in a software component whose code was written without sufficient attention being paid to security, in a hardware component that can be penetrated and programmed to carry out destructive actions, or in a non-secure communications protocol.

In order for a system to be considered secure, all the aspects noted must be checked and secured separately. The only thing that is required in order to penetrate and take over the entire system is a small breach in one of them. Let us suppose, for example, that there is a website that contains sensitive information and is very highly secured, so that it is not vulnerable to attacks such as XSS, SQL Injection, and the like. Let us also suppose that there is another website, unimportant and totally unsecured, on the same server on which this secure site is located. In such a case, an attack can be launched on the other site, meaning that the computer where the sites are stored can be accessed through it. Once the computer has been taken over, none of the systems protecting the secure site are relevant any longer, and the secure site is compromised.

While cyber weapons that have been discovered and signed are blocked from being used in their original form, this is still a far cry from blocking them totally and rendering all the code that was developed irrelevant. First, every offensive weapon is composed of a number of modules (software components), including the module responsible for concealing the weapon in the attacked system, various information-gathering modules, an information-storage module, and a module for sending information to the command and control servers of the weapon. If a Trojan horse is discovered and signed, some of its modules can be reused by incorporating them in the code of another Trojan horse. Such a combination creates a new attack weapon that is likely to evade the radar of the anti-virus systems. Another way to reuse malicious code is by concealing it using methods known in the world of software as obfuscation[32] and packing.[33] These can sometimes change the malicious code so that it will not be discovered by protection software. Finally, even if the code that has been discovered

cannot be reused, a mutated code, which is based on similar ideas and methods of operation and exploits the same vulnerabilities as the original code, can be developed.

This claim is supported by the use of different variations of the Flame virus, which has recently been publicized in the media. Even after the original virus was discovered, various derivatives of it continued to attack the target computers until they were discovered.[34] Stuxnet, which is considered the most sophisticated virus discovered up to this point, opened the door for many others that imitate its modes of operation.[35] In fact, we can say with a high degree of probability that Flame and Stuxnet combined demonstrate in the clearest manner the ability to reuse malicious code because they have a large amount of code in common.[36] Although they were designed for completely different purposes (espionage and causing damage to industrial control systems, respectively), there are a number of functions that both must fulfill. These are penetrating the organization's computer system, concealing the existence of the weapon, analyzing the organization's network, and propagating within the network in order to find valuable target computers. Both weapons can carry out these functionalities by using the same code, which was written and checked only once.

Since the process of producing cyber weapons is long and expensive, the advantages of being able to use the same code for two different tools are enormous. However, this is a process that does not guarantee a positive result, despite the amount of effort that has been expended on it. Furthermore, even when a vulnerability is discovered, in order to exploit it and use it to penetrate the computer system, a great deal more work is required to write the appropriate code and build the files that can take advantage of the vulnerability.[37] It is also possible that no way will be found to do so because of the complexity of the vulnerability, and then further research will be necessary so as to identify another vulnerability that is easier to exploit. Therefore, when a creator of cyber weapons develops the ability to penetrate a system, his intention is to exploit it in several different scenarios and with several different tools in order to maximize the profit from his investment. However, the greater and more varied the use of a particular secret capability, the greater the chances that it will be exposed and blocked. This is a restraining factor in the considerations of

the cyber weapon creator with regard to propagating the tools and using the capability in other scenarios.

On the face of it, it might be expected that after malware is discovered and the existence and exploitation of the vulnerabilities become public, the programs in which the vulnerabilities were discovered (for example, Windows Operating System) would be updated immediately and the update sent to every computer on which the system is installed, thereby rendering all computers immune to the malicious code that exploits the vulnerabilities in question. This is not what happens, however. The process of protecting systems from malicious code that has been discovered comprises four main stages: discovering the vulnerability exploited by the code; closing the gap in the system; distributing a security patch to all users of the software; and only then installing it on all computers. Closing the gap through which the malicious code infiltrated the system is complex because after this is done, the programmers must also make sure that the performance of the system has not been affected by the change that has been made. The effects of the change must be carefully examined and various test scenarios run in order to make sure that the problem has been resolved. Depending on the complexity of the system, the process could take many weeks or even months.

Furthermore, even after a security update (patch) has been developed and distributed, many people do not update their computers automatically; this is especially true of companies that have an internal communication network that is not connected to the internet. In such cases, computers on the internal network will be updated only after the individual in charge of security acquires the software update or patch from the internet in order to perform the update. For these reasons, vulnerabilities can be exploited long after they have been discovered and publicized.

There is an interesting catch-22 phenomenon associated with security updates. When Microsoft, for example, encounters a security problem in its operating system, it develops a security update and seeks to provide it to all users who have been exposed to the problem. However, the moment the update is distributed, hackers and writers of malicious code become aware of its existence. They can analyze it in order to understand which security problem it solves, and then write malicious code that exploits the security gap that Microsoft itself has revealed. Of course, the malicious code can work only in systems on which the security update has not yet been

installed, but surprisingly, there are quite a few like that, belonging not only to private users who do not bother to update their computers frequently but also, and particularly, to companies whose computer personnel are responsible for taking action in order to update the company's computer system. This creates a window of several days or more during which the hackers can exploit the security gaps before they are closed.

The scenario described above is an example of the reuse of malicious code that is facilitated by the abuse of the security update distribution process. In general, Microsoft distributes security updates for its programs on the second Tuesday of each month, and this is called "Patch Tuesday."[38] The following day is called "Exploit Wednesday," because hackers analyze the security updates and begin to exploit them in order to penetrate computers that have still not been updated.

The ability to create new cyber weapons based on existing weapons or on a vulnerability that has been publicized is not always that simple and immediate. Hackers who exploit Microsoft's security updates in order to discover vulnerabilities in Windows must invest time in analyzing the patch and comparing the files that it corrects with the original files in order to identify where exactly the corrections have been made, since that is where the vulnerability lies. Finally, they must also find a way to exploit that vulnerability. This process can take anywhere from days to weeks, depending on the complexity of the patch and the determination of the hacker.

In contrast, an in-depth analysis of a sophisticated tool such as Flame would require more time and more professional and experienced personnel. In general, such an analysis is performed by states or security companies rather than by private individuals. An example is the cyber weapon, MiniFlame, which was analyzed in depth by the internet security firm, Kaspersky Lab.[39] This analysis, which took several months and required a large amount of manpower, was performed in order to develop protection against the weapon and to distribute it to the company's customers. However, the products of the analysis could serve as a basis for mutated code that utilizes similar techniques and sometimes even part of the code from the original cyber weapon. If these products were to leak from Kaspersky Labs to cyber weapon developers, it would not be surprising to discover new tools that share code with MiniFlame but are

used by other attackers against other targets, and possibly even against the original creator of the weapon, in a boomerang effect.

In recent years, there has been an increase in cyber attacks that require broad and prolonged offensive capability against strategic targets with a high level of defensive capability. Only a few states have this capability today, but it is not inconceivable that this trend will persist and that other states will achieve such capabilities for both defensive and offensive purposes. The trend is also evident in the global cyber crime market.[40] In Russia, for example, there are signs indicating that organized crime organizations have begun to join forces to increase their profits by sharing data and tools.[41] The Kaspersky Lab's 2012 Security Bulletin revealed that the number of malicious code attacks on the internet among the company's clients almost doubled between 2011 and 2012 (from 946,393,693 attacks in 2011 to 1,595,587,670 in 2012). These attacks took place in 202 countries. Criminal organizations used 6,537,320 unique domains as tools for perpetrating financial attacks, some 2.5 million more than in 2011.[42]

Conclusion

Many states and non-state actors are participants in a secret arms race in cyberspace. The map of interests of the various actors indicates that different kinds of attacks in cyberspace require state actors to be prepared for a range of possible attacks. At the same time, characteristics and properties of the cyber battlefield pose dilemmas for the attacker. Cyber weapons are reusable. When an attacker uses them, it reveals its capabilities to the victim, who can then reuse them, possibly even against the attacker itself (the boomerang effect). Weapons with strategic destruction capability, such as Stuxnet, are liable to fall, or have already fallen, into the hands of terror-supporting states and terrorist and criminal organizations, and will serve as a basis for cyber attacks. Independent development of cyber attack weapons or their purchase on the black market is liable to provide these elements with the ability to cause widespread damage, even if the tools obtained in this way do not reach the level of sophistication of the cyber weapons created by advanced states.

Both the possession of cyber weapons by private entities and the resulting uncontrolled proliferation are problematic. For example, a senior security researcher claimed that Stuxnet's code is found online – and even offered to share it with others.[43] On another occasion, an expert who had

analyzed Stuxnet claimed that the code was equivalent to a powerful weapon, but when asked why he did not destroy the copy in his possession, he preferred not to answer.

Aside from a discussion of ethical and moral questions, we believe that it is appropriate to implement both an intra-state and an international arrangement with regard to this issue in order to activate the regulation and enforcement mechanisms against proliferation of malicious code. Consideration should be given to limiting, and in certain cases, even banning, the possession of malicious computer codes so that they do not fall into the wrong hands. On this subject, we can perhaps learn from the war that is being waged against the illegal distribution of copyrighted intellectual property such as films and music.

Today, the arsenal of cyber weapons with the ability to cause tactical damage is reducing the procurement gap between states and non-state actors. Conversely, the gap between states with an arsenal of offensive capabilities against strategic targets on the one hand and states and actors that do not have the ability to achieve the high threshold for entry on the other is growing. It is not inconceivable that states and other actors will pursue the acquisition of cyber weapons that can cause physical damage, and there must be means of dealing with the dramatic increase in threats in cyberspace. Thus, there is an urgent need to discuss the concept of reusable cyber weapons that can be exploited for other attacks.

Notes

1 The American Heritage Dictionary of the English Language.

2 Mark Ambinder, "Did America's Cyber Attack on Iran Make Us More Vulnerable?" *The Atlantic*, June 5, 2012, http://www.theatlantic.com/national/archive/2012/06/did-americas-cyber-attack-on-iran-make-us-more-vulnerable/258120/.

3 Computer codes written for the purpose of carrying out an action on a computer system, usually data theft or the disruption of processes in the system, which is run without the knowledge or approval of the system's owner.

4 For example, when a malicious program is discovered by an anti-virus company, an electronic signature of the virus is created and sent to all the company's clients. This way, when another client is attacked by the same virus, the anti-virus program will identify the attack by the signature and block it effectively.

5 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 (Tel Aviv: Institute for National Security Studies, May 2012).
6 The process of discovering the technological and engineering principles of a product by analyzing its structure and modus operandi. Generally, this process includes dismantling the product and analyzing in detail how each component works.
7 Drone Wars UK, "Mapping Drone Proliferation: UAVs in 76 Countries," *Global Research*, September 18, 2012, http://www.globalresearch.ca/mapping-drone-proliferation-uavs-in-76-countries/5305191.
8 William Troop, "Got Drones? The Problem with UAV Proliferation," *The World*, March 26, 2012, http://www.theworld.org/2012/03/drones-proliferation/.
9 Dave Marcus and Ryan Sherstobitoff, "Dissecting Operation High Roller," *McAfee & Guardian Analytics*, 2012, http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.
10 Martin C. Libicki, *Cyber Deterrence and Cyberwar*, Rand Corporation, Project Air Force No. 3 (2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
11 Dorothy E. Denning, "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla (Santa Monica: Rand Corporation, 2001), p. 240, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.
12 Ian Trainor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, May 17, 2007.
13 Even and Siman-Tov, *Cyber Warfare*.
14 In this incident, malicious code was inserted on August 15, 2012 into the computer system of Aramco, the government-owned Saudi oil company. According to reports, some 30,000 computers were damaged.
15 Isaac Ben-Israel and Lior Tabensky, "An Interdisciplinary Look at Security Challenges in the Information Age," *Military and Strategic Affairs* 3, no. 3 (2011): 21-37, www.inss.org.il/upload/(FILE)1333532835.pdf.
16 Yoram Schweitzer, Gabi Siboni, and Einav Yogev, "Cyberspace and Terrorist Organizations," *Military and Strategic Affairs* 3, no. 3 (2011): 39-47, http://cdn.www.inss.org.il.reblazecdn.net/upload/%28FILE%291333532806.pdf.
17 James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," *UNIDIR Resources*, 2001, www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.
18 Rami Efrati and Lior Yafe, "The Challenges and Opportunities of National Cyber Defense," *Israel Defense*, August 11, 2012, http://www.israeldefense.com/?CategoryID=512&ArticleID=1557.

19 For instance, attacks against civilian targets, including critical national infrastructures, companies that are links in a chain of access to those targets, and companies on which an attack serves an economic need.
20 Eli Senior, "Interpol: 1,000 Cyber Attacks per Minute in Israel," *Ynet*, May 8, 2012, http://www.ynet.co.il/articles/0,7340,L-4226242,00.html.
21 Ibid.
22 See Marcus and Sherstobitoff, "Dissecting Operation High Roller."
23 Greg Farrell and Michael A. Riley, "Hackers Take $1 Billion a Year as Banks Blame Their Clients," *Bloomberg*, August 5, 2011, http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html.
24 Dorothy E. Denning, "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Service, US House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.
25 See Denning, "Activism, Hacktivism and Cyberterrorism," p. 269.
26 Guy Grimland et al., "Cyber Attack," *The Marker*, January 16, 2012.
27 Or Hirshauga and Nati Tucker, "Cyber Wars against Israel: 100 Million Attacks, No Significant Achievements," *The Marker*, November 22, 2012, http://technation.themarker.com/hitech/1.1871058.
28 John D. Sutter, "Anonymous Declares Cyberwar on Israel," *CNN*, November, 2012, http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html?hpt=hp_c1.
29 See Even and Siman-Tov, *Cyber Warfare*, p. 19.
30 For example, Hizbollah's cyber program. See Ward Carroll, "Hezbollah's Cyber Warfare Program," *DEFENSETECH*, June 2, 2008, http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/.
31 Vulnerability is a characteristic of a software/hardware/protocol component that makes it possible to use the component for a purpose other than the one for which it was intended, in a way that is advantageous to the person exploiting this feature. The advantage can be obtained in one or more of the following ways: taking control of the system, disrupting the system, or obtaining information from the system.
32 Code obfuscation is a technique from the software world that takes existing computer code that is intended to carry out a certain task and changes it in such a way that its functionality is not harmed, but the result is sufficiently different from the original so that an anti-virus program will not be able to identify it as a virus. Anti-virus programs that are based on identifying signatures in the code (a signature in this context is from a section of code intended to carry out a particular action, which can be attributed to a malicious program with a high degree of probability) will find it difficult to identify as a virus the code that was successfully obfuscated because none of the signatures known to it will appear in the result of the obfuscation process.

33 Code packing is a sophisticated type of code obfuscation. In the packing process, malicious computer code undergoes a radical change in form so that it no longer looks anything like a running code, but more like an innocent text file. This method almost completely prevents the anti-virus programs from discovering the malicious code before it begins to carry out its operation (for example, during the virus's penetration of the computer, it will not be discovered). Packing code works through an innocent utility that, when it starts to run, calls the text file in which the malicious code is hiding, translates the text into run commands, and in fact, turns itself into a virus. This can be compared to a virus from the world of biology, which takes over a living cell and exploits all of the cell's mechanisms for its needs.

34 Renana Ashuah, "Kaspersky Exposes miniFlame—Malicious Code Planned for Espionage Operations," *YedaTech*, October 15, 2012, http://www.yedatech.co.il/yt/news.jhtml?value=19827.

35 For an article on Stuxnet's successors, see Steven Cherry, "Sons of Stuxnet," *IEEE Spectrum*, December 14, 2011, http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet.

36 On Flame, see Aleks, "The Flame: Questions and Answers," *SECURELIST*, May 28, 2012, http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers.

37 Exploits are computer codes or files intended to exploit a vulnerability in a particular system in a manner that enables the writer of the exploit to penetrate or disrupt the system under attack. An example would be a program for viewing images on a computer screen that has a particular vulnerability that allows a code to be run on the computer under attack. Such a vulnerability is likely to be exploited in the form of an image file that includes code the attacker is eager to run on the computer under attack. Of course, such an image file must not only contain the code, but must also know how to exploit the vulnerability or the weak point of the image viewing software.

38 A patch is a system update.

39 Global Research and Analysis Team, Kaspersky Labs, "MiniFlame aka SPE: Elvis and His Friends," *SECURELIST*, October 15, 2012, http://www.securelist.com/en/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends.

40 This market was estimated in 2011 at more than 12.5 billion dollars, with Russia's portion of the cake some 2.3 billion dollars (nearly double its absolute value the previous year). See Group-IB, "State and Trends of the Russian Digital Crime Market, 2011," http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

41 Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strength," *Military and Strategic Affairs* 4, no. 3 (2012): 3-23, http://cdn.www.inss.org.il.reblazecdn.net/upload/%28FILE%291362315050.pdf.

42 Denis Maselnnikov and Yuri Namestinkov, "Kaspersky Security Bulletin 2012: The Overall Statistics for 2012," *SECURELIST*, December 2012, http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012.

43 The authors were present at a meeting with a figure from the security company.

Lessons from the Iron Dome

Yiftah S. Shapir

Israel has been under rocket attack for many years.[1] Particularly memorable are the shelling of Galilee panhandle towns in the 1970s, the Second Lebanon War in 2006, when Israel suffered over 4,000 rocket attacks in one month, and the ongoing rocket fire from the Gaza Strip over the past decade. Over the years, the State of Israel has developed a doctrine for defense against high trajectory weapons, of which rocket fire is one type. This doctrine is based on layers of defense, from passive defense, to active defense – involving interception of rockets and missiles by the Iron Dome system, David's Sling (in development), the Arrow 2, and the Arrow 3 (in development), to offense against launchers on their bases.

This article focuses on the Iron Dome system, which entered into operational service in early 2011 and demonstrated what it was capable of within a few months of its deployment. The article attempts to examine the lessons from the system's deployment and to reassess the decision about purchasing the system. It will also examine future ramifications of deploying this system and other systems that are expected to enter into service in the near future.

Background

Iron Dome is a system for intercepting rockets and artillery shells with ranges of up to 70 kilometers.[2] It was developed by Rafael Advanced Defense Systems in cooperation with Elta Systems, which produces the radar, and mPrest, which is responsible for the command and control system. The system uses a unique interceptor missile for shooting down rockets. Iron Dome batteries include a radar system, a command center,

Yiftah S. Shapir is a senior research fellow and director of the Military Balance Project at INSS.

and three launchers, each of which carries twenty interceptor missiles. One of the system's important advantages is its ability to identify the anticipated point of impact of the threatening rocket, to calculate whether it will fall in a built-up area or not, and to decide on this basis whether or not to engage it. This prevents unnecessary interception of rockets that will fall in open areas and thus not cause damage.

The system's development began in 2005 at the initiative of Brig. Gen. Dr. Danny Gold, head of the Defense Ministry's Research and Development Unit, and received a boost following the Second Lebanon War in the summer of 2006. In 2007, the Defense Ministry decided to procure the system and step up the pace of development. The firing of rockets from Gaza during Operation Cast Lead further accelerated deployment of the system. Thus, the final tests on the system were conducted in late 2010, and in early 2011, the first battery was delivered to the Israel Air Force. In late March 2011 the chief of staff, at the directive of the Defense Minister, ordered that the system be deployed to protect civilians. On March 28, 2011 the first battery was deployed in the Beersheba area, and one week later, a second battery was deployed to protect Ashkelon. On April 7, 2011, Iron Dome shot down its first rocket, which was fired from the Gaza Strip in the direction of Ashkelon.

At the time of this writing, there are five Iron Dome batteries. The third battery was deployed in June 2011 and the fourth in March 2012, while the fifth battery, which was originally planned for deployment in early 2013, was rushed into service in November 2012 during Operation Pillar of Defense to protect the Gush Dan area.[3] By late 2013, there are expected to be nine batteries,[4] and the current plan is to purchase a total of thirteen batteries.[5] During Operation Pillar of Defense, the Ministerial Committee on Procurement decided to allocate an additional 750 million shekels to expand procurement of the Iron Dome system.[6] The integration of these batteries means that a large number of soldiers will need to be recruited and trained, both in the regular army and the reserves.

Operational Firing

By April 2012, a year after Iron Dome's first operational interception, the system had demonstrated ninety-three interceptions in various incidents.[7] The first two most serious rounds of escalation took place in August 2011 following the shooting attack near Eilat, when over the course of six days

145 rockets and 46 mortar shells were fired at Israel, and in March 2012, when over the course of three days, 173 Grad and Qassam rockets and 37 mortar shells were fired after the killing of Zuhair al-Qaissi, a leader of the Popular Resistance Committees.[8] In the round of escalation in August 2011, in spite of Iron Dome's success in interception, a not-insignificant amount of damage was done to people and to property, including nineteen wounded and one person killed (in Beersheba). In March 2012, four people were wounded as a result of rocket fire. Data released about this round allows us to assess the effectiveness of Iron Dome in real fighting: the system successfully shot down 56 rockets out of 73 rockets employed. (This means that 100 of the rockets that were fired were aimed at open areas, where no damage was caused.) This is a success rate of 76.7 percent, a respectable rate by any standards.[9]

Iron Dome's most conspicuous success was during Operation Pillar of Defense in November 2012. The operation began in the afternoon of November 14, 2012 with the killing of senior Hamas operative Ahmed Jabari. By the time a ceasefire took effect on the evening of November 21, 2012, 1,506 rockets had been fired at Israel. Of these, 875 had fallen in open areas, and thus were not intercepted by Iron Dome. Another 152 launches were considered to be failed launches (this apparently means rockets that fell in the Gaza Strip). Iron Dome intercepted 421 rockets, and 58 rockets fell in built-up areas and caused damage. Five Israelis were killed by rocket launches and 240 were injured. According to the IDF spokesman, Iron Dome achieved a success rate of 84 percent.[10]

Operation Pillar of Defense proved the capabilities of the system, which justifiably won accolades, but the lessons from the operation are more complex. The operation also proved the tremendous importance of passive defense, specifically, the use of sirens for early warning, along with passive protection. One conspicuous example was the incident in which a rocket struck a residential building in Rishon Lezion and destroyed an apartment, but the residents, who were in the apartment's protected space, emerged unscathed. The results of the operation also proved that 100 percent protection is impossible.

Criticism

Along with the acclaim earned by the Iron Dome system, there was also not-insignificant criticism from various sources and for various reasons.

The defense establishment was harshly criticized because the Iron Dome system was chosen over other systems that the critics believed to be better, because of the promises of protection, which the critics felt were not realistic, and because of the large sums of money invested in the system.[11] What follows is a review of the criticism of the Iron Dome system broken down on a number of levels: technical-tactical, operational, and political.

Technical-Tactical Criticism

From a technological point of view, the system attained extraordinary success.[12] Iron Dome is a unique system, with nothing else like it anywhere in the world. There is only one other operational weapon system in the world that is designed to shoot down short range rockets and mortars: the US Army's Centurion system, which is based on the Phalanx anti-ship missile defense system. It intercepts rockets and mortars at short ranges by means of a fast 20-mm cannon. The Centurion has been used to protect US Army forces and US facilities in Iraq – in particular, in the "Green Zone" in Baghdad, a fortified area that was the command center of US activity in Iraq and was subject to repeated attacks.

Other systems have been proposed or are in development in various places around the world. The best known in Israel is the Skyguard, proposed by Northrop Grumman. The system is based on the Nautilus tactical laser system, developed in Israel in the 1990s. Its supporters claim that its development has been completed, but it has no purchasers and is not operational anywhere in the world.[13]

On the level of technology several arguments have been leveled against the Iron Dome system:

a. Its inability to cope with very short range threats. The system's minimum range has not been published, but according to critics, it cannot shoot down rockets or shells whose range is less than 5-7 kilometers, and in any case, it is not capable of shooting down mortar shells. While the system was being developed, it was announced that it would protect Gaza perimeter towns and cities. Among the threats mentioned were mortars, whose range usually does not exceed several kilometers. To be sure, such promises were generally made by political figures and not by the system's designers. The critics argue that the defense establishment should have favored acquisition of existing systems – Skyguard or Centurion – or integrating these systems with Iron Dome in order to cover the shorter distances.[14]

b. As a result of the system's response time, critics claim that it will also have a hard time coping with rockets fired on flat trajectories at even longer ranges – up to 16-18 kilometers, according to the critics.
c. The cost of interception is high. The cost of the interceptor missile is about $40,000-50,000. Furthermore, in some cases, two interceptor missiles are fired at one target, which further raises the cost of interception. This will greatly limit the State of Israel's ability to acquire interceptor missiles for a prolonged conflict.[15]
d. The system has a "saturation point." It is capable of engaging a certain (unpublished) number of targets at the same time, and no more. Additional rockets fired in a crowded salvo could succeed in breaching defenses and cause damage.

A full discussion of the system's technology is beyond the scope of this article. Suffice it to say that all of the systems mentioned (like any technological system) have limitations, and any deliberation of a system must consider all its aspects, not only the technological.

Operational Criticism

Operation Pillar of Defense and the rounds of escalation that preceded it proved that Iron Dome, in spite of its success, does not provide total protection. Rockets penetrated its defense, causing damage to property and casualties.

However, these events also demonstrated that the real problem was not the physical damage that the rockets caused – which in the final analysis was negligible – nor even the loss of life, unfortunate as it was. The problem was that in every one of the incidents, some one million residents of the State of Israel were forced to sit in shelters, and schools and other educational institutions were closed by order of the Home Front Command, which meant that many people did not go to work because parents were forced to stay home with their children.

In addition to the economic damage, there was also damage to morale, as people felt helpless in the face of the attacks. The other side of the coin can be seen in the victory rally held by Islamic Jihad in Gaza in March 2012. From Islamic Jihad's point of view, this feeling among the Israeli public was itself a victory,[16] and the situation recurred at the end of Operation Pillar of Defense, which highlighted the fact that for Hamas, the victory was in its ability to persist in harming the civilian population in Israel

notwithstanding the IAF attacks. For this reason, the damage to Gush Dan was a significant achievement for Hamas.[17]

This problem is of course not unique to Iron Dome, and is characteristic of any defensive weapon system. Even if Israel had had twelve or twenty Iron Dome batteries, and even if hypothetically there had been a much better weapon system than Iron Dome, the situation in principle would not have been any different. In any rocket attack against Israel, it would still have been necessary to activate the sirens, the Home Front Command would still have needed to issue alerts and instruct Israelis when to enter protected spaces, and the economic damage, as well as the damage to morale, would have been the same.

This raises two difficult questions. First, how many Iron Dome batteries does the State of Israel need? According to Iron Dome's developers, the "defensive footprint" of a battery is about 100 square kilometers, while according to its opponents, it is much less. This is not a large area.[18] In order to protect the population of all Israeli towns and cities in a war with Lebanon, many dozens of batteries would be needed. Since the number of batteries purchased must be limited (and the number of interceptor missiles as well), the question of whom to protect and whom not to protect is critical.

Second, and this question stems directly from the previous question, is there any point at all in protecting the civilian population? With such an expensive defensive system, would it not be better to protect strategic facilities whose survival is important to the proper functioning of the country? This question becomes even sharper when we examine the procurement of the enemy, and in particular, Hizbollah. The missile systems in Hizbollah's possession are improving, not only in range and ability to cover ever-larger areas of the State of Israel, but especially in accuracy.[19] As long as the weapons in Hizbollah's possession have a statistical distribution, there is no point in using them against strategic facilities because there is little chance of causing them damage. It is better for Hizbollah to use missile systems as a weapon of terror against a civilian population. However, when the weapons are more accurate (and more expensive too, and therefore held in smaller quantities), the maximum benefit will be achieved by using them against such targets. Therefore, it appears preferable for the side that is defending itself to direct its resources toward protecting those facilities rather than the civilian population.

These considerations imply that investing in active defense systems for the civilian population is unnecessary. While the damage to property and people can be somewhat reduced, it is not possible to protect the entire population, or even a large part of it. More critically, it is not at all possible to prevent the real damage of rocket attacks, i.e., the damage to the country's economy and its ability to function properly. If money has already been invested in developing an anti-rocket defense system, it is better to use it in order to protect strategic facilities and not the population. Based on these considerations alone, the investment in Iron Dome appears superfluous. However, these of course are not the only considerations.

Deterrence

An important argument in the decision to deploy a defensive system in general, and Iron Dome in particular, is its contribution to Israeli deterrence. Two main arguments are raised in this discussion. First, the success of the interceptions will make it clear to the enemy that firing rockets is pointless, and ultimately, it will stop. Yet even if we ignore for a moment the fact that such an argument is the antithesis of the entire classical theory of deterrence – which claims that deterrence is achieved through the threat of punishment, and not by preventing success[20] – it is hard to understand the argument, and even harder to assess its validity on the basis of cumulative experience. On the theoretical level, a party that fails in its use of offensive weapons may despair of further attempts to use them, but such a failure is also likely to encourage a search for solutions that can overcome defensive measures.

In practice, it is evident that the terrorist organizations in Gaza are not ignoring how Iron Dome affects their success, even when they themselves present the events as achievements and the success of Iron Dome as unimportant.[21] On the other hand, there are hints of the other side's efforts to find tactical solutions, evident from Iron Dome professionals who report on changes to the rockets' operating procedures made by the terrorist organizations in Gaza. These changes appear to have been an attempt to overcome defensive measures (apparently, by efforts to launch crowded salvos).[22]

Second is the argument made after Iron Dome's success in the latest rounds: the system gave decision makers freedom of action.[23] The implicit logic of this argument is that without Iron Dome's success, Israel would

have suffered much greater damage and decision makers would have found themselves forced to initiate an offensive campaign such as Operation Cast Lead. However, with the system's success, decision makers have a greater level of freedom to decide whether to attack or not, and when. This argument was especially prominent in commentaries published regarding Operation Pillar of Defense, which ended without a ground operation. The argument was made of course by those who believed that a ground attack in Gaza would not have been desirable.

This argument also has a flip side, which arose in discussions during Pillar of Defense and during the rounds of escalation that preceded it. It is the argument made by supporters of a ground operation, who claimed that Iron Dome has become a "fig leaf" for decision makers who from the outset did not want a ground operation.[24]

Both sides of this argument are problematic. Even in the past, Israel suffered rocket and missile attacks, and in the absence of any defensive option, Israel mainly used deterrent threats toward the enemy. However, Israel's leaders never felt that they lacked a degree of freedom to decide whether or not to attack the enemy, and when.[25] The claim that without one weapon system or another decision makers would have no discretion is an expression of no confidence in their ability to consider the issues and make rational decisions.

Political Decisions

The third level of the analysis is the point of view of decision makers in the political echelon. Here there are completely different considerations.

The first consideration is the system's contribution to the morale of the civilian population, particularly in outlying areas, which in any case often feels neglected by the government. This sentiment is evident in videos uploaded to YouTube by Israeli citizens during the rounds of escalation in March and June 2012, as well as during Pillar of Defense. Not much can be seen in the videos: a bright spot in the sky hitting another spot, the flash of a small explosion in the distance. But in the background we can hear the cheers of those watching the successful interception. This can be seen more clearly in newspaper headlines during Operation Pillar of Defense.[26] The significance of this phenomenon is tremendous. Not only did Iron Dome contribute to the morale of the populace; it made an important contribution to the resilience of the civilian population overall. It proved to them that the IDF was doing everything it could to protect them.

Second, from the point of view of political decision makers, the moment there is any technical possibility of protecting the public from rocket attacks, it would be difficult to decide against purchasing such a system. A political leader in a democratic country would have great difficulty standing before the voting public and saying that the technology exists but he has decided not to purchase it. No matter how weighty the reasons, such a leader would have less chance of being reelected. The public would find it difficult to accept such a decision.

The operational echelons of the IDF learned this the hard way. As long as the Iron Dome system was in the development stage, there was no problem declaring that a civilian defense system was being developed. However, the moment the first system was delivered to the IDF, the operational consideration was activated, and the IDF came to the conclusion (the most reasonable one, as described above) that such a system would provide the maximum benefit in defending important strategic facilities, such as IDF bases, and the optimal use of the system would be to place it in a military base and deploy it outside the base when there was an operational need. The decision provoked immediate reactions and sharp protests from the public, particularly in areas that were under rocket threat. Very quickly, the political echelon was forced to order the IDF to deploy the system to protect civilian towns and cities.

Third is the aspect of Israel's technological and industrial base. Israel's security concept has always seen the defense industry as a very important component of the country's security. In order to preserve this base, the industry must receive orders from the defense establishment to maintain its ability to manufacture and support sales of weapon systems abroad. However, beyond the sale of products, it is important for the industry to be given technological challenges. In the past these challenges were large projects such as the Lavi fighter aircraft, the Arrow missile system, and many other systems. These challenges are the engine that drives industry to high levels of technology, and they are responsible for Israeli industry's current position as a world leader. From this point of view, even projects that were not ultimately carried out, such as the Lavi, made an immeasurable contribution to the advancement of the industry. (This point was also apparently behind the defense establishment's decision to prefer the Iron Dome system to competing systems produced abroad.)

The fourth consideration is the close relationship between Israel and the United States, one of the pillars of Israel's defense. Cooperation on issues of missile defense is a key component of this relationship because of the great importance of missile defense to US strategy. We can thus understand the cooperation in development and production of the Arrow and Magic Wand systems and the special allocations from the Obama administration, as part of its budget request to Congress, for grants for Israel to purchase additional Iron Dome batteries (allocations that are beyond the overall defense aid).

Open Questions

Iron Dome has still not faced very difficult tests. An open question is what its real contribution would be in the event of a massive rocket attack from Lebanon. In the summer of 2006, in the course of one month, Israel was hit with 4,000 rockets. Today, Hizbollah's stores of weapons are much larger, estimated at 40,000-50,000 rockets. A possible scenario for fighting could include several thousand rockets fired every day. In such a scenario, there are several aspects of defense.

First is the question of what to protect and what not to protect. In this case, the question asked above will emerge in all its gravity: should Iron Dome be partially deployed in order to protect part of the civilian population part only to raise morale, or should the existing batteries be concentrated to defend those facilities whose survival would be critical to the functioning of the country?

Second is the question of the system's ability to be effective, even in protected areas. Even if a decision were made to defend certain civilian towns and cities (and certainly not all of them), would the system be effective? Would its ability to reduce the damage be such that it would even be felt in such a serious situation? And if the answer is negative, what would be the public's response to the damage it sustained, and would the system lose its value as a contribution to the morale and resilience of the population?

Third, the question that will always remain open for political discussion is "how much." The decision to purchase systems like Iron Dome was one decision. Decisions of an entirely different sort are how many batteries to purchase and what to defend. Will we defend ourselves to death?

In August 2012, the IDF spokesman announced that many of the year's recruits to combat units had expressed their desire to serve in Iron Dome units. This demonstrates the severity of the problem, since investment of resources in defense necessarily comes at the expense of resources for offensive capability. Even if a solution is found to the financial issue and additional money is found for defense, the human resources of the State of Israel remain as they were. Years ago, the most desirable units among recruits were the pilots' course, the paratroopers, and the reconnaissance units. The change is deep and fundamental. If in the past, Israel based its security on its offensive capabilities, today more and more of its resources and its power are being channeled to defense.

Conclusion

Israel is the first country in the world to deploy an operational anti-rocket system to protect the civilian population. Very few countries in the world have suffered such severe attacks on their civilian populations for such an extended period. It is therefore no wonder that Israel has invested such extensive resources in the search for solutions to the problem.

The solution chosen was not without controversy. Opponents of the project pointed to several of the system's flaws: some are inherent in any system and others are unique to Iron Dome, which, like any technical system, suffers from one type of technical defect or another. Other opponents also pointed to the high cost of the system, arguing that there were better technological solutions.

The above analysis shows that decision making is a complex process that takes into account various types of considerations, the operational consideration being only one of them. Social, political, and even international considerations are no less and perhaps even more important. Given this range of considerations, the decision to purchase anti-rocket defense systems appears to be a wise one.

Apparently the diplomatic and political considerations, which were indifferent to the technical differences among the various systems, were the decisive factors in decision making. Therefore, any debate on the question of the technical alternatives − Iron Dome or any other possible system − is pointless.

The more difficult decision must be the decision to limit the amount of money invested in defensive capability in order not to harm the IDF's

offensive capability. This decision requires a thorough discussion of the relationship between defense and offense in general. The Iron Dome system is only the tip of the iceberg of this comprehensive discussion, which is well beyond the scope of this article.

Notes

1 Rocket launchers were first used against Israel on September 16, 1968, when eight 130-mm rockets were shot from the direction of Jordan toward Beit Shean. Davar Correspondent, "For the First Time, Terrorists Use Heavy Weaponry during Shelling of Bet Shean," *Davar*, September 18, 1968, from jpress.org.il, see bit.ly/U2cTmq.

2 This figure is taken from Rafael's web site, www.rafael.co.il.

3 Yael Livnat and Yiftah Carmeli, "IAF Deploys Fifth Iron Dome Battery," IDF Spokesman, November 17, 2012, see bit.ly/11wfOdD.

4 Announcement by Defense Minister Barak as published by the IDF spokesman on August 21, 2012. See bit.ly/11bICrC.

5 Item from *Jane's Defence Weekly*, September 2, 2009. This is also the number of batteries approved by the Foreign Affairs and Defense Committee in February 2011 (UPI, February 11, 2011). Defense Minister Barak repeated this number in his comments to the media during Operation Pillar of Defense. See *Haaretz*, ongoing updates during Operation Pillar of Defense, November 18, 2012.

6 Matan Hetzroni, "Iron Dome to be Upgraded at a Cost of 750 Million Shekels," Channel 2 Online News, November 20, 2012.

7 Yael Livnat, "One Year since Iron Dome's First Interception: Success is due to the Soldiers," IDF Spokesman, April 5, 2012, http://bit.ly/Yo4uRS.

8 These figures are from the Shin Bet's monthly reports, www.shabak.gov.il.

9 Livnat, "One Year since Iron Dome's First Interception."

10 "Summary of Operation Pillar of Defense," IDF Spokesman, November 21, 2012, see http://bit.ly/10QRIKf. According to my calculations, 479 rockets were aimed at built-up areas (421 of which were shot down and 58 of which scored a hit). The interception of 421 out of 479 rockets is a success rate of 87.8 percent. This is the success rate of the system and not of the individual interceptor missile. Although in a number of published videos the interceptor missiles are seen in pairs, we cannot conclude from this that two interceptors were fired at every rocket.

11 The fundamental criticism of anti-missile defense systems relies largely on the tremendous criticism of the American strategic anti-missile defense systems. In Israel, Dr. Reuven Pedatzur, who based himself on the works of Professor Theodore Postol of MIT, has been a particularly prominent critic. Since the early 1990s, Pedatzur has published many articles opposing development of the Arrow. He later criticized in a similar fashion the attempts to develop an anti-rocket defense system. In the late 1990s it was

the Nautilus system, and subsequently, Iron Dome. See Reuven Pedatzur, "The Arrow Project and Active Defense: Challenges and Questions," Memorandum No. 42 (Tel Aviv: Tel Aviv University, Jaffee Center for Strategic Studies, 1993). On Iron Dome, see Reuven Pedatzur, "Iron Dome is Impotent against the Qassam," *Haaretz*, February 21, 2008. Among those who criticize the system on the basis of technological considerations, particularly prominent are supporters of the Skyguard laser system, who have set up a non-profit organization called Home Front Shield for this purpose. The organization's website has a great deal of material on this topic. See http://www.magenlaoref.org.il. A third type of criticism has appeared in reports of the State Comptroller dealing with the procedural and financial side of the decision making process on development of the system.

12 While this paper was prepared for publication, a new series of critical articles were published challenging the data on the system's success rate. While a full answer to the criticism lies beyond the scope of this essay, see Yiftah Shapir, "How Many Rockets Did Iron Dome Shoot Down," *INSS Insight* No. 414, March 21, 2013, http://www.inss.org.il/publications.php?cat=21&incat=&read=11166.

13 See "Nautilus/Skyguard: A Response to the Claims of the Defense Ministry" on the Home Front Shield web site, http://bit.ly/WBLjib. By the way, a search of Northrop Grumman's website (www.northropgrumman.com) no longer turns up any mention of the system (although Google still remembers the page that has information on it).

14 The Home Front Shield web site, http://bit.ly/TD1JFS. As noted, there are no official statistics on Iron Dome's minimum range.

15 Ibid.

16 See Amos Harel and Avi Issacharoff, "Israel's Wake-up Call," *Haaretz*, March 16, 2012, http://bit.ly/whWYrn.

17 Daniel Siroti, "Hamas Declares a Holiday," *Yisrael Hayom Newsletter*, November 22, 2012, http://bit.ly/U9t6pX.

18 Yaakov Katz, "IDF Postpones Final Tests of Iron Dome Defense System," *Jerusalem Post*, December 29, 2010. A simpler calculation shows that this is the area of a circle whose radius is about 5.6 kilometers. Note that the defensive footprint of anti-aircraft or anti-rocket missile systems is not necessarily circular. This information is given for illustrative purposes only.

19 Reuters/AP, "Nasrallah: With Accurate Missiles We Can Hit Hundreds of Thousands of Israelis," *Haaretz*, August 17, 2012, http://bit.ly/NJY20.

20 According to classical deterrence theory, defensive weaponry does not deter. This theory assumes that deterrence is achieved by the threat of weapons of mass destruction, a threat that if carried out cannot be acceptable to the deterred party. Nevertheless, the concept of deterrence has often been raised in discussions of defensive weapons as well. This occurred in Israel in discussions of the Arrow and Iron Dome, and abroad, in discussions of anti-missile defense systems. The theoretical discussion on deterrence

by means of conventional weapons is in any case much more complex than the discussion of "classical" deterrence. See for example, Stephen L. Quackenbush, "National Missile Defense and Deterrence," *Political Research Quarterly* 59, no. 4 (2006): 533-41.

21 See an unsigned article on the website of the Meir Amit Intelligence and Terrorism Information Center, "The War for Consciousness: Although the Latest Round of Fighting in Gaza has Ended with a Negative Balance for the Terrorist Organizations, They are Presenting it as a Victory," March 22, 2012, http://www.terrorism-info.org.il/he/article/17770.

22 One of the fascinating examples was a number of video clips uploaded to the internet during Operation Pillar of Defense showing the simultaneous interception of a large number of rockets over the skies of Beersheba. In my assessment, this shows that the terrorist organizations were attempting to defeat the system by launching a large number of rockets at the same time. On the other hand, the clip also shows the Iron Dome system's capability. See, for example, Shay Malul, "Siren in Beersheba and Twelve Successful Interceptions," http://www.youtube.com/watch?v=8kAyqbKwd1o. In this clip, at least fourteen Iron Dome interceptor missiles can be counted (the Grad rockets are not visible). Explosions from hits can also be counted, but it is impossible to know which of them were in fact interceptions and which were interceptor missiles self-destructing.

23 This argument is made by Uzi Rubin, "'Iron Dome' vs. Grad Rockets: A Dress Rehearsal for an All-Out War," BESA Center Perspectives Papers No. 173, July 3, 2012, http://bit.ly/Q1OZMx.

24 As an example of an article supporting a ground operation, see Yori Yanover, "The Morally Reprehensible 'Iron Dome': Hamas's Best Friend," *Jewish Press*, November 19, 2012, http://bit.ly/XwD1Oy. As an example of an opposing article, see Ari Shavit, "Getting off the Pillar of Defense," *Haaretz*, November 19, 2012, http://bit.ly/ZZNm48.

25 This was the case during the difficult periods of the War of Attrition. See for example "Following Second Katyusha Bombardment against Kiryat Shmona, Serious Warnings to Lebanon by Prime Minister and Defense Minister," *Davar*, May 12, 1970.

26 See, for example, Anshel Pfeffer, "Those Who Rule the Roost: Behind the Scenes of Iron Dome," *Haaretz*, November 23, 2012, http://bit.ly/10oK9v5. A further expression of the public's feeling could be seen on social networking sites. Facebook pages were set up for Iron Dome and received thousands of "likes." An interesting manifestation of the glorification of Iron Dome were the articles praising the decisions by Amir Peretz during his tenure as Minister of Defense. See for example Motti Bassok, "Who Was the First to Identify It? Thus Was Iron Dome Born," *The Marker*, November 19, 2012, bit.ly/Xr2jxy.

Determining Norms for Warfare in New Situations
Between Military Ethics and the Laws of War

Asa Kasher and Amos Yadlin

The ethical doctrine of the war on terror is a set of principles that reflects an orderly conception dealing with the proper ways of conducting warfare against terrorism. Such a doctrine mediates between abstract values such as the "IDF spirit," designed to guide commanders and soldiers' behavior in any circumstances during their operations, and regulations, ROEs, and orders given to guide their behavior in a mission of a certain kind, under specific circumstances, at a specific time, and in a specific place.

The ethical doctrine at the background of this article and the articles published in a previous issue of this journal is the ethical doctrine for fighting terror that was developed in the context of the war between Israel and Palestinian terrorist organizations during the first decade of this century. The writers of this article developed it with the help of a team at the IDF Defense College and with the participation of specialists in anti-terror warfare and IDF and academic specialists in ethics and international law. The doctrine was presented in various official forums, and was subsequently published in professional journals.[1] Although it has not been officially adopted as the IDF ethical code of war on terror, three chiefs of staff who were in office during the period of fighting terror and

Prof. Asa Kasher is the Laura Schwarz-Kipp Professor Emeritus of Professional Ethics and Philosophy of Practice, and Professor Emeritus of Philosophy, Tel Aviv University. Maj. Gen. (ret.) Amos Yadlin, former head of IDF Military Intelligence, is the Director of INSS.

many other officers have expressed support for its principles on various occasions, and many regard it as the Israeli doctrine.

Inaccurate media portrayals of the doctrine triggered responses of various kinds, including opposition to one principle or another that was attributed to us as the authors of the doctrine. Such responses are also reflected in articles published in the previous issue. In the current article and its follow-up, which will be published in the near future, we shall clarify several aspects of the ethical doctrine of the war on terror as we presented it in our articles; respond to a few of the arguments raised against it; and point out a number of updates, pertaining mainly to new situations in the war on terror in the Israeli theater and in other theaters, among them the theaters in Yemen, Afghanistan, Pakistan, and Somalia.

Discussion of the Doctrine: Background Terminology

We will first clarify our general approach to a discussion of the ethical doctrine of fighting terror.

Practicality: A doctrine of warfare should constitute a basis for the practical guidance of commanders and soldiers with respect to their actions in war in the form of a regulation, ROE, or an order. We are therefore interested solely in a discussion that leads to practical conclusions about the possible and proper solutions to operational problems that arise when it becomes necessary to defend the citizens and sovereignty of the state.

Responsibility: A discussion of an ethical doctrine from an essentially critical perspective is liable to emphasize the undesirable aspects of future situations liable to result if commanders and soldiers were to act according to the doctrine. We are interested solely in a discussion that leads to improvements, meaning a revision of the doctrine or its replacement by another, so that the new doctrine will result in fewer situations with undesirable aspects.

Universality: The ethical doctrine of fighting terror was formulated over years of Israeli warfare against Palestinian terror, in which one of the principal means of defense is "targeted killings." The doctrine was designed to survive the test of time by inducing the proper behavior not only in familiar surroundings, but in other times, situations, and locations as well, such as the US campaign in Yemen, which involved the killing of an American civilian as collateral damage,[2] or new kinds of operations such as the US campaign in Pakistan in which Bin Laden was killed.[3]

Caution: In context of a professional or academic discussion of any doctrine, it is assumed that the participants have studied the doctrine as

it was presented, and possess a significant factual basis concerning its contents, principles, and underlying explanations. As far as the ethical doctrine on which this article is based is concerned, the requirement of familiarity with the doctrine is imperative, as frequently it was not properly observed.

The Ethical Doctrine and International Law: An Introduction

The point of departure for the ethical doctrine of the war on terror is not international law. The difference between us and the specialists in international law is no accident and certainly not arbitrary. The reasons for this difference are fundamental and important.

First, the *moral grounds*: For us, the value of international law is not its very existence, but its contribution to the world's moral improvement as regards going to war and the conduct of warfare. Every norm of international law is subject to moral evaluation. When making such an assessment, the norm may be considered successful, or it may be considered unsuccessful, but the point of departure is a moral one.

Second, the *constitutional grounds*: Many perceive international law as a system of norms that are directly binding on the Israeli commander and soldier – a system comparable to the Israeli law that is binding on him as a citizen of the state and as a person in IDF uniform. We regard him (as does Israeli law) as subject solely to Israeli law, which binds him, inter alia, to obey international law to the extent that the state accepts it or regards it as binding and operates according to it. Before a norm of international law reaches the soldier, it must pass tests of its validity according to the law of the state.[4]

Third, the *historic grounds*: Consensual international law emerged through a complex historical development, based on certain conceptions regarding the nature of warfare and the restrictions the leaders and their military advisors could reasonably impose on it. These conceptions served their purpose at the time, namely, a classic conflict between states that involved the classic format of combat between two armies. The restrictions imposed on these conceptions also served their purpose at the time, insofar as there was reason to assume that the parties to the fighting would observe the norms restricting them.[5] The restrictions themselves were practical and even simple: the distinction between combatants and non-combatants, for example, was observed simply by distinguishing between those wearing

a given uniform and those not wearing any uniform. These assumptions underpinned the willingness of leaders to accept the norms contained in the international agreements.

None of these conceptions fits the war on terror. There is no point making assumptions on grounds of the traditional character of war; there are no grounds for an assumption concerning the existence of reciprocity in the observance of the norms restricting warfare, and there is obviously no practical way of observing the restrictions through practical and simple means such as the distinction between those wearing uniforms and those not. These changes in the situation have a negative impact on the willingness to behave according to international agreements, and there is every reason to question their applicability with respect to the new situations.

Fourth, the *rhetorical grounds*: Arguments about violations of international law are expressed through familiar propaganda means against the states fighting terror, particularly Israel, even if they are fraudulent and their factual basis is weak. The media at least in part creates or enhances the propaganda effect of such assertions, especially in Europe as well as in Israel. The overall propaganda effect includes the media portrayal as a factor that creates a negative attitude in international public opinion.

The expression "international public opinion" itself is problematic. It may reflect the opinion prevalent in certain circles that are of secondary or marginal importance in themselves but have a prominent media presence because the media has an interest in making them look good. We do not deny the need for a state to fight on this front as well, but there is no reason to ascribe decisive importance to the question of whether a certain action is portrayed in familiar media as a basis for allegations of violations of international law. Considerations of public image do not take precedence over considerations of self-defense, morality, and military ethics.

The importance we attribute to the difference between our point of departure and that of the devoted advocates of international law does not signify any contempt on our part for international law, as claimed by Eyal Benvenisti in his remarks against "various IDF spokespeople or consultants."[6] In order to understand what Benvenisti regards as "contempt," we can use his description of the danger he sees here: "Such statements are liable to create the impression that Israel has little regard for international law because the law is neither relevant nor moral."[7] According

to Benvenisti, Israel must not believe that the norms in the international agreements are irrelevant to new areas such as fighting terror or cyber warfare. He argues that the relevance of international law to each situation must be a fixed principle of the state. Furthermore, Israel must not believe the norms in international agreements to be immoral and inappropriate to the moral principles underlying its democratic regime, such as the principle of maintaining human dignity. The morality of international law must be a dogmatic principle of the state.

We reject the restrictions imposed by Benvenisti on the views of the democratic state concerning the relevance or morality of the norms in international law. A state is entitled to have a critical view of the relevance or morality of one or another aspect of international law: it is entitled to sign an international agreement, to sign it while objecting to parts of it, and even to conclude that parts of it are irrelevant and require significant addenda, or that parts of it are immoral and require significant change. In the main, the ethical doctrine of the war on terror is a proposal for perfecting international law.[8]

A significant supplement to international law does not imply a relaxation of the rules that bind soldiers and their commanders. On the contrary: as significant examples below will demonstrate, the addendum that we propose in the doctrine sometimes necessitates making the rules more stringent, in other words, the addition of rules that require more restraint and limitations on the use of military force than the existing rules require.

The International Discussion: Navigating in the Fog

The discussion of international law, its content, the extent of its general importance, and its importance from an Israeli perspective takes place on several levels simultaneously, from a very abstract level to a very concrete level. Before reviewing them briefly, the obfuscation typical of the allegations heard in Israel and elsewhere must be noted. For the most part, it is difficult to know which level is referred to by a person who advocates the importance of international law: is he referring to the abstract level, where we totally agree with what he says, or is he referring to the concrete level, where there is room for a critical approach, or even substantial disagreement? This substantial fog is evident in the words of Eyal Benvenisti and Pnina Sharvit Baruch, as well as in the margins

of Avihai Mandelblit's comments, and leads them to draw erroneous conclusions, as we shall see below.

The various levels are:

a. The spirit of international law
b. The international system of institutions, conventions, and customs
c. The doctrines reflected in international conventions
d. The interpretation of international conventions
e. The conceptions of binding customs
f. Applications concerning a given action, both in advance and in retrospect.

We regard the spirit of international law as worthy. It can be portrayed as the principle of an obligation to reduce the calamities of war as much as possible through certain arrangements that impose restrictions on embarking on a just war, as well as restrictions on proper actions during the combat. This principle reflects a long tradition of the "just war theory" with its known principles, such as the requirement that going to war be the last resort when trying to solve a political dispute, the requirement that a proper distinction be drawn between combatants and non-combatants, and the requirement of proportionality.[9] That said, these are abstract requirements, and there is much room between them and regulations, ROEs, and orders in concrete situations.

The spirit of international law has a moral character. Every democratic state should therefore reflect this in its actions because it also stands for moral principles in maintaining human dignity for all people. As a democratic state, Israel is also committed to maintaining the spirit of international law. No one among us disputes this.

The international system includes institutions such as the UN, with the Security Council at its center; international conventions that states take open themselves to observe based on diverse considerations, such as various conventions for fighting terror; and customs capable of becoming global customs of a binding character. The actions of this international system are supposed to realize the spirit of international law, and as such are morally important.

At the same time, the international system is operated by states, each of which acts according to its own considerations. The international system is therefore a political system, many of whose actions enable it to act immorally in the guise of the pursuit of peace and justice.

Two recent examples illustrate this observation. The first is the International Criminal Court (ICC), which is entitled to conduct a hearing concerning the actions of a state that is not a signatory to the convention that established it – but only if the Security Council requests that it do so. States with a power of veto in the Security Council do not permit such applications against their allies: Russia and China where Syria is involved, and the US where Bahrain and Yemen, not to mention Israel, are involved. The second example is the Global Counter-Terrorism Forum (GCTF), established at the behest of the US, which includes 29 states and the European Union, but does not include Israel,[10] probably because of opposition from Turkey, which serves with the US as a co-chair of the Forum. Although the international system acts to realize the spirit of international law, it does it selectively, which is inherently unfair.[11]

Political wisdom calls for cautious treatment of the international system: identification with its goals of promoting peace and maintaining human dignity in accordance with the spirit of international law, but also the constant exercise of judgment with respect to the extent and format of cooperation with its institutions, accession to its conventions, and acceptance of its customs. It appears that this has traditionally been Israel's general position, and presumably acceptable to all of us.

The rules that appear in international conventions, such as the parts of The Hague Convention pertaining to ground warfare (1907), reflect doctrines of war that are general and complicated conceptions concerning certain aspects of warfare. For example, the provisions of Chapter One of the Convention[12] constitute just such a conception of the nature of a party fighting in a war: not only is an army involved, but also quasi-military bodies fulfilling certain conditions such as a responsible command and the open bearing of arms. These rules reflect the spirit of international law (in the tradition of the just war theory) in a way that facilitates the transition from its abstract principles to the concrete level of regulations, ROEs, and orders. Insofar as the conceptions reflected in the rules help to apply the spirit of international law in practice, they are useful and morally valuable.

However these conceptions are neither simple nor harmless, because they are based on factual assumptions that may be incorrect and the practical conclusions resulting from them may be inappropriate. For example, one incorrect factual assumption posits that a distinction can be made between combatants and non-combatants by means of a "recognizable symbol that

can be discerned at a distance."[13] In the circumstances of the war on terror, this assumption is incorrect, as everyone knows. For example, a practical conclusion of the rules is that every soldier who belongs to the side that is waging a just war of clear self-defense is a legitimate target for deadly attack by the side that is waging an unjust war against him. This conclusion continues to arouse trenchant, persuasive moral opposition.[14]

What is the appropriate attitude toward a doctrine that reflects the rules of the international convention, given the possibility that it is based on factually incorrect assumptions, or leads to inappropriate practical conclusions? On the theoretical level, the answer is simple: it is appropriate to develop an additional doctrine, based on factually correct assumptions, which leads to appropriate – or at least more appropriate –conclusions, and which also embodies the spirit of international law in the framework of the international system. This is how the ethical doctrine of the war on terror should be understood on a theoretical level, as presented in our study.

On a practical level, the answer is much more complex. Here the following question can be posed: Which policy is the most desirable with respect to a problematic doctrine that is grounded in the spirit of international law, acceptable in the framework of the international system, and expressed in a binding international convention? There is no comprehensive answer to this question because the inappropriate practical conclusions of the given doctrine are on one side of the scale and the undesirable consequences of disavowing one of the accepted elements of the international system and a binding international convention are on the other. One side of the scale does not always outweigh the other.

It is possible to act in a way that creates an undesirable impression of such a disavowal. If the given doctrine is based on a factual assumption that is incorrect under circumstances of a certain type, such as the war on terror in its current configuration, it can still be observed in circumstances of a different type, in which this factual assumption *is* correct, such as a frontal military conflict between two armies. In this way, it is possible to propose an additional doctrine and to act according to it as long as its assumptions are correct. Thus, two doctrines exist side by side that are grounded in the spirit of international law in the framework of the international system, each of which being used under different conditions, depending on the underlying factual assumptions. This format precludes any undesirable disavowal in the international theater and any use of a doctrine whose

fundamental assumptions are incorrect. This is how the ethical doctrine of the war on terror, as we have proposed it, should be understood.

Is this approach explicitly or tacitly acceptable to all of us? The point is addressed below, following a discussion of the next level – the interpretation level.

The possibility of guiding the commanders' and soldiers' conduct on the basis of the interpretation of international law is accepted among the participants in the discussion. Mandelblit writes, "Therefore it is necessary to maintain the existing, traditional rules governing the laws of warfare and apply them fully, at the same time furnishing *an interpretation that is suitable* to the challenges of asymmetrical fighting."[15] He does not explain what a "suitable interpretation" is, how it should be determined, or who should make it, but we shall respond to these questions later. Benvenisti writes, "The laws of warfare have essentially remained unchanged, but *they must adapt* to the reality of the power of control."[16]

Sharvit Baruch includes a similar sentence in her remarks, but adds examples to illustrate her point: "With regard to asymmetrical conflicts, there are already existing principles and rules that can and should *be applied in a way that takes into account the particular reality* of such conflicts."[17] The conception of interpretation does not appear in her essay, but there is no logical difference between an interpretation of the rules and applying them "in a way that takes into account" special aspects of the given situation in the combat.

In order to demonstrate her argument, Sharvit Baruch presents several important examples, the rules of aerial warfare among them: "When aerial warfare began, *there were naturally no rules about it*." Over time, states engaged in aerial warfare "acted in a certain manner...and on this basis *the relevant rules were formulated. These rules were based on the already existing principles and rules of the laws of warfare regarding fighting on land and at sea, with the requisite modifications made to them*."[18] Another example she gives is taken from the realm of cyber warfare: "Here too, *the new rules are based on existing ones with the requisite modifications*."[19] We will soon see what these examples mean for the ethical doctrine under discussion, but first we mention another example cited by Sharvit Baruch in the area of the war on terror, which is the domain of our doctrine.

"In 'classical wars,' there was[20] a relatively sharp distinction between combatants and civilians. Soldiers are the combatants and are considered

legitimate targets... while civilians (that is, those who are not soldiers) are not considered legitimate targets. However, what does one do when on the enemy's side there are no soldiers, but rather armed civilians, at various levels of organization, who do not necessarily fight all the time and who are difficult to distinguish from the rest of the population?" Here Sharvit Baruch adds several instructive points: "as the IDF's legal advisors, we felt that it is incorrect to view all members of the armed organizations as civilians directly participating in hostilities; it would be more appropriate to define those who are part of the enemy's fighting forces and have functions that are parallel to those of soldiers in a regular army as combatants who have no immunity against attack as long as they belong to these forces."[21]

Here we should call a spade a spade: what the "legal advisors" like Sharvit Baruch were proposing to the IDF was a new doctrine of the war on terror in the spirit of the given international law.

No commentary appears as to what constitutes appropriate interpretation of the existing traditional rules, to use Mandelblit's terminology. Under the heading, "applied [existing principles and rules] in a way that takes into account the particular reality," to use Sharvit Baruch's terminology, there is no application of existing principles and rules. What does appear under these two headings is a new doctrine of war on terror in the spirit of the given international law, whose original subject was classic warfare. As a matter of fact, Sharvit Baruch's examples show that new rules, defined in the spirit of the existing rules, are involved. Benvenisti outdoes them all; he describes the change that is to take place following the prevalent use of sophisticated technologies that make accurate strikes possible as follows: "Legally speaking, there is a transition from the realm of private law, such as enforcing a contract between two sides, to the realm of public law, which supervises the exercise of authority by decision makers, regulatory bodies, the people in power, the people in charge, and those who decide whom to attack...when to attack, how to attack, and how much collateral damage they cause."[22] These, then, are new rules in the framework of a comprehensive legal conception that can differ from its predecessor.

In other words, our ethical doctrine is not alone in proposing new rules in the spirit of the familiar international law, based on the theory of a just war; those advocates of international law who criticize us for this are doing exactly the same thing. There is no difference of principle or

practice between their treatment of the given international law and ours: we are both adding new rules to it. What, then, is the difference between their approach and ours?

We found two differences between our approach and the approach of the international law disciples in the three articles that we are discussing. The first difference is rhetorical. They wish to portray the behavior of Israel, particularly of the IDF, as conforming to the existing rules of international law. Such a portrayal is designed, both from the outset and in retrospect, to counter any hostile argument accusing Israel, especially the IDF, of violating those rules. Our ethical doctrine is worded differently: Israel and the IDF are acting in the spirit of the existing rules of international law according to new doctrines that amount to supplements to the existing rules, while conforming to the spirit of the latter. In fact, we are not the only ones doing this; other states fighting terror are also doing it. Sharvit Baruch herself refers to "the accepted understanding by the US Army and NATO forces" whereby "those who comprise the armed forces of any side to the conflict, even if that side is a non-state element, are not civilians; rather, they are combatants, analogous to regular soldiers, in terms of the application of the principle of distinction."[23]

The truth is that there is no way to avoid the introduction of new rules and new doctrines in the spirit of international law. Below, we cite in greater detail important examples of the new rules proposed in the spirit of international law, such as rules requiring minimizing of collateral damage, beyond the accepted rules that dictate proportionality. At this stage, we will limit ourselves to an extremely simple example. In the course of the discussion following which the articles under discussion were written, in response to our assertion that not only medical staff but also mental health officers are deserving of special consideration in the spirit of the 1st Geneva Convention, which grants medical staff special status,[24] a senior Red Cross representative stated that mental health officers were considered medical staff entitled to special status. The recognition of mental health officers as entitled to special status is not an "interpretation" of the term "medical staff," nor is it the "application" of this expression to the treatment of mental health officers. It is a new rule in international law expressing a conception concerning the place of a mental health officer, who is often a social worker or a psychologist, alongside the physician, the nurse, the paramedic (and the chaplain, who is protected under the same clause),

which is in the spirit of the international law dealing with medical staff, but expands it by adding a new rule. The actual expansion of a group of people with a specific status amounts to the addition of a new rule, even if that expansion appears to be natural.

The rhetoric of "maintaining the existing rules," while "interpreting" or "applying" them according to the special circumstances of the war on terror, may have advantages in the field of public relations, but it is important to avoid allowing the norms of propaganda, public relations, media, or psychological warfare to filter down into the professional understanding of the requisite activity. This rhetoric cannot and should not conceal the fact that what is involved is the development of new doctrines.

Furthermore, the general rhetoric of completely and absolutely "maintaining the existing rules" subverts the important decision by Israel not to ratify the 1977 Protocol 1 Supplementary Amendment to the Geneva Convention; this was designed to enforce accepted rules of behavior in classic warfare in a conflict between a state and guerilla fighters who blur the difference between non-combatants in the vicinity and themselves. Israel was not the only state to refrain from ratifying this protocol: the US did not ratify it, while Australia, the UK, Germany, France, Canada, and other states added a reservation to their ratification, stating that they did not accept some of the new rules.

The International Committee of the Red Cross (ICRC) is trying to make the rules of the supplementary protocol binding on all states, whether or not they have ratified it at all, or whether they have ratified it completely or in part. It did so in a 2005 document[25] asserting that the rules of the supplementary protocol constituted customary international law, namely, a system of rules that states observe in practice. This assertion is controversial;[26] as a state that has not ratified the protocol itself, Israel certainly does not accept it. All inclusive statements about "maintaining the existing rules" are liable to be interpreted as general assertions of a commitment to observe what Israel has not taken upon itself. This is the danger arising from the rhetoric used by the devoted advocates of international law, who in effect are pushing Israel into a diplomatic and military corner where it has decided it does not want to be. The way we are presenting the ethical doctrine does not incur such a risk.

At this point, it is appropriate to comment on the conception of the proper behavior by a state in an area in which "international law is

developing." Sharvit Baruch believes that this expectation, that is, to "convene the representatives of all the nations in the world and agree on a new convention that would grant greater freedom of action to armies in asymmetrical conflicts" is "totally out of touch with international reality."[27] First of all, it is not clear why Sharvit Baruch believes that the substance of the international agreement is "greater freedom of action for armies in asymmetrical conflicts." The substance is agreeing with a new doctrine that will impose restrictions in the spirit of international law (in the tradition of the just war theory) in a way that will be appropriate to the nature of the conflict with terrorists. Such a doctrine is not meant to be tested according to the freedom of action it grants as compared with the doctrine for classic warfare. It may contain new restrictions, just as it may contain provisions allowing more freedom of action. Furthermore, it is unclear why Sharvit Baruch is convinced that there is no point in any international agreement unless "all the nations in the world" are parties to it. If we omit the rhetorical "all the nations of the world" requirement and confine ourselves to democratic states involved in the war on terrorism, there is no basis in "international reality" for assuming that the acceptance by the democratic world of a doctrine of war on terror in the spirit of international law is "totally out of touch with international reality."[28]

In an incidental remark, Sharvit Baruch indicated another direction for development: "The rules are practical and adapted to reality…consolidating practice in accordance with the changing reality."[29] With respect to the possibility of "adapting the rules," we have already seen above that this defensive rhetoric overlooks the fact that what is actually involved is the introduction of new doctrines regarding the "changing reality." Furthermore, "consolidating practice" is also nothing but the formulation of a new doctrine for guiding practice. Insofar as international law is developing in the area of customs, it is obvious that we can formulate new doctrines and act according to them in the spirit of international law (in the tradition of the just war theory). At the same time, in a persistent effort to shape the practice of the democratic world in its war against terrorists, we can learn from the new doctrines of other democratic states that are also fighting terrorists. Our ethical doctrines are designed to contribute to this effort to develop customary international law.

Another difference between our approach and that of the advocates of international law is that their approach results from professional activity in

the field of international law, while ours results from professional activity in the fields of command and ethics. The rhetorical use of terminology such as "interpretation" and "application" is designed to leave the job of developing new doctrines to the international law disciples. In our opinion, this is not a legal task, just as the task of designing the values and principles that should guide the conduct of a state, an organization, a profession, or a business corporation is not entrusted to the legal advisors of these entities. The state's values and principles are determined in the Knesset; the university's values are determined by its academic leadership, not its legal advisors. The values of medicine were formulated in the world of the physicians, with the help of medical ethics specialists. The values of a construction company will be determined by its specialists in issues of its identity, with the help of some advisors.

In Israel, the boundaries between the realm of law and the realm of ethics are often excessively blurred.[30] It is unacceptable, however, to allow this confusion to create the impression that lawyers are responsible for developing new doctrines. Nor does the obligation to develop new doctrines in the spirit of existing international law require that the job be left to jurists: the spirit of international law is the just war theory, which is a set of traditional principles that continues to be a topic of discussion in philosophy, political science, history, theology, and law.

There is therefore no difference of substance between our approach and those of Benvenisti, Mandelblit, and Sharvit Baruch concerning an accurate description of the requisite activity under the current circumstances. "The IDF, like any army of a law-abiding nation in the West," asserts Mandelblit, "is committed to scrupulous observance of the requirements of the laws of warfare."[31] What are these "requirements"? Let us be forthright: these are the requirements to act in the spirit of recognized international law in the form of new rules added to it in compliance with its spirit. That is what we all know should be done. That is what we are all doing. "The existing rules of the laws of warfare are the correct and appropriate system even when dealing with asymmetrical conflicts," Sharvit Baruch argues.[32] What are these "existing rules"? If they refer to the abstract principles of the spirit of international law (in the tradition of the just war theory), there is no disagreement between us. If, however, they refer to the rules expressed in the articles of the Geneva Convention, for example, then Sharvit Baruch herself does not act according to her argument, since she develops new

rules under the misleading heading of "applying" the existing rules, as if "applying" the rule about "medical staff" makes it possible to include mental health staff, which is non-medical, as part of it; as if "applying" the rule about proportionality makes it possible to require much more, such as minimizing collateral damage, and so on. A responsible description of the customary practice in the ethical and normative training of commanders and soldiers leads us out of the fog to the clear recognition of the obligation to develop new doctrines, based on the state's ethical conceptions, particularly those of the IDF (and the Israel security agency, the General Security Service).

Noting What is Off Target

The critical position expressed in terms of "maintaining the rules of international law as is" is correct, as far as the principles of the spirit of international law and the just war theory are concerned. It is incorrect when more detailed rules designed to guide commanders and soldiers are involved. The slogan, "maintaining the rules as is," without any admission that significant new conceptions, doctrines, and rules are being introduced, moves those who use it to be interested in describing their position in terms that distinguish it from anything expressed in our ethical doctrine. We therefore find ourselves witnessing a series of false descriptions that attribute to us stances that have never been ours, and which we have never stated.[33] We will thus give several examples of these false descriptions, and clarify our stance on the issues involved in them.

Sharvit Baruch seeks to express a middle-of-the-road position: "In my opinion... the existing rules of the laws of warfare are the correct and appropriate system,"[34] which also means objecting to two different and opposing types of positions. "The first [position] is that existing rules are unsuited to these conflicts because they allow a disproportionate use of force liable to harm the civilian population...Therefore, in places where there is no organized state that is capable of protecting its citizens, but rather non-state elements that do not consider the welfare of their population to be their first priority, because they lack either the will or the ability to do so, it becomes the obligation of the other side to exercise particular caution with regard to that population."[35]

According to the second position, "when fighting in densely populated areas against non-state elements, especially those that do not honor the

basic rules of war and do nothing to distinguish themselves from the civilian population, fewer restrictions should be imposed on the use of force...According to this argument, the existing rules are irrelevant and should be ignored, or at least their restrictions should be lifted, because otherwise one side must fight with one hand tied behind its back."[36] Since Sharvit Baruch does not quote or provide footnotes, we must ask where our position and arguments belong in her picture: in the first category of positions, or in the second?

If we dispense with the obfuscations that Sharvit Baruch brings to the discussion with her slogan of "the existing rules... are the correct and appropriate system," an interesting picture emerges: insofar as the spirit of international law (or the traditional just war theory) is involved, there is no difference between Sharvit Baruch's position and our own; this was already explained above. Once we switch to doctrines that can be used in a conflict of the current type, however, our doctrine belongs in neither Sharvit Baruch's first category nor her second one.

Our doctrine does not belong in the first category because, among other things, we ascribe decisive importance to the question of effective control of the territory in which war is being waged. A state bears responsibility for the fate of every person in a territory over which it exercises effective control, and does not bear a corresponding responsibility to exercise "a greater obligation of caution" involving people in a territory over which it does not exercise effective control. Incidentally, this is another significant example in which our ethical doctrine is more stringent than the accepted rules of international law.

Our doctrine does not belong in the second category either because, among other things, it does not involve a claim that the "existing rules" should be "ignored," or "their restrictions should be lifted." When we argue that the doctrine of international law in its recognized format is inappropriate for the current conflict, we are not ignoring the rules, since we definitely wish to maintain their spirit and develop a corresponding doctrine that is appropriate to the current conflict and is based on the same principles of the spirit of international law (in the tradition of the just war theory). We did not create our doctrine in order to "ease restrictions"; we sought to define other corresponding rules suitable to the current conflict.

The rules in our doctrine frequently restrict the use of force more than the general allowances made under international law. For example, in the

spirit of the distinction principle, which is in the spirit of international law and corresponds to the general distinction between combatants and non-combatants in classic warfare, we defined a rule of graded distinction according to the risk level of the contribution to terrorist activity. Moreover, while the principle of proportionality, which is also in the spirit of international law, requires that the military benefit derived from an action liable to cause collateral damage justify such damage, or in other words, bars excessive force, our doctrine requires that an effort be made to minimize the damage. Inter alia, such an effort requires continual examination of the possibility of using sophisticated weaponry.[37] Since non-minimal damage can be both proportional and non-excessive, here too the rules of our doctrine restrict the use of force more than the recognized rules of international law.[38]

An important comparison of our doctrine with the rules of international law arises from the ruling of the High Court of Justice on targeted killings.[39] Although Chief Justice (ret.) of the Supreme Court Aharon Barak discusses the propriety of actions such as targeted killings on the basis of the customary international law and Israeli law, his conclusions regarding the distinction between what is permitted and what is forbidden in military operations of this type are very similar to the conclusions arising from our ethical doctrine. Two differences emerge from the comparison between his legal argument and our ethical argument. First, the norm of customary international law requires an independent retrospective examination of the action. While we do not regard ourselves as being among the enthusiastic advocates of a suspicious and distrustful attitude toward every military action, our ethical doctrine does not contradict this norm with respect to an independent and professional retrospective examination. In the future, we will include it in the presentation of the doctrine. Second, the ruling states that it is better to arrest, investigate, and judge a terrorist than to kill him, insofar as this is possible [Section 40 of Chief Justice (ret.) Barak's opinion]. This is also the conclusion that is reached from our doctrine. In this context, the ruling deals explicitly with "conditions of seizure of territory during combat in which the army controls the area where the operation is conducted," so that arrest, interrogation, and trial are "possibilities that can sometimes be realized." The ruling exempts the army from the duty to implement such a possibility when the anticipated

collateral damage resulting from it is greater than the collateral damage anticipated from killing the terrorist in a targeted killing.

Here the conclusions in the ruling differ from our conclusions. In our opinion, it is improper to act in a way that creates a real risk of collateral damage when the territory seized during combat is subject to effective control by the army, because in such a territory, the army is responsible for the protection of every person who is not a participant in hostile action. The army's ethical and legal justification for imposing restrictions on such a person does not include justification for killing him as a result of killing a terrorist.[40] According to our approach, there is no justification for causing any collateral damage whatsoever in territory under the effective control of the army.

Of the many examples of the discrepancy between Sharvit Baruch's reasoning and our doctrine, we will mention only one more:[41] "Another point raised by those in favor of this argument [of the second type] is that it is unfair to demand that one side of the conflict honor the rules while the other side willfully ignores them."[42] This argument is unacceptable to us, and insofar as it is directed against us, reflects an important misunderstanding of what we are saying.

The principle of reciprocity in the observance of the rules of international law is important on two counts. First, it is of military, political, ethical, and moral importance: Does the violation of the rules by one party alter the definition of "what is permissible and what is forbidden" for the other party, which is suffering from the violation? For example, if one party violates the rules by making extensive use of chemical weapons, thereby gaining a significant military advantage, should the other side continue to observe the rules in the same way, even if it thereby incurs the risk of military collapse? Many consider a positive answer to this question unreasonable and even intolerable in practice.[43]

This uncompromising demand is one of the innovations of the above-mentioned 1977 additional protocol. It is unacceptable to us (and to certain states, including the US). On the other hand, general permission for every possible violation of the rules after the enemy has broken them, or some of them, is both unreasonable and intolerable. The fundamental goal of reducing war calamities as much as possible without abandoning the sustained effort to achieve victory remains unaltered. Given a violation of the rules by the enemy, the question is therefore to what degree, and under

what conditions, the definition of what is permissible and what is forbidden changes. Our doctrine assumes that the terrorist enemy is violating the rules at the level of the spirit of international law (and the principles of just war theory); at the same time, it is understood that absolutely no blanket permission to ignore the rules at this level is granted.

Second, at a level that is regrettably addressed by few, the reciprocity principle plays a role in the dialogue on justification between a state and its soldiers.[44] A democratic state is committed to the human dignity of its citizens, including its soldiers. Because maintaining human dignity also includes preserving human life, a democratic state owes its soldiers a clear justification for any decision it makes to place them in dangerous situations. Obviously, such justification is not given to a soldier under fire; a state formulates its justification for itself in advance, and gives it to its soldiers at the appropriate time. The justification for obeying the rules of international law is based on the state's decision to undertake to behave according to these rules. The soldier is entitled to ask the state why it is imposing on him the obligation to behave according to those rules, even when this weakens its military power. The state's response will include, among other things, the political wisdom reflected in its commitment to such behavior. Part of this political wisdom is expressed in the expected implementation of the reciprocity rule: it is good for us to limit ourselves to some extent, so that our counterpart on the other side will limit himself in the same or at least in a similar way. What happens to this justification in terms of the "political wisdom" when it is clear to the soldier that the reciprocity principle is never observed at the front?

Here the state cannot avoid a basic change in the justification of its actions − from the terms of the "political wisdom" underlying the reciprocity principle to the terms of what all of us regard as "the basic values of our state."[45] The first principle of our doctrine states not only a state's obligation to protect its citizens, but also its obligation to do so while constantly respecting the human dignity of every person as such. Here, again, our critics are breaking and entering when the door is wide open.

In conclusion, we regard the spirit of international law as an important compass in formulating the military ethics of the war on terror. At the same time, in their current version, the rules of international law require supplements in the form of new doctrines such as our ethical doctrine for the war on terror. Democratic states, including Israel, should be supplied

with doctrines that will properly guide them when they find themselves in a hazardous conflict with an enemy – not merely in the wars that are familiar from the past, but also in the newer wars, in which the enemy is a local organization or a global network of organizations rather than a state, or in which the enemy uses terrorism deliberately and continually, or in which the conflict takes place in the cyber sphere. Doctrines like these will not be considered interpretations of existing international law; rather, they will constitute significant addenda in the spirit of the familiar and acceptable international law.

Notes

The authors would like to thank Prof. Yaffa Zilbershats for her useful comments on the draft of this article, and an anonymous reader on behalf of this journal for important comments on the previous version of the article.

1 Asa Kasher and Amos Yadlin, "Military Ethics of Fighting Terror: An Israeli Perspective," *Journal of Military Ethics* 4, no. 1 (2005): 3-32, 60-70; Asa Kasher and Amos Yadlin, "Assassination and Preventive Killing," *SAIS Review* 25, no.1 (2005): 41-57; Asa Kasher and Amos Yadlin, "The Military Ethics of Fighting Terror: Principles and Explanations," *Scales of Justice* 6 (2007): 387-419 (Hebrew translation of the first article in English); Asa Kasher, "Operation Cast Lead and the Ethics of Just War," *Azure* 35 (2009): 29-55; Asa Kasher, "Operation Cast Lead and the Ethics of Just War," *Azure* 37 (2009): 43-75 (English translation of the preceding article).

2 See: topics.nytimes.com/reference/timestopics/people/a/anwar_al_awlaki/index.html. The terrorist was Anwar al-Aulaqi; Samir Khan, the editor of an al-Qaeda newspaper, was killed by his side, even though he did not appear on the designated list for targeted killing. The decision by a democratic state to allow the killing of its citizen as collateral damage of an action against a dangerous leading terrorist is a questionable decision of a new kind. It is questionable because a state's obligation to its citizens is usually to protect them, and certainly not to harm them. The decision is of a new kind because no such permission had been granted up to that point. The targeted killings carried out by Israel against Palestinian terrorists caused collateral damage, but not among Israeli citizens. This problem is discussed in the follow-up article to this article.

3 Peter L. Bergen, *Manhunt: The Ten-Year Search for Bin Laden – from 9/11 to Abbottabad* (New York: Crown, 2012). The decision to permit the killing of Bin Laden unless "he conspicuously surrenders" is questionable. On the one hand, he could have been captured alive, even if he had not "conspicuously surrendered" but had frozen during the first few seconds of contact with US Naval Seals. On the other hand, he headed a quasi-military organization that fought against the US, and it might therefore have been permissible to kill

him in order to avoid jeopardy even if it is of low probability. This problem is discussed in the follow-up article to this article.

4 In this context, a question can be raised concerning the most basic norms of international law (*jus cogens*) – those that are accepted by the community of the world's states as incontestable, binding norms, such as the ban on torture (in a specific sense of this expression). Are such norms directly binding on soldiers, or are they binding on the soldier because his state admits that they are binding on it and on those acting on its behalf? The follow-up article to this article deals with this question as well, and argues that even such basic norms are indirectly binding on the soldier through the state's mediation, and not directly binding on him.

5 This is an important assumption whose moral consequences, and the policies arising from it, should be thoroughly discussed. We mention here that there are norms, such as the obligation to behave properly toward POWs, which have been honored to an impressive extent, just as there are others, such as the obligation to avoid deliberate harm to civilian population, that have been clearly violated, such as the London blitz on the one hand and the dropping of atomic bombs on Hiroshima and Nagasaki on the other.

6 Eyal Benvenisti, "How the Challenges of Warfare Influence the Laws of Warfare," *Military and Strategic Affairs* 4, no. 1 (2012), p. 38.

7 Ibid.

8 If Benvenisti believes that the impression created by our statements concerning the ethical doctrine constitutes a concrete danger, perhaps he might attempt to show that this impression is erroneous. Anyone who read our work and did not rely on journalists' impressions of them did not regard them as reflecting "contempt" of the kind attributed to us by Benvenisti. We will return to this point in the next section.

9 Michael Walzer's book, *Just and Unjust Wars* (Tel Aviv: Am Oved, 1984), is a detailed and important presentation of this theory. The English-language editions of this book are occasionally revised by the addition of a preface dealing briefly with additional wars. The fourth edition of the book appeared in 2006.

10 See the US State Department website: http://www.state.gov/r/pa/prs/ps/2011/09/172010.htm.

11 In 2012, a concrete possibility arose of Sudan becoming a member of the UN Human Rights Council as one of the African members; however, Sudan waived the appointment. The International Criminal Court in The Hague issued two arrest warrants against Sudan President Omar al-Bashir: in 2009 for war crimes, and in 2010 for genocide. When a state can be a member of the UN Human Rights Council even when its president is wanted by the International Criminal Court for genocide, crimes against humanity, and war crimes, what degree of confidence should be accorded an international system that permits this combination?

12 Appendix to the Convention Concerning the Laws and Customs of War on Land, Part 1, Chapter 1, Sections 1-3.
13 Ibid., Section 1, Condition 2. The tendency to give an exemption from the obligation for identification by means of uniforms in order to accommodate "freedom fighters" or those fighting "for self-determination" is evidence of political currents operating in the depths of the development of international law, but we will not discuss this in detail.
14 For example: Jeff McMahan, *Killing in War* (Oxford: Clarendon Press, 2009).
15 Avihai Mandelblit, "Lawfare – The Legal Front of the IDF," *Military and Strategic Affairs* 4, no. 1 (2012), p. 55, emphasis added.
16 Benvenisti, "How the Challenges of Warfare Influence the Laws of Warfare," p. 34, emphasis added.
17 Pnina Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," *Military and Strategic Affairs* 4, no. 1 (2012), p. 41, emphasis added. How laws of warfare are adapted is a complex issue, and will be discussed further below.
18 Ibid., emphasis added.
19 Ibid., emphasis added.
20 It is not clear why Sharvit Baruch here and elsewhere in the essay uses the past and not the present tense. It would appear that she, like us, contends that the laws of classical warfare are still applicable.
21 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 42.
22 Benvenisti, "How the Challenges of Warfare Influence the Laws of Warfare," p. 34.
23 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 42.
24 Chapter 4, Section 24.
25 ICRC, "Customary International Humanitarian Law," http://www.icrc.org/eng/war-and-law/treaties-customary-law/customary-law/index.jsp.
26 For example, see Jeremy Rabkin, "Lawfare," *Jewish Review of Books* 3, no. 2 (2012): 29-32.
27 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 49.
28 Perhaps it is not superfluous to mention that even given the difficulty in achieving general international agreement, an attempt to formulate such an agreement is still useful. An important example from "the international reality" is the ongoing effort in the UN to devise a universal definition of terrorism in the framework of a comprehensive international convention for waging war against it.
29 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 41.
30 See Asa Kasher, "Professional Ethics and Collective Professional Autonomy: A Conceptual Analysis," *Ethical Perspectives* 12, no. 1 (2005): 67-98; see also "Professional Ethics," in *Introduction to Ethics A*, ed. Asa Kasher (Jerusalem: Jerusalem Center for Ethics, 2009), pp. 1-20, and Yitzhak Zamir, "Ethics and Law," in *Introduction to Ethics A*, pp. 21-33.
31 Mandelblit, "Lawfare – The Legal Front of the IDF," p. 55.

32 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 40.
33 An odd phenomenon that accompanies this tendency toward false descriptions is the absence of any reference to what was said in our articles. The reader will search in vain in the critical articles before us for any example of an argument attributed to us. Is it possible that the critics drew themselves a picture of our opinions on the basis of various newspaper stories without reading our articles themselves? In this matter, see the requirement for caution that we stipulated in Section 1.
34 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 40.
35 Ibid, p. 39.
36 Ibid., p. 40.
37 On this point, Benvenisti's statements are consistent with our doctrine, which portrays technology as a focal point that characterizes the current war. See Benvenisti, "How the Challenges of Warfare Influence the Laws of Warfare," p. 34.
38 Section 44 of Supreme Court Chief Justice (ret.) Barak's High Court of Justice ruling on targeted killings (769/02) discusses only the "narrow meaning" of proportionality, namely, the relation "between the military target and the civilian damage," even though the existence of other elements of proportionality in international law is mentioned. Our ethical doctrine contains elements beyond the "narrow meaning," as we have just seen.
39 High Court of Justice Ruling 769/02 was issued on December 14, 2006, long after after our ethical doctrine was published. One of our articles in which our doctrine is presented is mentioned in the ruling.
40 In another place, the ruling quotes Section 27 of the 4th Geneva Convention, which requires protection of the dignity of a person who is not a participant in hostile action in a territory that has been occupied in combat, subject to limitations on the means of supervision and security [Section 23 of Chief Justice (ret.) Barak's ruling].
41 Another important example is the attitude toward the terrorists' non-dangerous civilian surroundings, which we will address in the follow-up article.
42 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 48.
43 For an enlightening discussion of the possibilities of "combat retaliation," see Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict,* 2nd ed.(Cambridge: Cambridge University Press, 2010), pp. 253-60.
44 Asa Kasher, "The Principle of Distinction," *Journal of Military Ethics* 6, no. 2 (2007): 152-67.
45 Sharvit Baruch, "Legal Dilemmas in Fighting Asymmetrical Conflicts," p. 48.

Duqu's Dilemma: The Ambiguity Assertion and the Futility of Sanitized Cyberwar

Matthew Crosston

The debate over the applicability or non-applicability of international law to cyberwar and the need for a cyber-specific international treaty might be irrelevant. Both camps, pro and con, argue about the need for cyberwar to have the Law of Armed Conflict (LOAC) or some new international legislation properly cover the cyber domain. Both camps, however, misread how the structure of the cyber domain precludes strategically "piggybacking" on conventional norms of war. International laws on conventional war are effective because of the ability to differentiate between civilian and military sectors. There is a civilian/military ambiguity in the cyber domain that makes such differentiation unlikely if not impossible well into the future.

Hence "Duqu's Dilemma": with the focus on establishing legitimate targets and setting limitations on allowable action, the United States and its allies expose themselves to vulnerabilities while engaging in a futile endeavor that does not lead to improved cyber control. The effort to establish cyber rules akin to conventional norms is fruitless since these rules are not enforceable or logical. They will simply handcuff lawful states. This signifies that greater effort should be expended on creating preemptive strategy that accepts the military/civilian ambiguity problem. The tendency of scholars and policymakers to strive for "sanitized" cyberwar by constraining targets during operations means that cyber strategy remains devoid of true deterring power.

Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and Founder and Director of the International Security and Intelligence Studies (ISIS) program at Bellevue University.

Whether one believes LOAC can or cannot apply to the cyber domain, whether one pushes for an international cyber treaty or thinks such treaties will be meaningless, one aspect is constant: the desire for rules governing cyberwar behavior. The problem is in attempting to create a code of cyber conduct that demands a distinct separation between civilian and military sectors. The cyber domain is not amenable to this separation since the aforementioned fusion, where participants, facilities, and targets are hopelessly entangled between civilian and military institutions, has basically been a missing explanation as to why the global effort to enhance and clarify norms has remained uneven and inadequate.

The Ineffectiveness of International Law

Addressing the issue of cyber security, the East-West Institute stated in 2011, "There is an urgent need for international cooperation on this most strategic of issues. If we fail on this task, global stability could be as threatened as it would be by a nuclear exchange."[1] International norms established with the Geneva and Hague conventions were meant to be explicit lines of protection for civilian populations when states engaged in war. That respect for and preservation of civilian life is now held to be sacrosanct, regardless of what form or delivery method war takes. As such, there is an expectation that cyberspace can be subjected to the discipline of conventional norms.

Others argue that establishing these customary understandings in the cyber domain is one of the most important geopolitical battles today, going so far as to say that it is Ground Zero for global diplomacy, national security work, and intelligence.[2] The goal is to bring the principles of arms control into the cyber domain. Indeed, the most optimistic want voluntary agreements that impose constraints on the development of cyber capabilities and ostensibly ameliorate behavior in cyberspace. Some, however, have acknowledged that there are potential dangers in trying to achieve this. Stewart Baker, a former general counsel at the NSA and assistant secretary for policy at DHS under President George W. Bush, voiced the obvious fear: the United States and its allies would obey whatever was written down and agreed to while no adversaries would.[3]

There may be a larger problem, however, than non-compliance: conventional war has the distinct advantage, historically, of being fairly explicit about target classification. Most military networks that would

initiate and enact a cyber attack depend upon and work within countless numbers of civilian networks. In addition, many of the actors that are part of the planning, initiation, and deployment of cyber attacks are not necessarily formal military but rather civilian employees of government agencies. In other words, the world of cyber conflict and cyberwar is not a world that can achieve such explicit classification. In fact, future trends only show this fusion growing deeper and tighter in time. As such, any attempt to introduce norms and rules that are predicated upon knowledgeable differentiation will likely end up confused and ineffective.

This "ambiguity assertion," for lack of a better term, has so far been relatively ignored in the various cyber debates. The latter tend to revolve around how loose or rigid, how informal or formal, how international or local such codes of constraint should be. Many of these proposed codes aim to constrain cyber behavior so as to protect banking, power, and other critical infrastructure networks "except when nations are engaged in war."[4] Without addressing the ambiguity problem, however, states find themselves in a quandary: where are the lines of distinction between civilian and military drawn? Perhaps the biggest dilemma, therefore, is not the problem of figuring out attribution (who was the trigger man), but rather this futile attempt to clear up the inherent and purposeful ambiguity that characterizes the critical infrastructure used to house, develop, and utilize a state's cyber capabilities.

Many of the current cyber discussions are flawed by the manner in which they implicitly want to analogize conventional conflict with cyber conflict, to make cyber attacks equivalent to armed attacks. To do this, however, the conversation must turn to legal definitions and parameters: when does cyber conflict constitute the use of armed force or a formal act of war? What actions would constitute a war crime? How much damage does it take to trigger a necessary retaliatory response?[5] These questions are much more difficult to answer in the cyber realm because of the logistical nightmare provoked by the ambiguity assertion. This fact has not been emphasized appropriately to date, nor is it strategically addressed at all.

Up to now, questions have focused instead more on comparable lethality, damage estimates, and the aforementioned attribution problem. To an extent, however, all of these problems are enveloped by the civilian/military ambiguity issue. The inability to establish that separation means that lethality could be more extreme by being more than just military

casualties, damage could be more devastating by being more than just military facilities, and attribution might not even be relevant: defining the WHO of an attack does not solve the problem if the HOW behind the WHO is inextricably fused among government, military, and civilian properties and people. In other words, many assume that figuring out WHO in cyberwar will solve most problems. The ambiguity assertion reminds everyone to be careful what they wish for: in cyber war, the WHO will never be conveniently distinct because of the HOW.

International law clearly does not alleviate the problem of civilian/military ambiguity in cyber conflict. Whether the discussion extends to codes of conduct, treaties, or international laws writ large, none of these potential documents attempts to address the inherent structural problem of modern societies and how they currently organize, conduct, and develop their cyber capabilities. Further confirming this is the equal amount of time, effort, and frustration expended in the sister projects of establishing terms and defining parameters. Examining that frustration will illustrate how impactful the ambiguity assertion is when contemplating how the world should deal with the rules for cyberwar.

The Frustration of Setting Terms

Part of the problem in getting international law to cover cyberspace efficiently involves a longstanding failure to translate essential terms and parameters into something that would truly impact on the cyber domain. Progress in moving beyond this problem has been extremely limited. Indeed, even a cursory glance across the literature over the past decade attests to the fact that cyberwar does not fit perfectly into the already existing legal frameworks on war and use of force.[6] Despite this reality, these terminological and doctrinal difficulties have been continually investigated with the aim of forcefully coordinating existing terms and doctrines in the cyber arena. This article argues that the lack of success is attributable to the unwillingness to engage the civilian/military fusion.

The desire for explicit terms, parameters, definitions, laws, and treaties is based more on the worry that failure to produce such explicitness will leave cyberwar outside the boundaries of rules that currently govern conventional war. The consequences are considered stark: critical civilian infrastructure could be targeted, as could basic necessities such as agriculture, food, water, public health, emergency services, telecommunications, energy, banking

and finance, and so on. The ambiguity assertion, however, articulates the difficulty in obtaining such explicitness: most if not all of a state's cyber capability utilizes and depends upon critical civilian infrastructure that also provides many important civilian functions. No state to date has created a cyber operations capability that is wholly distinct and separate from civilian networks and civilian infrastructure. In other words, go after the "military" targets and you will also de facto be going after "civilian" targets. The literature to date seems to ignore this fact. Consequently, much of the literature engages in a false riddle, trying to impose a theoretically precise answer on an empirically ambiguous reality.

This is further confirmed by the number of respected scholars, diplomats, and policymakers who miss the relevance of the ambiguity assertion by demanding that the laws of cyberwar should actually *forbid* the targeting of purely civilian infrastructure, indicating that cyber actors should try to respect the Geneva Conventions as much as conventional actors do.[7] The problem, of course, is that in cyberwar, purely civilian infrastructure is a category of diminishing returns. Indeed, given the obvious trend that sees only intensification and deepening of the civilian/military fusion, purely civilian infrastructure will end up more myth than reality.

The failure to address this structural riddle has been matched by an over-emphasis on agency. This manifests itself mainly in the focus on limiting and controlling potential cyber actions from adversarial states. James Lewis of CSIS emphasizes how a state can reduce risks for everyone by imposing common standards, like moving from the Wild West to the rule of law.[8] Eugene Spafford concurred, citing how cyber security is a process, not a patch, requiring continual investment for the long term as well as the quick fix, without which states will always be applying solutions to problems too late.[9] These are some of the brightest and most respected names in the cyber discipline. Their warnings are not irrelevant, but the emphasis on state actor agency, while failing to recognize the impact and importance of inherent cyber structure, leaves a vulnerable gap in cyber strategic thinking. Indeed, the contemporary failure to create explicit norm coordination should be seen as a demand to consider new strategy that can accept this structural incompatibility as inherent and not something to "overcome." For structural ambiguity is not only intrinsic: states are purposely deepening the ambiguity for its strategic advantage

and economic efficiency. States, therefore, should not focus on how to force a distinct civilian/military separation, but should rather develop new strategic thinking that accepts the ambiguity problem as a logistical reality that must be accounted for.

For empirical confirmation of the futility of trying to address these problems of conventional norms and explicit parameters, look no further than the United States military over the past half-dozen years. It is easy to produce a laundry list of frustration and unfulfilled hopes: General Alexander of US Cyber Command mentioned that progress was being made, but that the risks were nonetheless growing faster than the progress at present;[10] Vice Admiral Michael Rogers, commander of the US Navy's fleet cyber command, admitted to Congress that no agreement had been reached amongst the various commands on ironing out the rules of cyber conflict, but hoped that there would be positive developments "at some point in the near term";[11] and even the Pentagon produced a cyber document that ultimately stated that the laws of armed conflict apply in cyberspace as in traditional warfare, even while admitting that the basic terms "act of war" and "use of force" were still somewhat *ill-defined* in the cyber domain.[12] This shows the real term effects that the lack of new strategic thinking has when states do not address the ambiguity of civilian/military fusion.

Turf Wars and Tightropes: Military Discussion on Cyber Parameters

Just as with scholars, policymakers, and diplomats, the military has been steadfastly committed to establishing strict rules of cyber engagement that are akin to the conventional rules of war.[13] For several years, there has been a pending revision of the military's standing rules of engagement in the cyber realm.[14] It seems that while the military hoped that the scholarly and diplomatic communities would be able to help define much of the needed clarification, the two latter communities were themselves hoping to see the military lead the way with its revision. This obfuscation of responsibility, however, is not as relevant as many observers and analysts might think: failure to address these issues is not so much a case of one community trying to pass the buck on to another, but rather testimony to the confusion created when the ambiguity assertion about civilian/military fusion is not addressed.

General Alexander stated that in debating the rules of conflict in cyber operations, the United States was trying to do the job right.[15] Those debates, however, constantly oscillate back and forth between positions that do not address the primary innate structural concerns of the cyber domain. Consequently, the military has spent a half-dozen years promising imminent progress that does not materialize. The Pentagon's official report was itself described as "ducking" a series of important fundamental questions, including defining such basic terms as "war," "force," and "appropriate response."[16] This is pointed out not to poke fun at the military. Quite to the contrary, this article makes the argument that given the reluctance of all parties concerned to engage the ambiguity assertion, with an eye to developing new strategy that embraces it rather than hopelessly using old strategy to overcome it, the military has had no real chance of making substantive progress to define the parameters of cyber action concisely.

It is no coincidence that the American military has sincerely worked on issues such as administrative network control, cyber organization, force composition, and cyber intelligence/operation differentiation, in addition to basic terminology parameters, without any major questions being considered definitively and comprehensively closed.[17] How, for example, can USCYBERCOM be expected to connect all the dots and be the competent arbiter in determining a case for action when it readily admits difficulty in even articulating who exactly comprises the fraternity of cyber warriors operating and defending home networks?[18] If the issues at hand were neither so serious nor so far-reaching on the future of cyber conflict, it would be almost comical. Only recently has it seemed possible that relevant military bodies have started to reach the epiphany discussed here:

> Although there are some noteworthy first steps toward establishing an international set of cyber norms – evident in bodies such as the Convention on Cybercrime – any global framework governing military response actions in cyberspace will surely materialize at an onerous pace. After all, how can the rules of war, built upon the tactile presence of combatants and weapons and sovereign territory, be retooled for a world where 'troops' can be dispatched in milliseconds from a multitude of states?[19]

At least the above quote begins to frame the discussion around the innate incompatibility between how war in cyberspace would likely be conducted and how that compares to all previous wars. It is still, however, emphasizing agency over structure: establishing an international set of cyber norms mainly to hallmark the division between civilian and military assets and mitigate action already undertaken. This might help explain why formal strategic documents concerning cyberspace end up being nothing but simple platitudes about how the United States intends to protect itself. Take for example the Department of Defense's (DoD) Strategy for Operating in Cyberspace, released in mid-2011 and consisting of five "strategic initiatives":

> *Strategic Initiative 1*: Treat cyberspace as an operational domain to organize, train, and equip so that the DoD can take full advantage of cyberspace's potential.
> *Strategic Initiative 2*: Employ new defense operating concepts to protect domestic networks and systems.
> *Strategic Initiative 3*: Partner with other US government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.
> *Strategic Initiative 4*: Build robust relationships with US allies and international partners to strengthen collective cyber security.
> *Strategic Initiative 5*: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

Take full advantage; employ new concepts; partner with others; build robust relationships; leverage ingenuity. All of these phrases are wonderful slogans, but they are not accompanied by any explicit new strategic thinking that could hope to actually institute said initiatives. Trying to adapt conventional strategy slightly and then force the cyber domain into it is likely to remain a project bearing little fruit. Examining that conventional strategy and proposing new strategy that engages the structural dilemma is the final section of this paper.

Engaging Ambiguity: Strategic Thinking for the Civilian/Military Cyber Fusion

The need for a new strategic approach is best illustrated when the arguments of two highly respected strategic thinkers – one military and

one legal, who happen to fall on opposite sides of the LOAC cyber debate – ignore the problem of civilian/military structural cyber fusion. Dunlap, while accepting the need for improvement, believes the tenets of the law of armed conflict to be sufficient to address the most important issues of cyberwar.[20] The concern for distinguishing between legitimate military and civilian targets does not seem to bother Dunlap in its impact on the applicability of LOAC:

> LOAC tolerates "incidental losses" of civilians and civilian objects so long as they are "not excessive in relation to the concrete and direct military advantage anticipated." In determining the incidental losses, cyber strategists are required to consider those that may be reasonably foreseeable to be directly caused by the attack. Assessing second- and third-order "reverberating" effects may be a wise policy consideration, but it does not appear LOAC currently requires such further analysis.[21]

Dunlap's distinction is actually quite important given the current intellectual climate: he has introduced some much-needed realism into the debates by reminding people that LOAC has never been a flawless strategy that provides perfect protection for civilians and civilian objects. The problem highlighted here, however, is that his concerns over military/civilian differentiation are misplaced.

These pro-LOAC arguments are effectively built around the fact that cyberwar does not have to have a perfect record in delineating and then protecting civilians because LOAC does not, either. But these arguments assume that such delineation is generally possible. The future of cyberwar is unlikely to be able to create such possibility because it has long been established how many of the military's critical functions, assets, service providers, and supply chains all rely heavily on civilian traffic and networks.[22] As such, new strategy needs to be positioned so as to prevent the use of cyber weapons in general, because once they are used, the likelihood of incurring civilian risk, damage, and casualties will be de facto. "Sanitizing" the impact of cyber weapons once they are used by trying to constrain targeting choices will not work.

The anti-LOAC camp makes the same mistake when discussing why the law of armed conflict does not bring clarity to cyberwar:

> The laws of war are in place to ensure that parties to a conflict target combatants rather than civilians, and, if civilians are targeted, to ensure that such individuals have forfeited their protected status. To determine whether cyber-attacks properly distinguish between civilian and military targets, one must understand [the] distinction.[23]

The opposition camp fails in the belief that such a distinction can in fact be created in the cyber realm. This camp does not see the strategic influence of the ambiguity assertion, focusing rather on the deficiencies within LOAC and other contemporary norms and treaties: in short, make better laws and the cyber world will come to heel. As such, this camp is even further from cyber reality, ignoring a problem that is only going to deepen and intensify over time. The opposition camp, in essence, is a more liberal approach to conflict because the end goal is to create an atmosphere of trust that can minimize higher levels of violence and treachery.[24] This flies even more in the face of the current and future structure of cyberwar.

Both of these camps believe in being able to monitor and regulate and circumscribe cyberwar after it has begun, as happens successfully with conventional war. This is a false hope. The ability to monitor, regulate, and circumscribe cyber action is best done through strategy that can inculcate preemptive fear and thereby induce caution and hesitation. Current conventional strategies that aim for trust, target distinction, and minimizing noncombatant impact are simply inexplicably ignoring how cyberwar is organized, structured, and operationalized.

Liberal thinking also dominates the legal community, which is heavily leaned upon for law projects and the strategic thinking that purportedly infuses said projects for the cyber domain:

> [An effective solution to the global challenge of cyber attacks] cannot be achieved by individual states acting alone. It will require global cooperation. We therefore outlined the key elements of the cyber treaty – namely, codifying clear definitions of cyber warfare and cyber-attack and providing guidelines for international cooperation on evidence collection and criminal prosecution – that would provide a more comprehensive and long-term solution to the emerging threat of cyber-attacks.[25]

The only thing left to add here is to note yet another camp focusing on mitigating risk and limiting damage in the cyber domain ex post facto. Regardless of philosophical standing, political agendas, or theoretical acumen, every camp that examines the problem of parameters and definitions in the cyber domain seems to exclude considerations of preemptive strategies built upon fear and inducing reluctance to action. General Alexander of US Cyber Command cited the need to establish the lanes of the road for what governments can and cannot pursue and asserted that establishing those lanes was the necessary first step to addressing the challenge of cyber attacks.[26] What all of the camps examined here have in common is a tendency to give lip-service to strategy, but then really focus exclusively on ex post facto operations to establish progress. If the focus continues to be on agency action rather than on structural deficiency, then progress will not simply remain slow: it will become non-existent.

Duqu's Dilemma: Why It Matters

This analysis has pinpointed flaws in the current thinking and efforts to establish clear definitions and parameters governing the rules and operations within cyberwar. The emphasis placed here on inherent structural difficulties, namely, the innate cyber civilian/military fusion, has shown the likely damaging and deadly consequences to societies when strategies do not focus on the effort to stop cyber action preemptively, focusing instead on operational considerations after conflict has begun.

Only now are isolated legal analyses highlighting these problems beginning to emerge:

> It is unlikely that a state such as the United States could take precautions against the effect of attacks on military objectives by separating military objectives from civilians and civilian objects in cyberspace. This is because of the interconnectedness of US government and civilian systems in the near complete government reliance on civilian companies for the supply, support, and maintenance of its cyber capabilities... Proportionality assessments likely will prove particularly precarious in cyberspace, where outcomes are more difficult to predict than in the physical world: physical attacks at least have the advantage of physics and chemistry to work with. Because, say, the blast radius of a thousand pound bomb is fairly well understood, one can predict what

> definitely lies outside the blast radius and what definitely lies inside. Error bands and cyber-attacks are much wider and less well-known... [Most reports do not explain how] these public-private partnerships could be constituted in a manner that adequately considers laws of war issues nor do [they] address the likely use of active defenses by the private sector.[27]

As illustrated above, this structural issue is more than just semantics. It literally covers who engages cyberwar, what can be destroyed in cyberwar, who can be a victim during cyberwar, even the philosophical and ethical questions meant to be asked about cyberwar itself. Duqu's Dilemma is an entreaty to move away from unattainable goals and idealistic dreams in a futile hope to create sanitized cyberwar. Cyberwar will never be sanitized. Consequently, contemporary strategic thinking about the cyber domain must start treating the ambiguity assertion with the same gravity that the more famous attribution problem receives.

Notes

1 Tom Leithauser, "Rules of War Should Apply to Cyber Conflict," *Cybersecurity Policy Report*, February 14, 2011.
2 Tom Gjelten, "Shadow Wars: Debating Cyber Disarmament," *World Affairs* 173, no. 4 (2010): 33-42.
3 Ibid.
4 Aliya Sternstein, "Experts Recommend an International Code of Conduct for Cyberwar," *National* Journal, June 10, 2011.
5 Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-conflict and Just War Theory," *European Conference on Information Warfare and Security* 177-XI (July 2010).
6 Vida Anatolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?" *Naval Law Review* 51, no. 132 (2005): 1-34.
7 Don Tennant, "The Fog of (CYBER) War," *Computerworld* 43, April 27, 2009, pp. 28, 30-32.
8 James Fallows, "Cyber Warriors," *Atlantic Monthly* 305 (March 2010): 58-60, 62-63.
9 Ibid.
10 John Curran, "Updated Rules for Cyber Conflict Coming Soon, Defense Officials Say," *Cybersecurity Policy* Report, March 26, 2012.
11 Lolita Baldor, "Cyber Warriors," *Army Times*, August 6, 2012, p. 23.
12 Siobhan Gorman and Julian Barnes, "Rules for Laws of War: US Decides Cyber Strike Can Trigger Attack," *The Australian,* June 1, 2011.

13 Anonymous, "Military Ponders Cyberwar Rules," *Los Angeles* Times, April 7, 2008.
14 Ellen Nakashima, "Pentagon Seeks to Expand Rules of Engagement in Cyber War," *Washington Post*, August 10, 2012.
15 Ibid.
16 Ellen Nakashima, "Cyber Offense Part of Strategy," *Washington Post*, November 16, 2011.
17 Wesley Andrues, "What US Cyber Command Must Do," *Joint Forces Quarterly* JFQ 59 (Fourth Quarter 2010): 115-20.
18 Ibid.
19 Ibid., p. 120.
20 Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* (Spring 2011): 81-99.
21 Ibid., p. 90.
22 Erik Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *Air Force Law Review* 68 (2012): 167-206.
23 Michael Gervais, "Cyber Attacks and the Laws of War," *Journal of Law and Cyber Warfare* 30, no. 2 (2012): 525-79.
24 Ibid., p. 561.
25 Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review, Inc* (2012): 817-85.
26 Ibid., p. 884.
27 Hannah Lobel, "Cyberwar Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict," *Texas International Law Journal* 47, no. 3 (2012): 617-40.

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 Warfare 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 warfare and critical infrastructure protection
- Defense budgets
- Intelligence

Submitted articles should not exceed 5500 words (including citations in standard format) and should be accompanied by an abstract of 200 words. Previous issues of the journal may be accessed on the INSS site at: http://www.inss.org.il/.

Submissions should be sent to:
Daniel Cohen
Coordinator, *Military & Strategic Affairs*
danielc@inss.org.il