Military and Strategic Affairs

Volume 5 | No. 3 | December 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. 3 | **December 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.

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

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

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

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

The Threat of Terrorist Organizations in Cyberspace

Gabi Siboni, Daniel Cohen, and Aviv Rotbart

This article discusses the threat of terrorism in cyberspace and examines the truth of the perceptions of this threat that have formed in recent years. It examines the capabilities that a non-state actor can achieve and whether these can constitute a real threat to the national security of states. For an analysis of the main threats facing a state from a multi-year perspective and in light of anticipated changes in a state's strategic balance, the factors that threaten the state are presented and the roots of the threat are identified. The article thus examines whether terrorism, whose impact is generally tactical, could make (or perhaps has already made) the transition to a cyber weapon capability with strategic impact. Specifically, the question is could terrorists develop cyber weapon capabilities that could inflict widespread damage or damage over time, of the sort that brings states to their knees and causes critical systems to crash.

Keywords: cyberspace, cyber terror, cyber weapons, terrorist organizations, non-state actors, cyber crime, enterprise information systems, core operational systems, intelligence guidance capability, technological capabilities

Introduction

The first motion picture ever screened before an audience was produced by the Lumiere brothers in 1895. It showed a train entering a station, seemingly moving toward the viewers in the hall. The spectators, who were convinced that the train was approaching them, screamed in panic

Dr. Gabi Siboni is a senior research fellow and the head of the INSS Cyber Warfare Program. Daniel Cohen is the coordinator of the Cyber Warfare Program at INSS. Aviv Rotbart is a doctoral student in the Department of Computer Science at Tel Aviv University.

and fled the building. During the first movie ever shown, it seemed to the spectators that what they were seeing was reality.[1]

Cyber terrorism is a field in which reality and science fiction are sometimes intertwined. If we examine one of the key concepts in cyberspace – namely, dealing with terrorist threats – we find that the rationale underlying the concept (which emerged after the formative events at the beginning of the twenty-first century, such as the Y2K bug and the September 11, 2001, terrorist attacks) is that the world appears to be at the peak of a process that belongs to the post-modern and post-technology era, an era with no defensible borders, in which countries are vulnerable to invasion via information, ideas, people, and materials – in short, an open world. In this world the threat of terrorism takes a new form: a terrorist in a remote, faraway basement has the potential ability to cause damage that completely changes the balance of power by penetrating important security or economic systems in each and every country in the world and accessing sensitive information, or even by causing the destruction of vital systems.[2]

Can the reality of September 11, 2001 – when a terrorist organization that had planned an attack for two years, including by taking pilot training courses, eventually used simple box-cutters to carry out a massive terrorist attack – repeat itself in cyberspace? Is a scenario in which a terrorist organization sends a group of terrorists as students to the relevant courses in computer science, arms them with technological means accessible to everyone, and uses them and the capabilities they have acquired to carry out a massive terrorist attack in cyberspace realistic or science fiction? In order to answer this question, we must first consider what capabilities a non-state actor can acquire, and whether these capabilities are liable to constitute a real threat to national security. An analysis of the main threats facing a country over the course of several years, given expected changes in its strategic balance sheet, requires identifying the entities threatening a country as well as the roots of the threat and the reasons for it.

No one disputes that non-state actors, terrorist organizations, and criminals are using cyberspace for their own purposes and deriving benefit from a field in which everyone is at the same starting point – a field that also enables small individual players to have an influence disproportionate to their size. This asymmetry creates various risks that did not attract attention or provoke action among the major powers in the past. The question is whether the activity of these players in cyberspace constitutes a threat with the potential to cause major and widespread damage, and if so, why such damage has not yet occurred.

This article assesses whether attacks in cyberspace by terrorist organizations, whose effect until now has usually been tactical, will be able to upgrade (or perhaps have already upgraded) their ability to operate cyber weapons with strategic significance – weapons that can inflict large scale or lasting damage of the sort that causes critical systems to collapse and "brings countries to their knees." The purpose of this article is to discuss the threat of cyberspace terrorism and assess the truth of the concepts that have emerged in recent years concerning this threat.

This article focuses on the activities of non-state organizations with political agendas and goals, even if operated or supported by states. A distinction is drawn between these activities and those that are conducted directly by countries, which are beyond the scope of the article, as are the activities of organizations whose aims are mainly of a criminal nature. For the purposes of this article, a terrorist act of a non-state organization in cyberspace will be defined as an act in cyberspace designed to deliberately or indiscriminately harm civilians. For example, disruption of the internet site of a commercial bank by a non-state organization with political goals will be defined as an act of terrorism in cyberspace. Figure 1 illustrates the scope of discussion in this article.

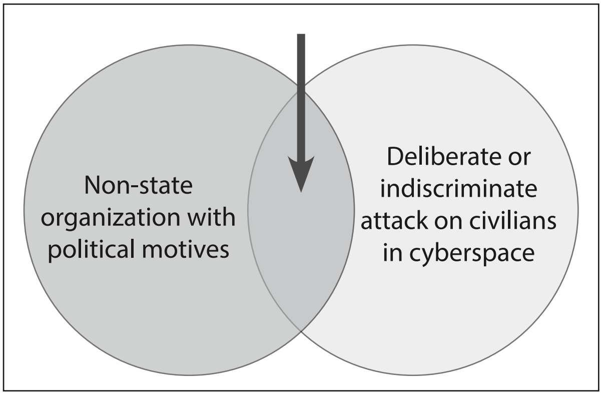

Non-state organization with political motives
Deliberate or indiscriminate attack on civilians in cyberspace

Figure 1. Terrorist Acts in Cyberspace

The Methodology of the Study

A number of benchmarks had to be met in order to assess the activity of terrorist organizations in cyberspace. The first was identification of the motives for using cyberspace as part of the political struggle being waged by the terrorist organizations. Toward this end, two principal motives were identified. The first is the use of cyberspace in support of terrorist activity, mainly the acquisition of money and recruits or money laundering in order to finance the activity. The second is the use of tools in cyberspace to provide the actual strike against the targets that the terrorist organization set for itself, as well as its use for other violent means. In this context we will analyze the cooperation between non-state organizations and the states that operate them and support their terrorist activity.

The second benchmark of this study required an assessment and in-depth understanding of the capabilities that terrorist organizations can obtain, bearing in mind that not every computer operator, even if a technological genius, can generate an effective and significant terrorist attack. In this context we also examined the assumption that significant attacks in cyberspace will continue to be confined to high-technology countries and will require considerable resources in terms of both intelligence and technology. Next, having established an understanding of the terrorist organizations' array of relevant technological and intelligence capabilities, it was necessary to consider whether such activities by terrorist organizations have actually been identified. Finally, all the findings were analyzed in order to formulate conclusive insights and recommendations as part of the defense needs.

Analysis of Capabilities

Cyberspace contributes to the enhancement of knowledge and acquisition of capabilities. In addition, technology is useful in creating an anonymous communications network.[3] Similarly, cyberspace serves as a platform for expanding the circle of partners for terrorist activity. In contrast to the recruitment of terrorist operatives in the physical world, in cyberspace it is possible to substantially enlarge the pool of participants in an activity, even if they are often deceived into acting as partners by terrorist organizations using the guise of an attack on the establishment. This phenomenon is illustrated by the attacks by hackers against Israeli targets on April 7, 2013,[4] when some of the attackers received guidance concerning the methods and targets for the attack from camouflaged Internet sites. The exploitation of young people's anti-establishment sentiments and general feelings against the West or Israel makes it possible to expand the pool of operatives substantially and creates a significant mass that facilitates cyber terror operations. For example, it has been asserted that during Operation Pillar of Defense over one hundred million cyber attacks against Israeli sites were documented,[5] and that during the campaign and the attacks there were quite a few operatives who followed developments through guidance apparently provided by Iran and its satellites.[6]

On the one hand, the array of capabilities and means at the disposal of terrorist organizations in cyberspace is limited because of its strong correlation with technological accessibility, which is usually within the purview of countries with advanced technological capabilities and companies with significant technological capabilities. On the other hand, access to the free market facilitates trade in cybernetic weapons and information of value for an attack. One helpful factor in assembling these capabilities is countries that support terrorism and seek to use proxies in order to conceal their identity as the initiator of an attack against a specific target. In addition, the terrorist organization must train experts and accumulate knowledge about ways of collecting information, attack methods, and means of camouflaging offensive weapons in order to evade defensive systems at the target.

This study reveals that to date terrorist organizations have lacked the independent scientific and technological infrastructure necessary to develop cyber tools with the ability to cause significant damage. They also lack the ability to collect high quality intelligence for operations. The ability of terrorist organizations to conduct malicious activity in cyberspace will therefore be considered in light of these constraints.

As a rule, a distinction should be drawn among three basic attack categories: an attack on the gateway of an organization, mainly its internet sites, through direct attacks, denial of service, or the defacement of websites; an attack on an organization's information systems;[7] and finally, the most sophisticated (and complex) category, attacks on an organization's core operational systems,[8] affecting its core functions – for example, industrial control systems.[9] Cyber terror against a country and its citizens can take place at a number of levels of sophistication, with each level requiring capabilities in terms of both technology and the investment made by the attacker. The damage that can be caused is in direct proportion to the level of investment.

An Attack at the Organization's Gateway

As noted, the most basic level of attack is an attack on the organization's gateway, that is, its internet site, which by its nature is exposed to the public. The simplest level of cyber terrorism entails attacks that deny service and disrupt daily life but do not cause substantial, irreversible, or lasting damage. These attacks, called "distributed denials of service" (DDOS), essentially saturate a specific computer or internet service with communication requests, exceeding the limits of its ability to respond and thereby paralyzing the service. Genuine requests go unanswered because the service is overloaded by having to deal with the attacker's requests.

DDOS attacks carried out by a terrorist organization[10] need to be effective and continue for a significant amount of time to ensure that as many people as possible become aware of the attack and are affected by the denial of service. Suitable targets for such an attack are, among others, banks, cellular service providers, cable and satellite television companies, and stock exchange services (trading and news). Popular cellular applications whose disruption can be a nuisance, such as WAZE, access to e-mail service, and appointments calendars, as well as Voice over Internet Protocol (VoIP) call applications, may be added to this list.

Another method of attacking an organization's gateway is through attacks on Domain Name System (DNS) servers – servers used to route internet traffic. Such an attack will direct people seeking access to a specific site or service towards a different site, to which the attackers seek to channel the traffic. A similar, but simpler, attack can be conducted at the level of an individual computer instead of the level of the general DNS server, meaning that communications from a single computer will be channeled to the attacker's site rather than the real site which the user wishes to surf. Damage caused by such attacks can include theft of information; denial of service to customers, resulting in business damage to the attacked service; and damage to the reputation of the service. The attacker can redirect traffic to a page containing propaganda and messages he wants to present to the public.

One popular and relatively simple method of damaging the victim's reputation at the gateway of the organization is to deface its Internet site. Defacement includes planting malicious messages on the home page, inserting propaganda that the attackers wish to distribute to a large audience, and causing damage to the organization's image (and business) by making it appear unprotected and vulnerable to potential attackers.

An Attack against the Organization's Information Systems

The intermediate level on the scale of damage in cyberspace includes attacks against the organization's information and computer systems, such as servers, computer systems, databases, communications networks, and data processing machines. The technological sophistication required at this level is greater than that required for an attack against the organization's gateway. This level requires obtaining access to the organization's computers through employees in the organization or by other means. The damage that can be caused in the virtual environment includes damage to important services, such as banks, cellular services, and e-mail.

A clear line separates the attacks described here from the threat of physical cybernetic terrorism: usually these attacks are not expected to result in physical damage, but reliance on virtual services and access to them is liable to generate significant damage nevertheless. One such example is the attack using the Shamoon computer virus,[11] which infected computers of Aramco, the Saudi Arabian oil company, in August 2012. Even though the attack did not affect the company's core operational systems, it succeeded in putting tens of thousands of computers in its organizational network out of action while causing significant damage by erasing information from the organization's computers and slowing down its activity for a prolonged period.[12]

An Attack on the Organization's Core Operational Systems

The highest level on the scale of attack risk is an attack on the organization's core operational and operating systems. Examples include attacks against critical physical infrastructure, such as water pipes, electricity, gas, fuel, public transportation control systems, or bank payment systems, which deny the provision of essential service for a given time, or in more severe cases, even cause physical damage by attacking the command and control systems of the attacked organization.

A successful offensive could cause the release of hazardous materials into the air and physical harm to a large population. This is the point at which a virtual attack is liable to create physical damage and its effects are liable to be destructive. Following the exposure of Stuxnet, awareness increased of the need to protect industrial control systems, but there is still a long way to go before effective defense is actually put into effect. Terrorist groups can exploit this gap, for example by assembling a group of experts in computers and automation of processes for the purpose of creating a virus capable of harming those systems.[13]

Another way of obtaining physical cyber weaponry is likely to emerge from the black market in cyber weapons and its expansion to include physical infrastructure, in addition to the virtual weaponry that it already offers now. It should be noted that as of the date of this writing, such a scenario has not actually occurred. Because it involves complex and costly cybernetic weaponry, however, it is possible that clandestine trading in this area is already underway in the internet underworld.[14] As noted, this is the highest level on the cyber attack scale, and the costs and damage caused by it are correspondingly high, as evidenced by the Stuxnet worm.[15]

Development of attack capabilities, whether by countries or by terrorist organizations, requires an increasingly powerful combination of capabilities for action in cyberspace in three main areas: technological capabilities, intelligence guidance for setting objectives (generating targets), and operational capacity.

Technological Capabilities

The decentralized character of the Internet makes trade in cyber weaponry easy. Indeed, many hackers and traders are exploiting these advantages and offering cyber tools and cyberspace attack services to anyone who seeks them. A varied and very sophisticated market in cyber products trading for a variety of purposes has thus emerged, with a range of prices varying from a few dollars for a simple one-time denial of service attack to thousands of dollars for the use of unfamiliar vulnerabilities and the capabilities to enable an attacker to maneuver his way into the most protected computer system. Thanks to cyberspace, this market is growing by building on the infrastructure of social networks and forums that allow anonymous communications between traders and buyers.[16] In an interesting phenomenon, seen only recently, these traders are leaving the web underground and stepping out into the light. They can be found on the most popular social network of all: Facebook.[17] A blog by information security company RSA[18] describes a new situation, in which the traders offer their wares not only as goods, but also as a complete service, including the installation of command and control servers, training in the use of the tools, and even discounts, bargains, and the option of buying only certain modules of the attack tool in order to reduce the price. The growth of this market raises the question whether and how terrorist organizations can use all the knowledge and tools that have accumulated in the cyber crime market.

In order to answer this question, it is necessary to assess the gap between the abundance of tools and capabilities currently offered for sale openly on the Internet and the requirements of terrorist organizations. Today's market for attack tools is aimed at cyber criminal organizations, mainly for purposes of fraud, stealing funds from unwitting bank account holders, and identity theft by collecting particulars from credit cards, bank account numbers, identity cards and addresses, entry passwords to financial websites, and the like. These tools are not necessarily suitable for the needs of terrorist organizations. At the same time, many terrorist organizations might engage in the practices of cyber criminal organizations for the sake of fundraising to finance their main terrorist activity. The principal objective of terrorist organizations – causing substantial damage and instilling fear – can be accomplished in a number of ways and at different levels of difficulty and severity. The tools of the cybernetic underworld can be of great assistance in DDOS attacks and in stealing large quantities of sensitive information from inadequately protected companies (for example, information about credit cards from unprotected databases), which will almost certainly arouse public anxiety. Terrorists still have a long way to go, however, before they can cause damage to control systems, which is much more difficult than stealing credit cards, and towards which cybernetic crime tools are of no help. With respect to the intermediate level described above concerning attacks on an organization's information systems, it appears that the underworld possesses tools capable of assisting cyber terrorism. Some adjustment of these tools is needed, such as turning the theft of information into the erasure of information, but this is not nearly such a long process, and the virus developers will almost certainly agree to carry it out for terrorist organizations, if they are paid enough.

Intelligence-Guided Capability

One of the key elements in the process of planning a cyber attack is the selection of a target or a group of targets, damage to which will create the effect sought by the terrorist organization. Towards this end, a terrorist entity must assemble a list of entities that constitute potential targets for attack. Technology that provides tools facilitating the achievement of this task is already available free of charge. For example, the Facebook and LinkedIn social networks can be used to find employees in the computer departments of infrastructure companies, food companies, and the like. Taking the Israel Electric Corporation as an example, academic studies[19] show that company divisions can be mapped, employees can be found in the various departments, and those with access to the company's operational systems can be selected, all with no great difficulty.[20] If these employees are aware of the importance of information security, and therefore cannot be directly attacked, their families and friends can be traced through Facebook, and the desired target can be attacked through them. Social networks constitute an important source for espionage and collection of business and personal information about companies and organizations,[21] and terrorist organizations can easily use the information distributed through them for their own benefit.

It is also necessary to map the computer setup of the attacked organization, and to understand which computers are connected to the internet, which operating systems and protective software programs are installed on them, what authorizations each computer has, and through which computers the organization's command system can be controlled. For example, if a terrorist organization wants to control the functioning of a turbine that produces electricity, its task, although much more technical and difficult than mapping the company's organizational structure, is now especially easy, following the publication of a study by a "white hat" hacker, who conducted the first "internet census" in history.[22]

Using a ramified network of robots (software programs implanted in computers that wait for an order from the command and control center to which they are connected), the white hat hacker compiled a list of 1.3 billion IP addresses in use, for some of which he published technical data such as the type of open gates, the requests to which these addresses respond, and more. The published results of the census are freely available to all interested Internet surfers. For a malicious hacker, these data are sometimes necessary in order to attack and take over the entire computer system of an individual or organization. Thus a company's organizational structure can be mapped, and if its network is not adequately protected, information can also be gleaned about the computers used by the company's employees.

Good protection and awareness of information security capabilities can make it very difficult for hackers and terrorists to carry out the abovementioned actions. Organizations with critical operational systems usually use two computer networks: one external, which is connected to the internet, and one internal, which is physically isolated from the internet and is connected to the organization's industrial control systems. The internet census does not include information about isolated internal networks because these are not accessible through the internet. Any attack on these networks requires intelligence, resources, and a major effort, and it is doubtful that any terrorist organizations are capable of carrying out such attacks. Here the terrorist organizations can take advantage of another study conducted by hackers from the University of Berlin,[23] which uses a Google map (enabling researchers to present and share geographic information that they have collected) to display a large number of industrial control systems (ICS) deployed throughout the world that are connected to the internet. The information displayed on the map is taken from an enormous database freely available to everyone through the Shodan website,[24] which makes the life of a terrorist hacker much easier. This service uses information collected by Google for its mapping and location-based advertising services and makes it accessible to the public. It is possible that the hackers who recently broke into the home networks of hundreds of Israelis used services from the Shodan website in order to collect intelligence for the attack, and perhaps also to obtain tools (cyber ammunition) to actually carry it out.[25]

Operational Capability

After collecting intelligence and creating or acquiring the technological tools for an attack, the next stage for planners of cybernetic terrorism is operational – to carry out an actual attack by means of an attack vector.[26] This concept refers to a chain of actions carried out by the attackers in which each action constitutes one step on the way to the final objective, and which usually includes complete or partial control of a computer system or industrial control system. No stage in an attack vector can be skipped, and in order to advance to a given step, it must be verified that all the preceding stages have been successfully completed.

The first stage in an attack vector is usually to create access to the target. A very common and successful method for doing this in cyberspace is called spoofing, that is, forgery.[27] There are various ways of using this method, with their common denominator being the forging of the message sender's identity, so that the recipient will trust the content and unhesitatingly open a link within the message. For example, it is very easy to send an e-mail message to an employee at the Israel Electric Corporation (mentioned above), in which the sender forges the address of a work colleague, a relative, or another familiar person. The attacker's objective in this case is to make the receiver of the message trust the content of the message and open its attachments or enter the internet addresses appearing in it.

The forging of e-mail is an attack method that has existed for many years. Defensive measures have accordingly been developed against it, but attackers have also accumulated experience. Incidents can now be cited of completely innocent-looking e-mail messages that were tailored to their recipients, containing information relating to them personally or documents directly pertaining to their field of business. The addresses of the senders in these cases were forged to appear as the address of a work colleague. As soon as the recipients opened the e-mail, they unknowingly infected their computers with a virus.

The forgery method can be useful when the target is a computer connected to the internet and messages can be sent to it. In certain instances, however, this is not the case. Networks with a high level of protection are usually physically isolated from the outside world, and consequently there is no physical link (not even wireless) between them and a network with a lower level of security. In this situation the attacker will have to adopt a different or additional measure in the attack vector – infecting the target network with a virus by using devices that operate in both an unprotected network and in the protected network. One such example is a USB flash drive ("Disk on Key" or "memory stick"), which is used for convenient, mobile storage of files. If successful, the attacker obtains access to the victim's technological equipment (computer, PalmPilot, smartphone), and the first stage in the attack vector – creating access to the target – has been completed. Under certain scenarios, this step is the most important and significant for the attacker. For example, if the terrorist's goal is to sabotage a network and erase information from it, then the principal challenge is to gain access to the target, that is, access to the company's operational network. The acts of erasure and sabotage are easier, assuming that the virus implanted in the network is operated at a sufficiently high level of authorization. Under more complex scenarios, however, in which the terrorist wishes to cause significant damage and achieve greater intimidation, considerable investment in the stages of the attack vector is necessary, as described below.

Lockheed-Martin, which fell victim to a cyber attack, offers a methodology for analyzing cyberspace attack operations, which it calls "the Cyber Kill Chain."[28] According to this methodology, a complex cyber attack comprises seven milestones, paralleling the actions of planning the operation and creating the attack vector. The first step entails collecting intelligence about the target. The right cyber weapon for the attack must then be selected and launched at the target. The next stage includes the exploitation of a vulnerability in the target computer that will make it possible to implant a malicious file on its system, followed by installing the tool in a way that will enable it to carry out operations within the system. The stage after that is to create communications between the tool and the attacker's command and control servers, so that the tool can be guided and a report obtained from it about events on the victim's computer. The final step in the cyber kill chain is the conducting of active operations from within the victim's computer, such as erasure, spreading of the tool, taking over the physical devices accessible from the computer, and the like. The term "Cyber Kill Chain" was chosen in order to emphasize that in order for the attacker to succeed in carrying out a cyber attack, he must successfully complete every milestone without being detected and without his access to the target being blocked.

A terrorist organization seeking to attack operational systems will have to carry out all the stages in the chain. These are advanced and complex operations, which terrorist organizations usually do not know how to implement by themselves. If the target is protected at a very low level, no great technological capability will be required of the attacker in order to create damage or achieve defacement. In most cases, however, the terrorists will have to acquire products or services from expert hackers. In other words, they will have to use "outsourcing."

Within the offensive cyber products market, terrorists will find accessible capabilities for a non-isolated target. In the same market, they will also find attack products, and presumably they will likewise find products for conducting operations on the target network (similar to the management interface of the SpyEye[29] Trojan Horse). Despite this availability, internet-accessible tools have not yet been identified for facilitating an attack on an organization's operational systems. Access to these tools is possible in principle,[30] but the task requires large-scale personnel resources (spies, physicists, and engineers), monetary investment (for developing an attack tool and testing it on real equipment under laboratory conditions), and a great deal of time in order to detect vulnerabilities and construct a successful attack vector.

Types of Cyberspace Attacks

It is possible to identify a number of types of cyberspace attacks in accordance with both their level of expected damage and the scope of their intelligence, technological, and operational investment. In most cases, these two measures correspond with each other. The following review paints a picture of the capabilities of a non-state organization in cyberspace.

Amateur Attack

This action is taken using tools that are (in most cases) known to information security companies and are identifiable by standard protection software programs. Defenses against these tools have been developed, and they are therefore likely to prove effective only against unprotected targets. Such tools are usually used only for research or gaming purposes because only in rare cases can they be used to steal valuable information or to sabotage protected computer networks. They have spy and sabotage capabilities, but these are not very sophisticated.

Minor Attack

This is an attack in which not much effort has been invested. Most of its activity consists of searching on the internet for readymade tools or purchasing them from companies that specialize in them. Attacks of this type do not usually succeed in causing damage to entities that are attentive to information security (state, military, and advanced industrial entities), but they can penetrate private computers, steal information, and sabotage them. In most cases, these attacks are one-time events (theft of an important file, erasing a disc drive), but they can also sometimes be part of an extensive attack, such as the theft of a computer's domain name system (DNS), which makes it possible to monitor its activity on the internet.

The tools used in a minor attack do not include the various software modules; they have a single inexpensive code component that carries out all the actions of the tool. This code component is written in a way that will not allow its capabilities to be easily altered or expanded, and it is target oriented. Through the internet anyone can obtain this type of limited-capability cyber weapon for a few thousand dollars at most.

This category also includes the use of botnet software agents for DDoS attacks. Creating the network is a more complex operation, but once it is created, it can be used for many DDoS operations. It can also be leased to others for denial of service from various websites lacking high-level protection against such an attack.

Medium-Level Attack

This is an attack capable of causing significant damage or carrying out advanced spy operations at a lower cost than that of a major attack (see below). Usually this operation does not use new, unique vulnerabilities (because these are very expensive); rather, it uses known or partially known vulnerabilities against which the target is not yet protected. The operation does not include expensive modules for implementation and testing such as those developed for Stuxnet. At the same time, by using modules for an attack on computer systems (erasure, disruption) and spy modules, such an operation can be very effective as part of a short-term attack for destructive purposes (because no effort will be made to conceal the destruction, which would be too expensive) or to spy on a victim whose systems do not have high-level protection.

A medium-level attack is much less costly than a major attack, as the former entails fewer man-years and does not require special, expensive hardware or the purchase of new and expensive vulnerabilities. An inexpensive vulnerability is sufficient for penetration of the victim's computer systems, bearing in mind that these are liable to be detected and blocked in the near future. The mid-level category also includes viruses capable of spreading throughout the computer network (worms) and waiting for an order from their operator. This attack model is particularly useful in creating a network of software agent robots for DDoS operations. This category also includes a DDoS attack against protected websites, which requires sophistication from the attacker and familiarity with the protection system at the target.

Major Attack

This is an attack into which many personnel, computer, and monetary resources have been invested, and which has been thoroughly tested in the laboratory before being put into operation. This operation uses unfamiliar vulnerabilities, giving the attacker a long time to operate it before it is detected and shut down. The operation is usually camouflaged in order to leave few footprints. The software tool contains a number of modules, some of which are likely to be designed to sabotage the victim's special-purpose software or hardware systems (e.g., Stuxnet), and will never operate elsewhere, in order to reduce the possibility of detection.

A major attack operation is likely to entail a wide range of modules corresponding to the target it was designed to attack, such as spy modules – searching for files or information and sending the findings to the operator – and attack and camouflage modules – sabotaging centrifuges while misleading the control system, so that the latter will report that the former are in good repair. Such an attack involves many man-years, advanced computer resources, and sometimes hardware systems and testing equipment designed to simulate the theater in which the hostile code will operate, for example centrifuges with Siemens control systems in the case of Stuxnet.

Table 1 summarizes the differences among the various categories of cyber attack by listing the criteria that make it possible to distinguish clearly between types of cyber weapons according to the level of their capabilities. The parameters are divided into several categories. The first includes the cyber weapon envelope and its ability to reach its target and operate freely there without being blocked. The first two parameters are included in this category. Their importance lies in the comfortable work environment that they enable the attacker to enjoy, in the knowledge that he can penetrate his targets and carry out operations there whenever and however he requires, without fearing that his capability will be blocked or his weapon exposed and removed. The next three parameters constitute the second category, which pertains to the cyber weapon's ability to carry out its main activity at the target, whether that be the theft of information, its destruction, or electronic or physical damage or disruption. The various weapons in this category are distinguishable by the algorithms that they apply in order to spy on the target, and by their ability to disrupt computer and physical systems. The ability to cause physical damage constitutes the highest level in this category. The final category represents the two parameters relating to the tool's behavior within the target's network, and the extent of its capability and the freedom that it grants to its operators to conduct the operation at the target. High-level capabilities in this category are those that make it possible to adjust the weapon by delivering modules from a distance and to change the definitions of the task, send orders to the tool, and define new intelligence targets for it. Sophisticated tools will also be able to manage a large data-collection operation on the target's network by spreading to other computers and collecting concentrated and coordinated information from them.

Table 1. Differences among Cyber Attacks

	Major Attack	Medium-Level Attack	Minor Attack	Amateur Attack
Ability to penetrate systems	Very good	Good	Good	Poor
Ability to camouflage activity	Very good	Good	Mediocre	Poor
Spy capabilities	Very good	Very good	Good	Mediocre
Ability to damage computer systems	Very good	Very good	Good	Poor
Ability to damage physical systems connected to the computer setup	Good	Poor	Poor	Poor
Ability to spread	Very good	Good	Poor	Poor
Ability to communicate with a control server	Very good	Good	Mediocre	Poor

The table indicates that the criteria significantly distinguishing major attack capabilities (which few countries possess) from other cyber attack capabilities are the ability to spread on the network, to communicate with the control server, and to damage physical systems connected to the computing systems. These operations require the greatest sophistication in conducting cyber attacks. Only a few countries have access to the knowledge and the ability to produce a weapon of this type. The "minor attack" column in the table reflects the low entry level to the cyberspace battlefield. It appears that even small weapons in the hands of non-state entities are capable of penetrating computer networks well, performing espionage at a very high level, and if they are designed for it, also sabotaging the computer system that they have penetrated. Because their camouflage capability is mediocre, they are unable to reside in the attacked system for as long as heavy or medium weapons, and will therefore have to achieve their objectives within a short time.

Activities in Cyberspace Attributed to Terrorist Organizations

This section examines terrorist operations in cyberspace in accordance with the above delineation, that is, operations whose purpose is to cause deliberate or indiscriminate harm to civilians through action in cyberspace by non-state organizations with political agendas and goals, even if operated or supported by states.

One of the first documented attacks by a terrorist organization against state computer systems was by the Tamil Tigers guerilla fighters in Sri Lanka in 1998. Sri Lankan embassies throughout the world were flooded for weeks by 800 e-mail messages a day bearing the message, "We are the Black Internet Tigers, and we are going to disrupt your communications systems." Some assert that this message affected those who received it by sowing anxiety and fear in the embassies.[31] Several years later, on March 3, 2003, a Japanese cult name Aum Shinrikyo ("Supreme Truth") conducted a complex cyber attack that included the obtaining of sensitive information about nuclear facilities in Russia, Ukraine, Japan, and other countries as part of an attempt to attack the information security systems of these facilities. The information was confiscated, and the attempted attack failed before the organization managed to take action.[32]

An attack through an emissary took place in January 2009 in Israel. In this event, hackers attacked Israel's internet structure in response to Operation Cast Lead in the Gaza Strip. Over five million computers were attacked. It is assumed in Israel that the attack came from countries that were formerly part of the Soviet Union and was ordered and financed by Hizbollah and Hamas.[33] In January 2012, a group of pro-Palestinian hackers calling itself "Nightmare" caused the Tel Aviv Stock Exchange and the El Al Airlines websites to crash briefly and disrupted the website activity of the First International Bank of Israel. Commenting on this, a Hamas spokesman in the Gaza Strip said, "The penetration of Israeli websites opens a new sphere of opposition and a new electronic warfare against the Israeli occupation."[34]

The civil war in Syria has led to intensive offensive action by an organization known as the Syrian Electronic Army (SEA) – an internet group composed of hackers who support the Assad regime. They attack Syrian opposition groups using techniques of denial of services and information, or break into websites and alter their content. The group has succeeded in conducting various malicious operations, primarily against Syrian opposition websites, but also against Western internet sites. SEA's most recent action was aimed mainly against media, cultural, and news websites on Western networks. The group succeeded in breaking into over 120 sites, including *Financial Times*, *The Telegraph*, *Washington Post*, and *al-Arabiya*.[35] One of the most significant and effective attacks was in April 2013, when the Syrian Electronic Army broke into the Associated Press's Twitter account, and implanted a bogus "tweet" saying that the White House had been bombed and the US president had been injured in the attack. The immediate consequence of this announcement was a sharp drop in the US financial markets and the Dow Jones Industrial Average for several minutes.[36] The SEA is also suspected of an attempt to penetrate command and control systems of water systems. For example, on May 8, 2013, an Iranian news agency published a photograph of the irrigation system at Kibbutz Sa'ar.[37]

During Operation Pillar of Defense in the Gaza Strip in 2012 and over the ensuing months, the Israeli-Palestinian conflict inspired a group of hackers calling itself "OpIsrael" to conduct attacks[38] against Israeli websites in cooperation with Anonymous. Among others, the websites of the Prime Minister's Office, the Ministry of Defense, the Ministry of Education, the Ministry of Environmental Protection, Israel Military Industries, the Israel Central Bureau of Statistics, the Israel Cancer Association, the President of Israel's Office (official site), and dozens of small Israeli websites were affected. The group declared that Israel's violations of Palestinian human rights and of international law were the reason for the attack.

In April 2013, a group of Palestinian hackers named the Izz ad-Din al-Qassam Cyber Fighters, identified with the military section of Hamas, claimed responsibility for an attack on the website of American

Express. The company's website suffered an intensive DDoS attack that continued for two hours and disrupted the use of the company's services by its customers. In contrast to typical DDoS attacks, such as those by Anonymous, which were based on a network of computers that were penetrated and combined into a botnet controlled by the attacker, the Izz ad-Din al-Qassam attack used scripts operated on penetrated network servers, a capability that allows more bandwidth to be used in carrying out the attack.[39] This event is part of an overall trend towards the strengthening of Hamas's cyber capabilities, including through enhancing its system of intelligence collection against the IDF and the threat of a hostile takeover of the cellular devices of military personnel, with the devices being used to expose secrets.[40]

Independent Cyber Attacks by Terrorist Organizations

Our analysis of attacks by terrorist organizations in cyberspace reveals that the low entry threshold for certain attacks and the access to cybernetic attack tools have not led the terrorist organizations to switch to attacks with large and ongoing damage potential. Until now, the terrorist organizations' cyber attacks have been mainly against the target organization's gateway. The main attack tools have been denial of service attacks and attacks on a scale ranging from amateur to medium level, primarily because the capabilities and means of terrorist organizations in cyberspace are limited. To date they have lacked the independent scientific and technological infrastructure necessary to develop cyber tools capable of causing significant damage. Given that terrorist organizations lack the ability to collect high quality intelligence for operations, the likelihood that they will carry out a significant cyber attack appears low.

In order for a terrorist organization to operate independently and carry out a significant attack in cyberspace, it will need a range of capabilities, including collecting precise information about the target, its computer networks, and its systems; purchasing or developing a suitable cyber tool; finding a lead for penetrating an organization; camouflaging an attack tool while taking over the system; and carrying out an attack in an unexpected time and place and achieving significant results. It appears that independent action by a terrorist organization without the support of a state is not self-evident. The same conclusion, however, cannot be drawn for organizations supported and even operated by states possessing significant capabilities.

There is also the possibility of attacks by terrorist organizations through outsourcing. A review of criminal organizations reveals that they have made significant forward strides in recent years. The Kaspersky laboratory recently exposed a new group of attackers, apparently commissioned by criminal organizations or by a state for industrial espionage purposes. This is a group of hackers named "Icefog" that concentrates on focused attacks against an organization's supply chain (using a hit-and-run method), mainly in military industries around the world.[41] Another development is the distribution of malicious codes using the crime laboratories of the DarkNet network, which has increased access to existing codes for attack purposes. Criminal organizations are already using the existing codes for attacks on financial systems by duplicating them and turning them into mutation codes.[42]

There is a realistic possibility that in the near future terrorist organizations will buy attack services from mercenary hackers and use mutation codes based on a variation of the existing codes for attacking targets. This possibility cannot be ignored in assembling a threat reference in cyberspace for attacks on the gateway of an organization or even against its information systems. It is therefore very likely that terrorist organizations will make progress in their cybernetic attack capabilities in the coming years, based on their acquisition of more advanced capabilities and the translation of these capabilities into attacks on organizations' information systems (not only on the organization's gateway).

The ability to carry out an attack that includes penetration into the operational systems and causes damage to them is quite complex. The necessity for a high level of intelligence and penetration capabilities, which exist in only a limited number of countries, means that any attack will necessarily be by a state. For this reason no successful attack by a non-state player on the core operational systems of any organization whatsoever has been seen to date. Although no such attack has been identified yet, there is a discernible trend towards improvement of the technological capabilities of mercenaries operating in cyberspace for the purposes of crime and fraud. Presumably, therefore, in exchange for suitable recompense, criminal technological parties will agree to create tools that can carry out attacks on the core operational systems of critical infrastructure and commercial companies. These parties will also be able to put their wares at the disposal of terrorist organizations.

Recommendations for Measures at the National Level

The range of threats in cyberspace is extensive. Basic defenses against these threats need not substantively distinguish among the sources of threats. The notion that a defense can be devised in cyberspace specifically against threats from terrorist groups therefore appears impractical. On the contrary, the defense concept for threats of attacks in cyberspace by terrorist organizations does not, and cannot, differ substantially from an overall defense approach to threats in this realm.

The fundamental concept for defense against cyber threats must be based on a number of basic elements: intelligence, a multi-layer defense approach, an attack approach, public awareness, and civilian defense.

Intelligence

The first basic element in defending against cyber threats is intelligence, including collection of intelligence based on guidance that takes situation assessments into account. In this context, it is important to identify threats and guide the parties collecting the intelligence with respect to information concerning terrorist groups seeking to operate in cyberspace. As noted, in many cases states are behind the activity of terrorist organizations, and intelligence gathered in the state context can also provide information for the terrorist organizations affiliated with or operated by it.

Intelligence constitutes an essential element, second to none, in dealing with threats in cyberspace. The ability to collect and analyze a large amount of information makes it possible today to create high quality intelligence both at the state level and, in more than a few cases, at the level of organizations and businesses that regularly monitor their information and communications networks for the purpose of detecting anomalous behavior that might indicate a future attack, or in order to discern irregular activity on the computer network. In this context, it is appropriate to emphasize that when a country – such as Iran – supports and sometimes even operates terrorist organizations, Western intelligence organizations should monitor not only the target country but also the organizations affiliated with it. In the context of Iran, this means monitoring Hizbollah, Hamas, and the "Syrian Electronic Army."

A Defensive Approach Containing Several Layers

This measure entails a perimeter defense as well as protection of critical assets, including the ability to maintain activity even after penetration by malicious code, and preemptive action against active parties, for example by disclosing intelligence information to law enforcement authorities in countries where the activity is taking place, or using legal tools in other countries. Such action could possibly disrupt the ability to operate the malicious code before it is distributed.

An Offensive Approach to Threats

This element in dealing with cyber threats includes two levels. The first pertains to the ability to take offensive action within – and sometimes also outside of – cyberspace through a preemptive strike against a terrorist organization's cyber resources (infrastructure, financing, websites, and operatives). The second level concerns the ability to conduct retaliatory actions after the attack, and after satisfactory identification of the parties responsible for the attack. Such a strike need not be confined to cyberspace; it can also include real physical elements. In some cases, a legal arrangement for the offensive activity is necessary in order to make the approach effective. In more than a few cases, a chain of operations can be identified if states (such as Iran) operate non-state organizations (such as Hizbollah and SEA), when all together they operate interested parties or even deceived parties within a network for the sake of bolstering their attack capabilities. The need to operate a broad system of attackers requires guidance in a number of contexts. The first involves determining the targets to be attacked, the second concerns the timing of the attacks, and the third pertains to the tools for carrying out the attacks. All of these require the establishment of websites and special forums to which the information is channeled. This activity creates vulnerabilities by enabling disruptive and deceptive action, thereby sowing confusion while softening the impact of the attack planned by its leaders.

Explanatory Activity

It can be assumed that explanatory activity will not be effective within the very hard core of cyber attack operatives. Preventative explanatory activity has two purposes. The first is to increase awareness of the possibility that attackers are liable to be harmed as a result of preemptive activity in the country in which they reside (for example, their exposure to law enforcement authorities in that country). The second is the exposure of those behind the organization. As noted, in many cases, the attackers have been deceived and are completely unaware that they are being operated by states and terrorist organizations. It is therefore possible that these actions can reduce the scope of the phenomenon to some extent.

Organizing Civilian Defense in Cyberspace

The vulnerabilities of the civilian cyber apparatus in Israel constitute a defensive gap inviting terrorist organizations to take advantage of it. The relatively weak defenses of these systems enable terrorist organizations to take simple action against targets in this sphere. Since civilian cyber systems create structural vulnerabilities, a civilian defense should be established in cyberspace, and the sooner the better. The recommendation of the Institute for National Security Studies to the Israeli government is that the defense of civilian cyberspace should be formulated so that it can provide a better solution to threats should be noted in this context.[43]

Terrorist organizations have not yet crossed the operational and technological threshold that would allow them to operate independently against Israel and other Western countries in the cyber warfare sphere. Developments in the criminal attack market, however, are liable to produce significant attack capabilities. These developments, combined with the support and guidance in intelligence and operations provided by technological powers like Iran, could lead to dangerous activity in the cyber field on the part of terrorist organizations. This threat, therefore, should not be taken lightly. Even though no significant activity by terrorist organizations in the cyber field has been observed yet, the development of the threat in this sphere requires appropriate organization.

Notes

[1] The authors would like to thank Noam K. from the National Cyber Staff and Doron Avraham and Keren Hatkevitz, interns in the Cyber Warfare Program at the INSS, for their assistance in preparing this article. Michal Aviad, *Documentary Film* (Tel Aviv: Heidekel, 2007), p. 5.

[2] For example, see Haim Pass and Dan Meridor, eds., *21st Century Battle: Democracies Fight Terrorism, Study Forum* (Jerusalem: Israel Democracy Institute, 2006), p. 25.

[3] For example, see Tor – a software program that helps create anonymity on the web. Every layer is encoded, and every station in the route folds its layer

and delivers it to the next station. This principle is called an "onion router," https://www.torproject.org.

[4] Oded Yaron, "Hackers Plan Cyber Attack against Israeli Targets in April," *Haaretz*, March 14, 2013, http://www.haaretz.com/news/diplomacy-defense/hackers-plan-cyber-attack-against-israeli-targets-in-april.premium-1.509214.

[5] "Steinitz: Military Threat against Israel has also Become a Cyber Terror Threat," *Globes*, July 9, 2013, http://www.globes.co.il/news/article.aspx?did=1000860690.

[6] See the statement by Prime Minister Benjamin Netanyahu on this subject: "Netanyahu: Iran and Its Satellites Escalating Cyber Attacks on Israel," *Globes*, June 9, 2013 http://www.globes.co.il/news/article.aspx?did=1000851092.

[7] This refers to any system for storing, transporting, or processing organizational information, whether or not it is connected to the internet, and whether or not it constitutes part of the organization's core business.

[8] An organization's core operational system is the hardware on which the organization's core processes are managed and the software used for that purpose (whether it is a security or a civilian business organization). Disruption or destruction of such a system can halt all or part of the organization's activity and could cause physical damage in certain cases.

[9] An industrial control system (ICS) is a tool that integrates software and hardware components and is designed to oversee a physical production process. The system contains sensors for monitoring the controlled process and inspectors who control this process. The system is also likely to include a connection to the organization's other computer networks and sometimes also to the internet.

[10] This type of attack is also carried out independently by activists and anarchists, or on behalf of and guided by a terrorist organization.

[11] "Shamoon Virus Targets Energy Sector Infrastructure," *BBC News Technology*, August 17, 2012, http://www.bbc.co.uk/news/technology-19293797.

[12] In this incident, malicious code was inserted into Aramco's computer system, and 30,000 computers were put out of action as a result.

[13] Ralph Langner, lecture on the subject of securing industrial control systems, Annual Cyber Conference, Institute for National Security Studies, September 4, 2012, http://youtube/sBsMA6Epw78.

[14] "The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Ply their Trade on the Internet," *Daily Mail*, October 11, 2013, http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html.

[15] Jesse Emspak, "Why We Won't Soon See another Stuxnet Attack," *Tech News Daily*, July 24, 2011, http://www.technewsdaily.com/7012-stuxnet-anniversary-look-ahead.html.

16 Aditya K. Sood and Richard J. Enbody, "Crimeware-as-a-Service – A Survey of Commoditized Crimeware in the Underground Market," *International Journal of Critical Infrastructure Protection* 6, no. 1, (March 2013), http://www.sciencedirect.com/science/article/pii/S1874548213000036.

17 A Facebook page offering cyber weapons for sale can be found at https://www.facebook.com/groups/53807916899/.

18 Limor Kessem, "Zeus FaaS Comes to a Social Network near You," *RSA*, *Speaking of Security*, April 2013, http://blogs.rsa.com/zeus-faas-comes-to-a-social-network-near-you/.

19 Michael Fire, Rami Puzis, and Yuval Elovici, "Organization Mining Using Online Social Networks," *arXiv:1303.3741* .

20 Aviad Elishar, Michael Fire, Dima Kagan, and Yuval Elovici, "Homing Socialbots: Intrusion on a Specific Organization's Employee Using Socialbots," International Workshop on Social Network Analysis in Applications (SNAA), August 2013.

21 Fernando M. Pinguelo, Bradford W. Muller, Norris McLaughlin, and P.A. Marcus, "Is Social Media a Corporate Spy's Best Friend? How Social Media Use May Expose Your Company to Cyber-Vulnerability," *Bloomberg Law*, http://about.bloomberglaw.com/practitioner-contributions/is-social-media-a-corporate-spys-best-friend/.

22 Internet Census 2012, Carna Botnet, http://internetcensus2012.bitbucket.org/paper.html.

23 Map of SCADA systems in the world, http://goo.gl/maps/nqnan.

24 The Shodan website, which contains information useful to hackers: http://www.shodanhq.com/.

25 Gili Cohen, "Hackers Attack Home Networks of Hundreds of Israelis," *Haaretz*, September 11, 2013, http://www.haaretz.co.il/misc/2.444/.premium-1.2117098.

26 Attack vector: http://searchsecurity.techtarget.com/definition/attack-vector.

27 Spoofing attack: http://www.webopedia.com/TERM/S/spoof.html.

28 Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): p. 80.

29 Doug Macdonald, "A Guide to SpyEye C&C Messages," *Fortinet*, February 15, 2011, http://blog.fortinet.com/a-guide-to-spyeye-cc-messages.

30 Thomas Rid, "Cyber-Sabotage Is Easy," *Foreign Policy*, July 23, 2013. http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it?pa.

31 Dorothy E. Denning, *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S House of Representatives, May 23, 2000, p. 269, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

[32] For a chronology of the Aum Shinrikyo actions, see http://cns.miis.edu/reports/pdfs/aum_chrn.pdf.

[33] Paul Everard, "NATO and Cyber Terrorism," in *Response to Cyber Terrorism*, (Ankara, Turkey: Center of Excellence Defence against Terrorism, 2008), pp.118-126.

[34] Daniel Cohen and Aviv Rotbart, "The Proliferation of Weapons in Cyberspace," *Military and Strategic Affairs* 5, no. 1 (2013): 59-80 .

[35] Dylan Love, "10 Reasons to Worry about the Syrian Electronic Army," *Business Insider*, May 22, 2013, http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1#ixzz2h728aL8P.

[36] Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets," *The Telegraph*, April 23, 2013. http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

[37] Yanir Yagna and Oded Yaron, "Israeli Expert Said, 'Syrian Electronic Army Attacked Israel' – and Denied It," *Haaretz*, May 25, 2013, http://www.haaretz.co.il/news/politics/1.2029071.

[38] Amir Buhbut, "Cyber Attack: Prime Minister's Office, Ministries of Defense, Education Websites Put out of Action," *Walla News*, April 7, 2013, http://news.walla.co.il/?w=/90/2630896.

[39] Nimrod Zook, "Cyber Attack: Izz ad-Din al-Qassam Fighters Hit American Express," *Calcalist*, April 2, 2013, http://www.calcalist.co.il/internet/articles/0,7340,L-3599061,00.html.

[40] Lee Yaron, "Defense Department Warns: Hamas Cyber Capabilities Stronger," *Bamahane*, November 14, 2013, p. 19.

[41] "Kaspersky Lab Exposes 'Icefog': A new Cyber-espionage Campaign Focusing on Supply Chain Attacks," September 26, 2013, http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks.

[42] For more on mutation codes, see Cohen and Rotbart, "The Proliferation of Weapons in Cyberspace."

[43] Gabi Siboni, "A National Response to Civil Defense in Cyberspace," Viewpoint Paper for Decision-Makers, Institute for National Security Studies, April 2013, http://heb.inss.org.il/index.aspx?id=4354&articleid=5904.

Intelligence 2.0: A New Approach to the Production of Intelligence

David Siman-Tov and Ofer G.

In recent years, intelligence has undergone profound changes, both in relationships within the intelligence system and in relations between it and the political and military environment that it serves. These changes are also reflected in the practice of intelligence today and in the new concepts appearing in the discourse on intelligence, which are displacing the traditional approaches, now outdated. The developments in intelligence are the necessary result of the profound changes taking place in the human situation and in the nature of warfare in the twenty-first century. At their center is the profound change in the character of the enemy and the nature of wars and the profound change inherent in the transition from the industrial age to the digital information age. This article examines the changes that have taken place in intelligence and presents a number of problems which the intelligence community faces today. Its main argument is that intelligence capabilities can be significantly improved and brought into the twenty-first century if we adopt a new approach to intelligence that draws its main inspiration from Web 2.0.

Keywords: intelligence, Web 2.0, intelligence cycle, research collection relations, Wikipedia, blogs, research collection

In recent years, the field of intelligence has been undergoing profound changes both within the intelligence system itself and in its relations with the political and military echelons. These changes manifest themselves in the intelligence community's current practices as well as its discourse, where new perspectives are gaining attention and displacing traditional,

David Siman-Tov is a former researcher at the Military Intelligence Directorate's Institute for the Study of Intelligence. Lieutenant Colonel Ofer G. is a branch head in the Research Department.

outdated approaches. The changes in intelligence are the inevitable results of profound changes taking place in human reality and the nature of warfare in the twenty-first century. At the core of these changes is the profound change in the nature of the enemy and the character of warfare, as well as the profound change inherent in the transition from the industrial age to the digital information age.

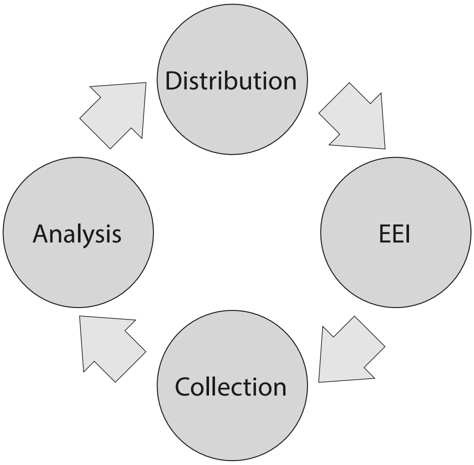
This essay examines the changes that have occurred in the production of intelligence and presents several problems that the intelligence community currently faces. The main argument of the essay is that it is possible to improve intelligence capabilities significantly and move them into the twenty-first century if a new approach to intelligence making is adopted, one that draws its inspiration primarily from the Web 2.0 phenomenon.[1]

The Intelligence Cycle as an Organizational Principle

The intelligence cycle was the major organizational principle on which intelligence institutions were constructed and around which they operated after World War II. In Israel's case, this cycle was preceded by activity carried out by individuals without an organization, without any particular method, without a hierarchy, and without any distinction between collection and analysis. Chaim Herzog, the third head of Israel Military Intelligence and the head of the intelligence department at the IDF's Operations Branch, described the situation as follows:

> At the start, there were primitive beginnings... small empires with small generals who maintained direct relations with Ben-Gurion, every one of whom ran to him with his intelligence....There were some good people [but] they lacked a military infrastructure, concepts, an analytical approach, research and working methods – collection, classification, analysis, and dissemination in a scientific manner. In other words, turning information into intelligence is a science in and of itself. We brought working methods from the [British] army and built military intelligence.[2]

The concept of the intelligence cycle identified several clear and separate stages, all of which together comprise the intelligence process: information collection, information processing (analysis), and distribution of the resulting intelligence to the various consumers. Furthermore, the process involves the commanding officer or leader extracting the so-called



essential elements of information (EEI). These steps become part of a cyclical recursive process (figure 1).[3]

Figure 1. The Intelligence Cycle

The concept of the intelligence cycle was applied with the founding of Israel's military intelligence establishment in the form of the IDF's Intelligence Branch (Military Intelligence, or MI). There, the intelligence enterprise was divided into two groups: collection agencies and analysis agencies. The collection branch (and later, the collection department) mediated between the two types of agencies with a great deal of success by providing overall direction from above while making use of the EEI, which included a limited number of carefully crafted questions. It remained for the analysts, accordingly, simply to receive the "ready-made" information; they had virtually no involvement in the work of information collection.

The rationale behind the intelligence cycle was to organize intelligence production according to clear guidelines. Compartmentalization, one of its leading principles, was not only the result of security concerns but also the result of a particular conceptualization of the work. It was meant to ensure that "everyone would do his job" and not "interfere" with the jobs of the other system components or become biased through contact with them.

Another norm stemming from the organizational principle of the intelligence cycle was the one-way flow of information: the analysts sent the EEI questions to the collectors, and the collectors sent the answers to the analysts. There was little room for either side's involvement in the daily workings of the other.

Yet another key principle upon which the intelligence cycle rested was the so-called "value chain," which holds that the more progress is made along the intelligence process, the greater the value of the intelligence product, that is, from raw data to distilled intelligence, and from there to an intelligence assessment expressed in an analytical research document.

The intelligence cycle did not have – and did not need – any form of shared discourse or space to develop knowledge, because each of the different components of the system had its own separate and distinct job, and because the operating assumption was that every component of the system could and should do its job independently.

The separation among the intelligence system's components grew even more pronounced starting in the 1970s as a result of the Yom Kippur intelligence failure and the Agranat Commission's report, which led, inter alia, to the concept of intelligence pluralism being incorporated as a formative principle designed "to ensure the effective functioning of all members of the intelligence community to provide warning." The Agranat Commission's full report, declassified in recent years, stated that, "it is necessary to institute wide-ranging changes in the structure of IMI that will allow the expression of opposing views by analysis department personnel."[4]

Cracks in the Intelligence Cycle

In the 1960s, sectors of the Israeli intelligence community began to challenge the validity of the intelligence cycle as the exclusive organizing principle of the intelligence enterprise. For example, direct contact between surveillance bodies and operations bodies such as the Air Force and the Navy, which began in the 1960s, serve as evidence of an understanding that, at least with regard to certain threats, it was necessary to create "short cycles" between collectors and analysts. Another example was the involvement of analysts in the development and debriefing of human intelligence sources (HUMINT). But these were still the exceptions to the rule, and most of the intelligence enterprise was conducted in accordance with the division of labor described above. By contrast, in recent years, many in the intelligence community have concluded that the intelligence cycle is no longer valid as the exclusive organizational principle. Additionally, in the American intelligence discourse there are now voices calling for the intelligence cycle to be "killed."[5] Why are these voices becoming more prevalent?

There are many causes and reasons, but an examination of the most fundamental influences reveals two historic revolutions that started at the end of the previous century. The first is the transition from the industrial age to the digital information age, manifested in the appearance of cyberspace, including the invention of the computer and the internet, which have profoundly changed human conduct. The second is the Revolution in Military Affairs in which the focus has shifted from confrontations between nations and armies to a growing range of nonconventional, non-state conflicts of a dynamic, hybrid, networked nature.

To deal with the shifting challenges of warfare, joint teams consisting of intelligence bodies and operations bodies were established as early as the 1970s (for example, the Air Force's Operations Intelligence Teams), but for many years these remained few and far between. Currently, given the frequency of asymmetrical conflicts in which the enemy can vanish into the surrounding population, the reduced window of opportunity for counteraction (a matter of minutes in some cases), and the ever-increasing challenge of minimizing harm to non-combatants, the concept of a war room that integrates all the relevant components of intelligence and operational systems – in order to complete the intelligence and operations cycle in real time – has become the standard way of thinking. This type of adjustment proves that it is possible to break organizational patterns given urgent operational needs.

On the basis of the same rationale – but in the context of intelligence challenges of a long term or infrastructural nature – a new form of intelligence structure has developed, one in which task-driven intelligence teams are built, combining all the relevant functions and capabilities (all types of collection and analysis) in order to deal with an intelligence issue in a holistic manner. Like joint attack cells, this structure also breaks organizational molds, but because these bodies operate over time rather than only during a specific operation, they pose a much greater threat to the classical organizational culture, which sanctifies compartmentalization.

Another development that has challenged the validity of the intelligence cycle is the creation of a networked log shared by all parties, which in wartime allows all participants to provide and receive updates in real time. The utility of such a log is obvious: all collectors know with great precision, and in an unmediated form, what the EEIs are and provide immediate responses; they understand in real time the problems of concern to the analysts or operational bodies and contribute as much as they can to their resolution. At the same time, analysts receive the information they need in a timely fashion and with unprecedented exposure to the work of collection, with none of the filters or limitations typical of the principle of the intelligence cycle. The challenge to the entire concept of the intelligence cycle lies not only in doing away with the compartmentalization but also *in breaking the principle of the value chain*. The networked log is an embodiment of the understanding that, at least when time is of the essence, collected material that has not undergone organized processing and classification but arrives in real time has much greater intelligence value than canonical intelligence data that the collection unit has officially approved as fit for dissemination.

We have provided examples of tools and organizational structures already in place in the Israeli intelligence community that are recognized as being an integral and necessary part of the intelligence enterprise. These are not yet used widely enough, however, and there are still arguments over the potential for transforming them from isolated instances of shared space to a dominant facet of the overall work of intelligence.

Another fundamental reason for challenging the intelligence cycle paradigm is the information age. More concretely, one may speak of the emergence of cyberspace as the catalyst accelerating the change in two senses: one is the focus on information flow, information variety, and accessibility of information for both analysts and collectors, and the second expresses the new ways and approaches in the development and preservation of knowledge. The transition of the center of gravity in the world of information and knowledge away from institutions and into the hands of the masses (Wikipedia being a perfect example) and the appearance of blogs and social media, which as we will show later on are part of the Web 2.0 revolution, are a major factor in destabilizing the traditional method of intelligence production. They increase the tension between the way in which civilian information develops, flows, and is stored, and the outdated nature of the intelligence cycle. The new approach of information sharing and knowledge development is trickling into the intelligence community, to a great extent via the influence of the younger generation that brings to the world of intelligence the culture of information sharing and knowledge development to which it is exposed during leisure time.

Furthermore, the nature of information collection in the cyberspace era is changing and is based more on textual information and databases than on telephone conversations using jargon intelligible only to collectors. In light of the complexity and scope of information available in this world, collection can no longer handle the raw materials at its disposal by itself; *a much stronger, richer and more profound connection is needed between collection and analysis*, with a focus on joint study and action in order to cope with the ever-growing challenge.

Similarly, technological and economic issues that surface in intelligence material underscore the advantage of having analysts who specialize in these fields and the need for their assistance in fully extracting potential information. At any rate, given the enormous volumes of information, collection efforts will flounder unless they incorporate analysis in order to separate the critical from the peripheral.

In short, the clear line between collection and analysis is blurring. Slowly but surely all participants in the intelligence system are becoming partners in the same task. It should be strongly emphasized, however, that the lines between the intelligence system's components have not disappeared altogether. Each side must retain its professional uniqueness in order to bring its added value to the overall endeavor. But each side must devote more time to getting to know the other side – its partner in the intelligence system. Analysts must become better acquainted with the uncertainties and capabilities of collectors, while collectors must become better acquainted with the uncertainties and needs of analysts.

With the emergence of cyberspace, new tools and methods were quickly integrated into intelligence production. Nonetheless, it appears that the intelligence cycle has not yet been broken and, in fact, continues to serve as the main organizational principle. For example, information items and reviews started circulating through automated systems such as email rather than being disseminated as hard copy, as had previously been the case, so as to shorten dissemination time, expand the list of recipients, and improve the ability to preserve information and retrieve it later. Yet the concept of unidirectional transmission of information from one component to another remains entrenched, and does not allow for the creation of a shared space to preserve and develop intelligence knowledge.

Another major difficulty is the inability to connect information systems of different organizations. These systems were built as closed loops, as there was almost no need for integration connectivity between them. The unfortunate result is that while connectivity within units has improved, connections among them are still minimal. The attempt over a decade ago to establish an intelligence network at IMI was not very successful; this network was secondary at best; it was not the main workspace, nor does any intelligence information develop on it.

Starting in the early 2000s, an attempt was made in the IDF to apply tools and methods of information management and development. In hindsight, these may now be called Web 1.0, and they included organizational and topical portals, various forums, and working rooms. The goal of the new tools and patterns was to manage intelligence information and create intelligence information communities, but almost every such attempt ended in failure: the portals that multiplied like mushrooms after the rain were closed one by one, becoming virtual tombstones. The intelligence forums and working rooms remained desolate and static. No new knowledge was produced in them, and before long they did not even serve to preserve current information. MI's attempt to adopt new tools for information management and preservation failed. The gap between the impressive vision of the project in its early years – "the creation of intelligence communities producing information and knowledge" – and reality was woefully large.

Among the causes of this failure is presumably the lack of any conceptual change in advance of the technological initiative. If no unit deems it is necessary to operate in a networked way with other units on a daily basis, then communities of knowledge, which are essentially the connections among different bodies, are unlikely to emerge. Furthermore, no attempt was made to translate or interpret the external tools that had been brought into the unique and truly distinctive world of intelligence.

Notably, difficulties in integrating and the failure to integrate civilian information systems and applications from the world of Web 1.0 into organizations are not unique to the intelligence community. In an essay analyzing the failure of portals in other organizations, the author argues that among other reasons one may point to organizations' failure to give heed to the social network of the workplace and to organizations' creation of a unidirectional platform of communications that ignored the opportunity for consumers – namely, the employees in the workplace – to contribute contents of their own to the portal. In addition, many of the failed portals were constructed uniformly, not allowing users to create a homepage based on their personal needs and desires.[6]

Web 2.0: Cultural and Conceptual Innovations

Web 2.0 is a technological and socio-cultural phenomenon referring to the second generation of internet products and services. While the first generation, or Web 1.0, focused on websites whose contents were created by webmasters and where the flow of information was unidirectional, from the producer to the consumer, the second generation refers to websites as an infrastructure for the joint creation of contents relying on information sharing and user creation. The revolution within this phenomenon is more cultural than technological, whereby the ordinary user is transformed from a passive consumer of information to an agent of its creation. Control is no longer in the exclusive hands of the media and institutions but has been handed over to the people, creating a hitherto unknown democratization of knowledge. It was absolutely fitting that the *TIME Magazine* voted the internet user as its Person of the Year in 2006.[7]

Thus, *Web 2.0 is the technological infrastructure for sharing and creating contents by the users themselves amongst one another using the social media*. Web 2.0 expresses the idea of the "prosumer" (producer + consumer), a term coined by Alvin and Heidi Toffler.[8] It represents the rise of the new economic element: consumers who are involved in the production of the services and products they consume. It also expresses the notion of the "wisdom of the crowd" via technology and a collaborative approach by which individual contributions add up to the development of knowledge of a scale and quality that could never have been created otherwise. A salient manifestation of this phenomenon is Wikipedia, which is not merely an online encyclopedia but rather the collaborative effort of users who create its contents.

Another concept relevant to the Web 2.0 revolution and manifesting its inherent social changes is the Y Generation, the current generation born into the internet revolution and experiencing the rapid changes it entails. This generation is characterized by the ability to adapt to rapid technological changes, work as a team, multitask, and make extensive use of social networks as a primary means of making contacts and transmitting contents. Unlike the previous generation, which made do with email as an alternative to traditional mail, members of Generation Y prefer Facebook as the platform for transmitting messages in various ways.

Web 2.0 is also characterized by a rich and varied user experience, with laptops, smartphones, tablets, and the like, alongside new and continuously changing ways of transmitting messages, from blogs to Twitter, which allows yet another form of contact based on followers. Add to all of these the concept of serendipity, which the internet facilitates and fosters. Often internet surfers receive unsolicited friend requests from people likely to interest them, or their attention is directed to items likely to be of value to them without actively having looked for them. This is radically different from the question-and-answer approach embodied by the intelligence cycle.

Intelligence 2.0

The Principles of the Intelligence Net

This section will describe how a relevant interpretation and implementation of Web 2.0 can provide a response to the problems currently afflicting intelligence. Clearly there is no magic remedy, and the approach suggested here does not stand on its own. Rather, we propose an examination of its application to the world of intelligence, while offering an interpretation that will tailor our suggested approach to the uniqueness of that world.

The first adaptation necessary is the prerequisite of applying the Web 2.0 concept differently in the two working environments of intelligence – the internal intelligence environment and the external environment in which intelligence is a central participant. The intelligence environment includes many different knowledge communities. Some deal with a specific enemy (such as Hizbollah or Iran), some deal with a specific sector (such as Lebanon and its power players), and some deal with weapons threats or technological threats and the like. The internal intelligence environment comprises several partners – the collectors and analysts at MI and the intelligence community, including the Mossad and Israel's Internal Security Service. By contrast, the external environment includes a long and varied list of planning and operations bodies in the IDF and the political system (such as the National Security Council staff and government ministries) as well as certain civilian research institutes. Within the internal environment, intelligence is mainly focused on obtaining information and developing knowledge about "the other," on the basis of an understanding of the needs of the external environment. In the external environment, intelligence aids the processes of formulation, planning, and execution, by means of the information it obtains and the knowledge it develops.

The organizational principle at the core of the Intelligence 2.0 concept is that of a shared, networked space of intelligence. Instead of a hierarchic, compartmentalized division of labor, we suggest adopting a shared, networked intelligence space and dynamic, evolving intelligence communities of knowledge. This is a shared space on several levels: a shared space for analysts and collectors working together to develop knowledge about the enemy, a shared space among various research units in order to enhance their understandings using a single infrastructure, and a shared space for the intelligence community and the communities using the intelligence (the intelligence "consumers," the technological knowledge community serving intelligence, and more). In the new shared space, the sharp distinction between producer and consumer blurs. All sides – analysts and collectors, the intelligence producers and the intelligence consumers – become partners within new communities of knowledge that share a single goal: the development of applicable knowledge for the benefit of political and military endeavors, without attempting to displace one another and while retaining all professionalism and discipline-specific expertise.

Suggesting a shared networked space as a new foundation for intelligence production does not conflict with the creation of shared physical spaces for intelligence units, whether in ad hoc locations for a specific operation (a shared command center for analysts, collectors, and operatives) or in shared production and research rooms for analysts and collectors to deal with a designated mission or for routine work. In this essay we do not discuss the possibility of shared physical spaces, which is worth exploring further as another significant factor affecting the work of intelligence.

Calls for the creation of a shared intelligence space are gaining ground in the current discourse. But it seems that in the context of this discourse, one fact is being overlooked: shared spaces, by virtue of their very nature, blur the lines between the various participants, especially among the various research bodies, thereby undermining the pluralism principle. Should the pluralism principle be put to the test of time, we will likely find it has not made any significant contribution to intelligence or to the prevention of errors and surprises; on the contrary, it has contributed only to isolationism and unhealthy competitiveness in the Israeli intelligence community.[9] Moreover, given the mass quantity and complexity of the challenges currently facing intelligence, the constraining paucity of resources, and above all the complex, hybrid, networked nature of many of the threats (global jihad is a good example), one must reject the pluralism principle and prefer unification of all intelligence efforts.

It is not necessarily the case that the networked approach to intelligence would abolish the pluralism principle; in fact, it may endow it with a new interpretation as well as better and more meaningful applicability. The recommendations of the Agranat Commission about the need for a multiplicity of opinions and transparency of information can be implemented through shared networked spaces. These spaces would reflect all intelligence information and provide better opportunities to express and present divergent opinions among intelligence personnel within the same organization or among intelligence personnel in different organizations representing different perspectives. Consequently, the proposed approach of a shared knowledge space would enhance the intelligence discourse and easily accommodate a platform for dissenting voices, intelligence debates, conflicting theses, and different stances and interpretations, while reducing the current duplication of work by fellow analyst groups.

Another key idea at the core of the new space is discourse, that is, the willingness of members of the knowledge communities to participate and share their insights. To a great extent, discourse is an alternative to the EEI paradigm, which for many years has not been serving its purpose. Discourse platforms created by Web 2.0 are likely to allow analysts and collectors to hold intimate discussions of their work, in real time *and* on a continuous basis. An analyst receiving a new report from a collector would be able to refer to it or ask for clarifications in close to real time. The collector would learn if the information provided to the community was helpful or not and would be able to supplement it with additional information that could not be included in the official framework of canonical intelligence data as currently disseminated by collectors' units.

A sequence of such responses – the transition from EEI to discourse – is an important foundation for examining the success of the knowledge community. A state in which community members do not feel comfortable being exposed and do not respond to one another's input would signify a possible failure in the way the discourse was constructed in that space, and the discussion leaders would have to take steps to solve the problem. It is essential that there be leaders of the knowledge community responsible for advancing the processes of knowledge development.

By implementing the idea of Intelligence 2.0, a fundamental change would occur in the retention of organizational knowledge and in the creation of an organizational memory. At present, knowledge that does not make it into official documents is lost. Most of the informal discourse is carried out through email, but it is not systematically stored and its potential to serve as an organizational asset is simply wiped out. Personnel who have held important positions over many years in the organizations are focal points of organizational knowledge. When they leave, the information in their heads and the materials accumulated and developed on their computers, simply vanish. These are organizational assets of the highest order, but they are not defined as such, and there is currently no attempt or means to preserve them. In the new approach we propose, the great emphasis placed on processes of internal discourse would allow the system to distill, reveal, and make accessible all the informal knowledge contained in the minds of intelligence personnel who are themselves knowledge focal points. They would be offered an opportunity to share personal insights and databases that they stored on their personal computers in a systematic, regular manner, as a matter of routine organizational activity.

Key Tools in Implementing the Approach

Having examined some of the major conceptual aspects that could characterize the Intelligence 2.0 approach, we will now present some of the essential tools of the world of Web 2.0 and examine the adaptation they would require for the world of intelligence.[10]

Within the shared intelligence space, it is possible to create an "Intelligence Wikipedia" accessible to all members of the intelligence community, who would also be partners in its constant revisions and updates. In this Wikipedia it would be possible to post updated analytical entries about the enemy as well as organizational information about intelligence doctrines and philosophies of use, various working plans, and intelligence projects.

Clearly this endeavor would require the formulation of rules that differ from those used in the civilian sector, where the wisdom of the crowd provides the foundation for Wikipedia's existence. By contrast, the wisdom of experts (individuals or small groups) would serve as the Intelligence Wikipedia's foundation. But the few experts in each field would be able to learn from one another and present the information and knowledge they have in the same Intelligence Wikipedia entry so as to create the fullest picture possible of the subject instead of competing with one another. Unlike Wikipedia, updates in the Intelligence Wikipedia would not be a voluntary or optional exercise, but would be incorporated into the guidelines and new job descriptions of the organization and would constitute a key obligation of the authorized editors. Another salient principle of the internet that is unsuited to the intelligence environment is the principle of anonymity, because in the intelligence environment great importance is attached to knowing who is responsible for a particular insight in order to enable clarifications and updates from the same individual.

Parts of this Intelligence Wikipedia would be available within the space that is shared by the world of intelligence and consumers outside of this world, but within that space it would not be possible to change the entries. That is to say, the Intelligence Wikipedia would be able to serve as a generic, accessible knowledge base serving members of the intelligence community as they prepare intelligence products, and these intelligence products could in turn serve as a knowledge base and could be updated via Intelligence Wikipedia entries. The updating of finished products as entries in the Intelligence Wikipedia could also enhance the timeliness of intelligence knowledge. That is, unlike the present situation, in which some of the information within an intelligence review quickly becomes outdated (but not to the extent that the entire review requires updating), the Intelligence Wikipedia would allow the review to be kept current because any corrections or updates could take place in real time.

In the shared space, blogs would serve as a central tool that some participants could use to record their personal insights in a continuous, timely manner. But unlike the situation in the civilian internet, it would be inappropriate to allow anyone in the intelligence community to start a blog without restrictions, guidance, or oversight. It might be necessary initially to limit the organization's network of blogs to include only the organization's knowledge focal points and senior personnel. Some of the veteran intelligence personnel have a great deal of unique knowledge – musings on methodological issues, insights regarding intelligence issues resulting from many years of service, personal experiences of intelligence events with doctrinal value, and more – that has no room for expression in the usual official products. Similarly, there are senior personnel who would like to be able to transmit, frequently and informally, their perspectives on processes in the organizations for which they are responsible and suggest directions for continued action. Blogs could serve as an ideal platform for these people and allow them to put their insights into writing.

One of the most important and promising directions that the Web 2.0 era can offer intelligence is the establishment of a social intelligence network,[11] which in the future would serve as an advanced alternative to organizational email. Organizational email, adopted as a main working tool in the IDF and MI in the early 2000s, was designed to transmit messages amid an organization's personnel. It was not meant to be a technological platform for the construction of knowledge, but in the world of intelligence it became one nonetheless, because of the great need for such a tool and the lack of an alternative. The use of organizational email for sharing and developing knowledge is rife with problems and drawbacks: for technical reasons and because of issues of compartmentalization, it is impossible to transmit a message to all appropriate addressees; it is impossible to carry out discussions over time (the shelf-life of an email discussion is short); email messages do not appear in a user's inbox according to any rational order of classification by intelligence issues, but rather in a uniform, undifferentiated list (alongside a great deal of junk mail); and, worst of all, it is impossible to save email messages systematically, meaning that the knowledge developed through them is lost.

The broad integration of social media would mark a profound revolution in connectivity among individuals in an organization and create living, dynamic knowledge communities that would serve as critical infrastructure for any future intelligence organization. Thus, instead of providing only the members' names, telephone numbers, and job descriptions (the current situation in non-social organizational networks), the social network would allow one to become acquainted with the organization's individuals the way Facebook allows one to form acquaintances in the civilian sector. Every individual would be able to define the relevant colleagues ("friends") and follow them and any new contents they may post to the network.

Moreover, the profile of every user would automatically, as well as through manual input, include areas of expertise and interest (as a consequence, for example, of jobs held and academic, military, and intelligence training) and official and unofficial publications and writings. By assessing these criteria, the system would be able to suggest appropriate contents as well as invite individuals to participate in certain online discussions and knowledge communities likely to be of interest, which they would not otherwise have discovered. Similarly, using the same criteria, other friends on the network would be able to locate this individual and request assistance, whether through a proactive search or through the system's capacity for suggesting introductions and sharing profile contents.

Another fundamental change inherent in Intelligence 2.0 would be the ability, which does not exist today, to hold asynchronous discussions, that is, long-term, discontinuous discussions of an issue. A culture of debate that does not require everyone to be available at the same time is a good approach to adopt not in order to replace physical meetings but as a necessary complement that provides added value. For example, embassy staff in the United States or India would be able to participate in a discussion about the country in which they are serving, and members of the intelligence knowledge communities located at opposite ends of a country would be able to meet. Individuals would also be able to contribute to a discussion that took place several months earlier but is still relevant.

One can develop this idea further and propose that discussion groups on the social network (knowledge communities) be officially designated as the primary organizational configuration for joint intelligence mission teams. At present, the notion of joint mission teams is suspended between two alternatives, neither of which is ideal for classical intelligence organizations. On the one hand, there is the model of a joint mission team functioning on a part time, limited basis, with members who participate while also fulfilling a host of other functions. Consequently, the joint mission team holds team member meetings only once every few weeks or months, and the processes of learning, sharing, and knowledge development take place in a very limited way because of time and information systems constraints. On the other hand, there is the alternative of the joint mission team whose mandate constitutes the only mission for its members, who work together in a shared physical space.

Conclusion

In this era, competition over learning is becoming a central battlefield, and intelligence organizations must become institutions that can quickly learn and adapt to changes occurring in their sphere of activity. Incorporating the concept of Web 2.0 into the intelligence enterprise, with relevant interpretations and modifications for the intelligence environment, has the power to generate a revolution that could fundamentally change the relationships among the various intelligence organizations, and between them and their consumers. This approach can endow working processes with the interconnectivity, synergy, flexibility, and speed that are critical in confronting the dynamic challenges and hybrid enemies of the current era.

Implementing the new approach entails serious difficulties and challenges for a variety of reasons. First, the approach would seem to contradict the intelligence traditions of secrecy and compartmentalization, on the one hand, and of competitiveness and pluralism, on the other. A culture in which "knowledge is power" and where sources and information are only revealed on a strict need-to-know basis will find it difficult to change abruptly and work according to the new guiding principle that "sharing is power" and sources and information should be disseminated on a need-to-share basis.[12]

Another significant difficulty, an offshoot of the above, is the lack of technological connectivity among intelligence organizations, not to mention between them and their consumers. The reality is one of network isolationism, the result of a long tradition of compartmentalization, differentiation, and competition among the components of the intelligence community, stemming in part from the guiding rationale of the intelligence cycle. The connectivity sought refers not merely to email (which also does not always exist), but rather to the creation of a shared network space that would allow the development of shared knowledge and a knowledge base to which everyone is a partner.

A further problem that sometimes prevents organizations in general, and intelligence organizations in particular, from adopting social media into their organizational midst is the organizations' fear of the creation of a new type of knowledge. This fear stems from veteran personnel's concerns regarding the new technology and the philosophy it represents and from concerns that communication through a social medium will distract the individuals in the organization from their tasks. Indeed, it should be underscored that implementation of a social network in the intelligence world is liable to generate tension between the chaotic nature typical of civilian internet surfing and the need for focus and mission-driven action in the intelligence world. How can one optimize the use of a social intelligence network in order to take full advantage of its unique features while also circumventing the problems that these very features pose for the mission-driven nature of intelligence?

Yet another significant challenge, illustrated by the American experience,[13] is the possibility that the new tools for creating contacts and transmitting messages among members of the intelligence communities, and the tools for saving and developing intelligence knowledge, will turn into additional secondary tools among the organizations' information systems. If that happens, not only will the new tools fail to serve the development of intelligence knowledge, they will in fact create duplication and prevent the social intelligence network from becoming the primary space in which organizational knowledge is kept and developed.

Meeting these challenges consists of several steps. Most importantly, it is critical to define the social intelligence network as the organization's primary operational working environment. This is the tool the intelligence community must use to communicate better internally and with external agencies that could, to a limited extent, be incorporated into it. Thus, an intelligence version of Facebook would serve, inter alia, as the workspace of mission-driven teams, and the Intelligence Wikipedia would be the place for retaining knowledge in the system. Processes of preparation and authorization of intelligence products would also occur in the new shared space.

A networked space based on the Web 2.0 concept must be effective and offer value-added elements for information management. To this end, it is necessary to make sure that all of the organization's information sources and knowledge assets be concentrated and available in this space, while giving more advanced options both to preservation of information and knowledge and to access to them (integrating and incorporating contents, document and file sharing, connections to external systems, access to databases, robust retrieval services). As groundwork, a true revolution in the field of inter-organizational information systems and connectivity is needed. The creation of shared spaces will be possible only if standardization occurs so that different systems can communicate with one another.

Beyond this, there is a need for a profound cultural and conceptual change, similar to the understanding that developed in the American discourse. Incorporating new technological tools is not enough. The change must also entail training and the institutionalization of new professions. Furthermore, there must be a doctrinal review of the development of intelligence knowledge, leading to a revamping of outmoded organizational processes and an end to patterns that only serve to reinforce inter-organizational isolation and competition.

There are several proposals in the current American discourse for pulling the intelligence wagon out of the rut in which it is stuck. Especially noteworthy is the "Living Intelligence" approach developed by the National Geospatial-Intelligence Agency (NGA), which calls for changing the old culture, habits, and patterns of intelligence production.[14] The innovation of this approach is its call for viewing social media as the primary working environment of the intelligence community. In other words, the approach is chiefly concerned with intelligence products and suggests making intelligence products, their production processes, and their manner of presentation networked and social. The approach also calls for creating integrated intelligence products, thereby significantly reducing the overlap and duplication currently typical of intelligence organizations.

Another component critical for increasing the likelihood of success of such a transformation is a command model that differs from the classical, hierarchic model that views the change as a process to be initiated primarily from above. The new model must also allow for managed chaos, while adopting and embracing the younger generation joining the intelligence community as leaders of change. Members of this generation started communicating on social networks long before their recruitment. They need only be allowed to maintain their habits of sharing their environment, to be reinforced without becoming entrenched, and to be granted the tools to which they are accustomed for the sake of sharing and creating knowledge. All of this must, of course, occur in the context of a dialogue between the networked command model and the classical model, in order to find the golden mean between the need for innovation from below and the necessity of segregating those areas of production where the allocation of responsibility and authorization of intelligence products are essential principles.

The organizational and institutional fear of incorporating social media as a way of communicating and creating knowledge is understandable, but it is liable to be the major hindrance to creating networked, cross-organizational intelligence communities. Efforts to limit the ways in which individuals in the community can contact one another will not succeed; individuals will simply turn to the civilian social media to do so, and the intelligence network will remain secondary at best and duplicate processes at worst. Importing social media into the intelligence community will generate the Intelligence 2.0 revolution and enable the entire intelligence endeavor to take a giant stride forward.

Notes

[1] This essay was first written and distributed within IDF Military Intelligence in 2012. Since then, as part of a fundamental organizational and conceptual change spearheaded by the head of IMI, some of the core concepts articulated herein have already been applied. The authors would like to thank Gur A. and Tal G. for their significant contribution to the learning process that was the framework for this essay.

[2] Chaim Herzog, cited by Zehava Ostfeld, *An Army Is Born* (Tel Aviv: Ministry of Defense Publishing House, 1994), p. 333.

[3] Israel Military Intelligence, *The Process of Intelligence Work*, IDF Archives, 1956. A copy of the booklet is preserved at the Institute for the Study of Intelligence at MI and kept at Training Base 15.

[4] See the full report of the Agranat Commission investigating the Yom Kippur War at the IDF Archives site, pp. 160 and 168, http://www.archives.mod.gov.il/.

[5] Kristian J. Wheaton. "Let's Kill the Intelligence Cycle," *Sources and Methods*, May 20, 2011, http://sourcesandmethods.blogspot.com/2011/05/lets-kill-intelligence-cycle-original.html.

[6] Shani Avnet, "Empowering Information Portals through User Experience," Netwise Ltd. The PowerPoint presentation is available at http://api.ning.com/files/x6R-TdDcUc0aH8798ORM5OWlq3G5G-1lnmXkOaf1WI8dFFg7BwS1RyyeiOuO7tCvYtSUlTTqOn2M-kjH8EJ5cGbX6OI1A2rt/file.pdf.

[7] *TIME Magazine*, December 25, 2006, http://www.time.com/time/magazine/article/0,9171,1570810,00.html.

[8] Alvin Toffler, *The Third Wave* (William Morrow, 1980); see also Alvin and Heidi Toffler, *Revolutionary Wealth* (New York: Doubleday, 2006).

9 Shmuel Even and Amos Granit, *The Israeli Intelligence Community: Where To?* Memorandum No. 97 (Tel Aviv: Institute for National Security Studies, 2009), p. 47.

10 D. Calvin Andrus, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," *Studies in Intelligence* 49, no. 3 (September 2005): 63-70, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904.

11 A social intelligence network was constructed in MI about two years ago and is being used by thousands of intelligence personnel – collectors and analysts – as a central system for intelligence production.

12 David Schroeder, "Efficacy and Adoption of Central Web 2.0 and Social Software Tools in the U.S. Intelligence Community," American Public University System, March 2011, http://www.academia.edu/1443504/Efficacy_and_Adoption_of_Central_Web_2.0_and_Social_Software_Tools_in_the_U.S._Intelligence_Community.

13 Ibid., p. 2.

14 Chris Rasmussen, "Toward Living Intelligence," Gov 2.0 Expo Showcase, Washington D.C., September 8, 2009, http://www.gov2expo.com/gov2expo2009/public/schedule/detail/10599. See also the YouTube video at http://www.youtube.com/watch?v=XdQPuTVDOH4.

Is Might Right?
Boko Haram, the Joint Military Task Force, and the Global Jihad

Daniel E. Agbiboa

In this paper, I critically examine the ongoing religious terrorism of Boko Haram in northern Nigeria, focusing on why the group exists and its growing connection to the global jihad. I evaluate the coercive and conciliatory responses of the Nigerian government to Boko Haram, with particular reference to the Joint Military Task Force. Problematizing a security-only, killing approach to dealing with religious terrorism, I argue that countries fighting terror abroad should learn from the Nigerian experience of fighting Boko Haram that the war on terror begets a vicious cycle of terror and war without end.

Key words: Boko Haram; religious terrorism; Northern Nigeria; global jihad; carrot and stick; joint military task force; non-killing

Introduction

This paper is about the current religious terrorism of a radical Islamist group from northeastern Nigeria that officially calls itself Jama'atu Ahlus-Sunnah Lidda'Awati Wal Jihad, meaning "People Committed to the Prophet's Teachings for Propagation and Jihad." However, the group has become known by the name given to it by locals: Boko Haram (BH), which in the Hausa language means "Western education is unlawful." Since its founding in 2002, BH has claimed over 10,000 lives, leaving millions in Nigeria gripped by fear.[1] The group's ultimate goal is to create an Islamic state governed by the supreme law of *sharia*.[2] Unfortunately, attempts

Daniel E. Agbiboa is a Queen Elizabeth House (QEH) Doctoral Scholar at the Department of International Development, University of Oxford, UK.

at negotiating with BH, including the recent amnesty offer extended to its members, have stalled because of distrust on both sides and the factionalized leadership of the group's different cells.

In this paper, I critically examine the problem of BH in northern Nigeria, focusing on why the group exists and its growing connection to the global jihad of transnational terrorist groups like al-Qaeda in the Islamic Maghreb and the Somali-based al-Shabaab. I evaluate the coercive and conciliatory responses of the Nigerian government to the BH security threat, with particular reference to the special Joint Military Task Force (JTF) and its current offensive strategy against the jihadist group. Problematizing a security-only approach to dealing with religious terrorism, I argue that countries fighting terror should learn from the Nigerian experience of fighting BH that the war on terror only begets a vicious cycle of terror and war without end.

Theoretical Framework: Confronting Terrorism

There is no standard definition of terrorism, as illustrated by Alex Schmid's finding of over 100 different uses of the term.[3] However, most definitions contain some common features. Terrorism, including politically or religiously motivated violence, is: (a) intimidatory in intent; (b) aiming to generate fear in a wider audience, and (c) pursued chiefly through the use of violence or psychological weaponry.[4] In this article, terrorism will be defined in accordance with the 1999 Algiers Convention as an act "calculated or intended to: intimidate, put in fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or create general insurrection in a State."[5] Conceived in this way, acts of terrorism can be carried out by states, state actors, non-state actors, groups, or individuals in the pursuit of specific objectives or valued ideals. This definition is especially relevant in the Nigerian context, where the government is inclined to use terror against its own populations.

With regard to how states can deal with terrorist groups, two competing counter-terrorism approaches may be gleaned from existing literature: coercion and conciliation. The crux of the debate is whether states should use harsh policies to punish terrorists and thus deter future acts, or focus on root causes and reduce incentives to use terrorism.[6] Phrased alternatively: Do coercive policies deter terrorism, or do they create a vicious cycle of violence? This question, on which there is little consensus, was brought to the fore after the 9/11 attacks.[7] A coercive approach includes the use of physical force by governments to injure or kill terrorists or their supporters. This approach extends to state terror, assassination, missile strikes, and invasion. Many states subscribe to this coercive approach, which explains Israel's reprisal policy and the United States' global war on terror.[8] The logic of coercion assumes that the tactic of retaliation against terrorists will discourage future acts. Conversely, states that fail to respond aggressively, or that concede to terrorist demands, acquire a reputation for being soft, thus encouraging terrorists.[9]

In contrast, a conciliatory approach holds that states should address the root causes of terrorism, thereby decreasing the legitimacy of the terrorist's claims and the traction for its cause. States use conciliation to resolve a crisis or to forestall future crises by negotiating with terrorists.[10] Examples of concessions include social reform, the release of prisoners, or negotiation with a state sponsor. Although critics view concessions as capitulation to terrorist demands, this approach in fact includes attempts to persuade groups and their supporters to relinquish terrorism by promising change.[11] Opponents of a coercive approach argue that it not only fails to deter terrorism, it actually increases opposition to the government and leads to cycles of violence. Northern Ireland, Israel, and Chechnya illustrate government behavior that not only failed to stop terrorism but actually prolonged violence.[12] Opponents also point to the offensive strategy pursued by the Bush administration in the US, which has too often been "counterproductive and self-defeating,"[13] jeopardizing international cooperation in the fight against terrorism and providing ammunition for terrorist recruitment in the Middle East and beyond.

Drawing on the conciliation approach, I argue against a security-only strategy of killing by demonstrating that more killing results in more terrorism. Deterrence is not effective against terrorists who are prepared to sacrifice their lives. Specifically, I argue that countries fighting terror abroad, such as the US, the UK, and France, should learn from the Nigerian experience of fighting BH that the war on terror only begets a vicious cycle of terror and spiraling violence with no end in sight. Reliance on hard power to fight religious terrorism misunderstands the nature of the violence and makes the threat considerably worse. I argue instead for a non-killing approach that identifies the motivations and grievances of terrorist groups and seeks to meaningfully address them.

A non-killing approach includes the concepts of peace (absence of war and conditions conducive to war), nonviolence (psychological, physical, and structural), and ahimsa (non-injury in thought, word, and deed).[14] The sustainability of a non-killing approach is supported by Glenn Paige's ground-breaking non-killing thesis, which cogently demonstrates that less than 0.5 percent of all humans who ever existed actually killed other humans.[15] Paige defines a non-killing society as "a human community, smallest to largest, local to global, characterized by no killing of humans and no threats to kill; no weapons designed to kill humans and no justifications for using them; and no conditions of society dependent upon threat or use of killing force for maintenance or change."[16] The crux of Paige's argument is that extant structures of society do not require lethality as a necessary condition for change or maintenance. This contention is put forward as a challenge and superior alternative to the time-honored belief that lethality is ineluctable in human relations – a belief that continues to (mis)inform the global war on terror.

Radical Islamism, which this paper directly addresses, is a by-product of a number of historical developments, including the social, political, and economic dysfunctionalities of Muslim societies that have blocked these nations from satisfactory development. The shortcomings of these societies created an aperture for extremists to exploit a sense of civilizational humiliation with a re-reading of Islamic history and doctrine that blames and abhors the West. As I will explain later with the case of BH, part of the problem is that jihadist groups are infusing religion into a long-churning brew of grievances about corruption, repression, injustice, and unfair distribution of wealth and power. As Daniel Benjamin argues, "In most Muslim countries there is a genuine rage at appalling governance and corruption – a central grievance of jihadists, who speak of the 'apostate' rulers, thus translating the anger into a religious idiom."[17]

A security-only military strategy typically leads to benefits for radical Islamists. They gain critical experience in tactics and create new networks of support as well as social bonds among disparate groups that enable future collaboration. This strategy also gives them opportunities to raise funds and acquire weapons and other accoutrements. Moreover, the use of military force as a counterterrorism strategy is frequently ill-advised because it is inevitably indiscriminate and often results in the alienation of precisely those individuals in a given community whom we do not want radicalized. Furthermore, military action against terrorist targets frequently results in the death of innocent people, no matter how much care is taken. The foregoing will become more evident when we consider the non-moderated and unaccountable military response to BH terrorism – a response that has caused more harm than good in Nigeria.

Understanding Religious Terrorism

The nexus between religion and terrorism has a long genealogy in Western scholarship. The concept of religious terrorism goes back to David Rapoport's paper[18] analyzing the use of terror in the three monotheistic religions. This seminal paper inspired many similar works that sought to explain "why violence and religion have re-emerged so dramatically at this moment in history and why they have so frequently been found in combination."[19] As Scott Appleby puts it: Why does religion seem to need violence, and violence religion?[20] In this strand of literature, religious terrorism has been raised above a simple label to a set of descriptive characteristics and substantive claims that appear to delineate it as a specific "type" of political violence, fundamentally different from previous or other forms of terrorism.[21]

The claim about the special nature of religious terrorism rests on a number of key hypotheses (H), three of which are succinctly depicted in figure 1.

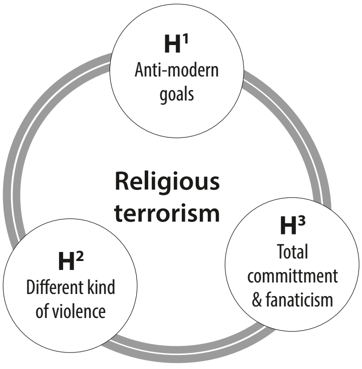


Figure 1. Three Hypotheses of Religious Terrorism

H^1: Religious terrorists have anti-modern goals of returning society to an idealized version of the past and are therefore necessarily anti-democratic and anti-progressive.

Audrey Cronin, for example, argues that "the forces of history seem to be driving international terrorism back to a much earlier time, with echoes of the behavior of 'sacred' terrorists... clearly apparent in the terrorist organization such as al-Qaeda."[22] For his part, Mark Juergensmeyer contends that religious terrorists work to "an anti-modern political agenda."[23] It is further argued that religious terrorists have objectives that are absolutist, inflexible, unrealistic, devoid of political pragmatism, and hostile to negotiation.[24] In his excellent article titled "The Origins of the New Terrorism," Matthew Morgan charges, "Today's terrorists don't want a seat at the table; they want to destroy the table and everyone sitting at it."[25] Daniel L. Byman notes of al-Qaeda, "Because of the scope of its grievances, its broader agenda of rectifying humiliation and a poisoned worldview that glorifies jihad as a solution, appeasing al-Qaeda is difficult in theory and impossible in practice."[26] This view is supported by Daniel Benjamin who argues that unlike most terrorist groups, al-Qaeda "eschews incremental gains and seeks no part of a negotiation process; it seeks to achieve its primary ends, including mobilization of a large number of Muslims, through violence."[27]

H^2: Religious terrorists employ a different kind of violence from that of their secular counterparts.

It is argued that for the religious terrorist, "violence is... a sacramental act or divine duty executed in direct response to some theological demand,"[28] as opposed to a tactical means to a political end. Furthermore, some have suggested that because religious terrorists have transcendental aims, are engaged in a cosmic war, and lack an earthly constituency, they are not constrained in their pedagogy of violence and take an apocalyptic view of violent confrontation: "What makes religious violence particularly savage and relentless is that its perpetrators have placed such religious images of divine struggle – cosmic war – in the service of worldly political battles."[29] For this reason, acts of religious terror serve not only as tactics in a political struggle, but also as evocations of a much larger spiritual confrontation. Thus, religious terrorists aim for maximum causalities and are willing to use weapons of mass destruction.[30] As Magnus Ranstorp puts it, they are "relatively unconstrained in the lethality and the indiscriminate nature of violence used [because they lack] any moral constraints in the use of violence."[31]

H^3: Religious terrorists have the capacity to evoke total commitment and fanaticism from their members.

It is argued that religious terrorists are characterized by the suspension of doubt and an end-justifies-the-means *weltanschuung* (worldview) – in contrast to the supposedly more measured attitudes of secular groups.[32] Mark Juergensmeyer argues that "these disturbing displays have been accompanied by strong claims of moral justification and an enduring absolutism, characterized by the intensity of the religious activists' commitment."[33] Moreover, it is suggested that in some cases the certainties of the religious viewpoint and the promises of the next world are primary motivating factors in driving insecure, alienated, and marginalized youths to join religious terrorist groups as a means of psychological empowerment. It is further argued that such impressionable, alienated, and disempowered young people are vulnerable to forms of brainwashing and undue influence by recruiters, extremist preachers, or internet materials.[34]

In the following paragraphs, I draw on the foregoing hypotheses of religious terrorism to explain BH's campaign of violence in Nigeria.

Religious Terrorism: Boko Haram – A Case Study

> We want to reiterate that we are warriors who are carrying out Jihad (religious war) in Nigeria and our struggle is based on the traditions of the holy prophet. We will never accept any system of government apart from the one stipulated by Islam because that is the only way that the Muslims can be liberated... We do not believe in the Nigerian judicial system and we will fight anyone who assists the government in perpetrating illegalities.[35]

Mohammed Yusuf, born on January 29, 1970, in the village of Girgir in Yobe State, Nigeria, founded BH in 2002 with the goal of establishing a *sharia* government in northern Nigeria's Borno state. Yusuf established a religious complex in his hometown that included a mosque and a school where many poor families from across Nigeria and from neighboring countries enrolled their children. However, the center had ulterior political goals, and soon it was also serving as a recruiting ground for future jihadists to fight the state. BH found support among the impoverished and alienated northern population, many of whom were attracted by the group's condemnation of the corrupt and apostate ruling elites in Nigeria.[36] The group includes members from neighboring Chad and Niger who speak only Arabic. BH has been able to attract more than 280,000 members across northern Nigeria as well as Chad and the Republic of Niger.[37]

BH's ideology is embedded in radical Salafism – a minority trend within Islam that dates back to the ninth century and whose main features were crystallized in the teachings of a fourteenth-century Islamic scholar, Taqi al-Din Ahmad Ibn Taymiyya (d. 1328). The hallmark of Salafism is a call to modern Muslims to return to the pure Islam of the Prophet Muhammad's generation and the two generations that followed. Muslims of this early period are called al-Salaf al-Salih (the pious forefathers), whence the name Salafi. BH's ideology is durable and has, for some Muslims, a compelling authenticity because of its appropriation of canonic Islamic texts. For example, BH adherents are reportedly influenced by the Qur'anic phrase evoking fanaticism and total commitment (see H^3): "Anyone who is not governed by what Allah has revealed is among the transgressors."[38] Group members view it as their necessary duty and goal to engage in a violent struggle against perceived enemies of Islam, both at home and abroad. Its members see the overthrow of secular governments as justified because their rulers are viewed as accepting or leaning toward the ways of Islam's enemies.

As the name suggests, BH is vehemently opposed to what it sees as a Western-based incursion that erodes traditional customs and values among Muslim communities in northern Nigeria. The group's first leader, Mohammed Yusuf, told the BBC in 2009, "Western-style education is mixed with issues that run contrary to our beliefs in Islam."[39] Elsewhere, the charismatic leader argued, "Our land was an Islamic state before the colonial masters turned it to a *kafir* [infidel] land. The current system is contrary to true Islamic beliefs."[40] Thus, BH clearly reveals itself as a group with the anti-modern goals of returning society to an idealized version of the past (see H^1).

BH became an ultra-radical group in 2009 following confrontations between the Islamist group and the state's security agency in Bauchi State, which was mandated to enforce a newly introduced law requiring motorcyclists in the entire country to wear safety helmets. The violent confrontation was triggered by a BH funeral procession in Maiduguri during which BH mourners reneged on the helmet law. Members of an anti-robbery task force, made up of the police and army, opened fire on the BH mourners, killing 17 members in the process. Mohammed Yusuf demanded justice, but "the authorities neither investigated the alleged excessive use of force nor apologized for the shooting."[41] On July 21, the group's hideout in Bauchi was also ransacked by state security forces and materials for making explosives were confiscated.

Following this crackdown, the Islamist group mobilized its members for reprisal attacks. On July 26, BH members burned down a police station in Dutsen Tanshi, on the outskirts of Bauchi, resulting in the death of five Boko Haram members and severe injury to several police officers. In response, the military and police raided a mosque and home in Bauchi where BH members had regrouped, killing dozens of the group's members. The police reported that 52 BH members, two police officers, and a solider were killed in the violence in Bauchi. Yusuf vowed revenge, saying he was prepared to fight to the death in retaliation for the killing of his followers. True to his promise, the BH leader mobilized his followers for coordinated attacks across Maiduguri, attacking the police stations and homes of police officers, including retired ones. They torched churches and raided the main prison – freeing inmates and killing prison guards.

In response, on July 28, Yusuf's compound was shelled by the Nigerian army and many of his followers were arrested, with at least several dozen killed in police custody.[42] On July 29, in Postiskum, state security forces also raided the group's hideout on the outskirts of the town, killing at least 43 of Yusuf's followers. The riot was temporarily quelled after Nigerian forces captured and killed Mohammed Yusuf and roughly 1,000 of his followers. Yusuf's death and the bloodshed of BH's members drove the movement to transform itself into a network of underground cells with a hidden leadership – a situation that today makes any military solution illusory.[43] The movement went dormant for a year before reemerging in 2010 with increasingly sophisticated attacks that were purportedly connected to the growing foreign support of global jihadist groups like al-Qaeda in the Islamic Maghreb and the Somali-based al-Shabaab, as well as the al-Muntada Trust Fund and the Islamic World Society. Far from eliminating the threat of BH, the resort to violence on the part of the Nigerian government ultimately radicalized the Islamist group and drove its leaders to forge ties with the global jihadist movement as a survival strategy.

BH's modus operandi has involved the use of suicide bombing and gunmen on motorbikes, killing police, politicians, and anyone who criticizes it, including Muslim clerics who disclose information of their whereabouts to state security services. In 2012, BH launched several attacks against police officers, demanding the release of all its prisoners and the prosecution of those responsible for the killing of its founder.[44] In June and August 2011, BH terrorists bombed the Nigerian police headquarters and the UN Headquarters, both located in Nigeria's capital, Abuja. During the first ten months of 2012 alone, more than 900 people died in attacks by BH – more than in 2010 and 2011 combined.[45]

On July 6, 2013, a group of alleged BH Islamists stormed a boarding school in Yobe State, northeastern Nigeria, burning 29 students and one teacher alive.[46] Following the horrific murder, Abubakar Shekau, the current BH leader, released a 15-minute video calling for more such attacks. Confirming BH's anti-democratic and anti-progressive stance (see H^1), Shekau unequivocally stated in the video, "The Quran teaches that we must shun democracy, we must shun the constitution, [and] we must shun Western education." In the latest bloodbath in Borno state, a group of BH Islamists are believed to have assassinated 44 people while praying in a mosque. The foregoing attests to the indiscriminate nature of violence used by BH and the lack of any moral constraint (see H^2).

Boko Haram and the Global Jihad

One of BH's major ambitions is to become a key player in the global jihad, which is being fought by transnational terrorist groups like the Islamic Maghreb's al-Qaeda, its affiliates in Mali and the entire Sahel, and Somali-based al-Shabaab. The rapidly growing Muslim populations of Africa have been targeted by jihadist groups for recruitment, and parts of the Sahel have become a safe haven for the radicals of the Maghreb. It will not be surprising if Boko Haram's intentions are to exploit conflicted areas and join the *mujahedin* (warriors of the jihad) in foreign and Arab countries like Chechnya and Afghanistan. Members of BH are known to have received training with the Somali-based al-Shabaab. BH members have also fought in Mali alongside groups affiliated with al-Qaeda, and it would be a major threat to the Egyptian regime and to Israel if they joined jihadist groups in the Sinai Peninsula.

BH has also expanded its propaganda efforts to demonstrate solidarity with al-Qaeda and its affiliates. In July 2010, current BH leader Abubakar Shekau released an online statement praising al-Qaeda and offering condolences to al-Qaeda of Iraq for its loss of Abu Ayyub al Masri and Abu Omar al Baghadadi, two top al-Qaeda operatives in Iraq. In another video released in November 2012, Shekau expressed his full support for the jihad being fought in Afghanistan, Pakistan, Kashmir, Chechnya, Iraq, Saudi Arabia, Yemen, Somalia, Algeria, Libya, and Mali. In the video, Shekau delivered his speech in Arabic, which gives the impression that he is appealing to the leaders of al-Qaeda and the wider jihadist family. In the 39-minute video, Shekau repeatedly calls the jihadist fighters "brothers."[47] In August 2011, General Carter Ham, Commander of the US Africa Command (AFRICOM), claimed that al-Qaeda and al-Shabaab are financing BH, and that both global jihadist terrorist groups shared training and fighters with BH. He described this as "the most dangerous thing to happen not only to the Africans, but to us as well."[48] In November of that year, Algerian Deputy Foreign Minister Abdelkader Messahel said he had "no doubts that coordination exists between Boko Haram and al-Qaeda," citing intelligence reports and common operating methods.[49]

A major shift in BH's ideology and strategic goals can be seen in the 2011 suicide car bombing of the UN building of Abuja. This was the first time that BH attacked a distinctly non-Nigerian target, following the al-Qaeda attacks of UN targets in Algeria and the al-Shabaab UN attacks in Somalia.[50] On November 24, 2012, a BH spokesman, Abul Qaqa, confirmed what many had long suspected: "It is true that we have links with al-Qaeda. They assist us and we assist them."[51] Boko Haram has also confirmed links in Somalia. According to a statement allegedly released by the group, "very soon, we will wage jihad... We want to make it known that our jihadists have arrived in Nigeria from Somalia where they received real training in warfare from our brethren who made that country ungovernable... This time round, our attacks will be fiercer and wider than they have been."[52] BH has since increased its suicide operations, with at least 19 suicide bomb attacks on various local targets in Nigeria, including churches, mosques, beer parlors, newspaper offices, government officials, and security forces.[53]

In 2012, the US State Department added BH's most visible leader, Abubakar Shekau, to the list of specially designated global terrorists. Recently, the US announced a $7 million bounty for the capture of Shekau, placing him in the top echelon of wanted jihadist leaders.[54] Four other al-Qaeda leaders in Africa were also included in the "Rewards for Justice" list. The US State Department noted that that BH and al-Qaeda's affiliate in Yemen and Saudi Arabia are cooperating to "strengthen Boko Haram's capacity to conduct terrorist attacks."[55] If Boko Haram decides to enhance its global activity beyond the boundaries of Nigeria, it will pose a serious threat to the jihadist targets. The Sinai Peninsula as well as the Syrian battlefield could well be a concern for the neighboring countries.

State Responses

Jeffrey Seul once argued that "religion is not the cause of religious conflict; rather for many... it frequently supplies the fault line along which intergroup identity and resource competition occurs."[56] In line with this perspective, it has been argued that the stark polarization in Nigeria – 75 per cent of northerners live in poverty, compared with 27 per cent of those in the Christian south – is a factor behind local insurrections such as that of Boko Haram. According to a recent report on northern Nigeria by Human Rights Watch, unemployment, lack of economic opportunities, and inequalities of wealth are a source of deep frustration in parts of the Muslim north.[57] The extent of relative deprivation in northern Nigeria has led several analysts to argue that "religious dimensions of the conflict have been misconstrued as the primary driver of violence when, in fact, disenfranchisement and inequality are the root causes."[58]

While acknowledging the skillful way in which BH has exploited the extant circumstances of relative deprivation and political grievance in northern Nigeria to promote its vision of turning Nigeria into an Islamic state governed by *sharia*, I argue that the ultra-violent turn BH took should also be traced back to the extrajudicial killing of its leader, Mohammed Yusuf, and the ongoing arbitrary arrest, torture, and killing of its members by state security forces. Until 2009 BH was seen as radical but not ultra-violent.[59] The killing of the group's founder under police custody provoked a staunch reaction from BH members who primarily want to settle their scores with the police and army.[60] In a video that was released in June 2010, Abubakar Shekau – the group's current leader – vowed to avenge the deaths of its members. In a typical Al-Qaeda-style video, Shekau warned, "Do not think Jihad is over: Rather Jihad has just begun."[61] It is no coincidence that between January and September 2012, at least 119 police officers lost their lives in suspected BH attacks, more than in 2010 and 2011 combined.[62]

How has the Nigerian state responded to BH? Two major approaches may be identified: conciliatory and coercive. The former – a rare approach by the Nigerian government – involves political negotiation with all stakeholders in the BH conflict. At the state level, applications of the carrot approach have been few and far between, involving overtures and rapprochements to BH insurgents. In the most recent and noteworthy attempt to negotiate with BH, President Jonathan established a 26-member amnesty-oriented body, the Committee on Dialogue and Peaceful Resolution of Security Challenges in the North. The committee, comprising former and current government officials, religious authorities, and human rights activists, was given a three-month mandate to try to convince BH members to lay down their arms in exchange for a state pardon and social integration.[63] However, BH's supreme leader, Abubakar Shekau, responded to the amnesty entreaties of the Nigerian government by saying that his group has not committed any wrong, and that amnesty would not be applicable to them. Rather, Shekau argued, the Nigerian government was committing atrocities against Muslims. In his words: "Surprisingly, the Nigerian government is talking about granting us amnesty. What wrong have we done? On the contrary, it is we that should grant you [a] pardon."[64] Shekau vowed not to stop his group's jihad to establish Islamic state in Nigeria under a strict form of *sharia* law.[65]

True to his avowal, less than a week after BH rejected Nigeria's amnesty offer, the jihadist group launched two violent back-to-back attacks in northern Nigeria. In the first attack, BH fighters laid siege to the town of Bama in Borno State, killing 55 people, mostly police and security forces, and freeing over 100 prison inmates. Days later, BH killed 53 people and burnt down 13 villages in central Nigeria's Benue State.[66] In the wake of these violent attacks, President Jonathan declared a state of emergency in three northern states where BH has been most active – Borno, Adamawa and Yobe – in an attempt to restore order and reclaim control of the territories taken over by the radical group.[67] According to Jonathan, "What we are facing is not just militancy or criminality, but a rebellion and insurgency by terrorist groups which pose a very serious threat to national unity and territorial integrity."[68] The president vowed to "take all necessary action... to put an end to the impunity of insurgents and terrorists."[69] To this end, the Nigerian government established a special Joint Military Task Force (JTF), known as "Operation Restore Order," to mount an aggressive pursuit of and crackdown on BH members and major hideouts.

It is important to note that this is not the first time the Nigerian government has declared a state of emergency as a result of BH attacks. Following a string of BH bombings across northern Nigeria in late 2011, President Jonathan declared a state of emergency, suspending constitutional guarantees in 15 areas within four northern states. The state of emergency, however, failed spectacularly to stem the tide of violent attacks in the restive region. Nor did coercive regulation issued in April 2012, granting security forces emergency powers to crush the BH threat, succeed in this regard. In fact, during the six months that the state of emergency was in effect, BH carried out more attacks and killed more people than in 2010 and 2011 combined.[70] The preference for a military solution to BH is hardly surprising if we recall the words of the late Nigerian political scientist, Professor Claude Ake: "More often than not, the postcolonial state in Nigeria presented itself as an apparatus of violence, and while its base in social forces remained extremely narrow it relied unduly on coercion for compliance, rather than authority."[71]

In Nigeria's largest military deployment since the 1967-70 Civil War, the federal government ordered some 8,000 troops to the troubled northern region in a military offensive against BH. A curfew was imposed on Maiduguri as the JTF used air strikes to target BH strongholds. A blockade was also imposed on the group's traditional base of Maiduguri in Borno State, in order to reestablish Nigeria's territorial integrity.[72] However, far too often, members of the JTF have been accused of killing innocent people in the name of policing terrorism in northern Nigeria. In Borno state, for example, JTF members have resorted to extra-legal killings, dragnet arrests, and intimidation of the hapless Bornu residents.[73] Far from conducting intelligence-driven operations, the JFT simply cordoned off areas and carried out house-to-house searches, at times shooting young men in these homes.[74] These raids have become so frequent that parents have advised their sons to flee as soon as they hear of an attack.

In a series of probing interviews with residents of Maiduguri, Human Rights Watch reported: "During raids into communities soldiers have set fire to houses, shops, and cars, randomly arrested men from the neighborhood, and in some cases executed them in front of their shops or houses."[75] During recent crossfire between members of the JTF and BH fighters in Baga, near Nigeria's border with Cameroon, up to 187 people were killed and another 77 were injured. But Baga residents have accused the JTF, not BH, of firing indiscriminately at civilians and setting fire to much of the historical fishing town.[76] The Nigerian authorities rarely brought anyone to justice for these crimes against civilians. One of the problems of using the military and the police in northern Nigeria is that they are national – not local – forces and are therefore unlikely to share ethnic and cultural backgrounds with the local population. Recently, US Secretary of State John Kerry issued a strongly worded statement saying, "We are... deeply concerned by credible allegations that Nigerian security forces are committing gross human rights violations, which, in turn, only escalate the violence and fuel extremism."[77] Yet the US is in no credible position to be "deeply concerned" about the use of violence and human rights violations in Nigeria because the US continues to apply a similar strategy in its global war on terror in the Middle East and beyond.[78]

I argue that countries fighting terror abroad, such as the US, the UK, and France, should learn from the Nigerian experience of fighting BH that the war on terror is a war without end, which only begets a vicious cycle of terror. A security-only military approach to fighting terrorism not only precludes democratic culture and attitudes, but further radicalizes the religious terrorist group and strengthens the collective resolve of its members, who are unlikely to compromise (which means betraying their faith). Likewise, threats of violence or prison are rarely an effective deterrent. According to a recent statement by BH leader Abubakar Shekau, "Since we started this ongoing war, which they call state of emergency... in some instances soldiers who faced us turned and ran."[79] Shekau's claims that BH has gained the upper hand in the war contradict the one-sided claim by the Nigerian government that the JTF is winning the war on terror.

In the final analysis, countries fighting terrorism must learn that a declared war on terror has only a limited capacity to make a real difference because "[it] can never address the underlying conditions that can shape those [like BH] who reject the prevailing order and develop radical positions, or opt to use violence in the first place."[80] The global war on terror is likely to achieve a pyrrhic victory that will further undermine governmental authority, embolden the mobilization and spread of radical jihadist groups in Africa, and ultimately force the problem underground to emerge stronger at a later time, as the BH case has demonstrated. What Nigeria has lacked since independence is a viable concept of strategic counterterrorism – a doctrine that will guide our actions, help undermine the recruitment of terrorists, and change the environment they inhabit into an increasingly non-permissive one. An effective counterterrorism policy in Nigeria must go beyond a security-only killing strategy to embed counterterrorism in an overarching national security strategy that appreciates the broader context in which Islamist radicalization occurs and seeks to meaningfully and non-violently alter it. In other words, Nigeria must shift away from a security policy that makes counterterrorism the prism through which everything is evaluated and decided.

A long term strategy that will make Muslim societies less able to serve as incubators of radicalism and will undercut the jihadist appeal must use force sparingly and responsibly. It must aim to address fundamental human needs by incorporating development, security, and respect for human rights. Poverty and unemployment in the Muslim north, coupled with the population's increase and the government's inability to deal effectively with non-state groups, can turn northern states into an ideal recruitment ground for global jihadist groups like al-Qaeda and al-Shabaab. Finally, there is a need for an intelligence-led strategy to better confront BH's localized terrorist activities and global aspirations. In addition, there is a necessity for greater international cooperation in order to identify and intersect BH's ever-increasing external funding and weapons sources as well as the training that is crucial to the group's operational capabilities.

Notes

[1] Daniel E. Agbiboa, "Living in Fear: Religious Identity, Relative Deprivation, and the Boko Haram Terrorism," *African Security* 6, no. 2 (2013): 153-70; Daniel E. Agbiboa, "The Ongoing Campaign of Terror in Nigeria: Boko Haram versus the State," *Stability: International Journal of Security and Development* 2, no. 3 (2013): 1-18.

[2] Human Rights Watch, "Spiraling Violence: Boko Haram Attacks and Security Forces Abuses in Nigeria," October 4, 2013, http://www.hrw.org/sites/default/files/reports/nigeria1012webwcover.pdf.

[3] Alex Schmid, *Political Terrorism: A Research Guide to Concepts, Theories, Data Bases, and Literature* (Amsterdam: North-Holland, 1983), pp. 70-111.

4 R. F. Young, "Revolutionary Terrorism, Crime and Morality," *Social Theory and Practice* 4, no. 3 (1977): 288.

5 1999 OAU Convention on the Prevention and Combating of Terrorism, Article 1, cited in Daniel E. Agbiboa, "(Sp)oiling Domestic Terrorism? Boko Haram and State Response," *Peace Review: A Journal of Social Justice* 25, no. 3 (2013): 431-32.

6 Gregory D. Miller, "Confronting Terrorisms: Group Motivation and Successful State Policies," *Terrorism and Political Violence* 19 (2007): 332-33.

7 Human Rights Watch, "Spiraling Violence."

8 William O'Brien, "Israel's Counterterror Strategies, 1967-1987," *Middle East Review* 20 (1987): 23-30; Reuben Miller, "Responding to Terrorism's Challenge: The Case of Israeli Reprisals," *Virginia Social Science Journal* 25 (1990): 109-23.

9 Ibid.

10 Reuben Miller, "Responding to Terrorism's Challenge."

11 Daniel Benjamin, "Strategic Counterterrorism," *Foreign Policy at Brookings*, Policy Paper 7, October 2008, pp. 1-17.

12 Gregory Miller, "Confronting Terrorisms."

13 Ibid.

14 Ada Aharoni, "Nonkilling Global Society," in *Peace Building*, ed. Ada Aharoni (Oxford: UNESCO and Eolss Publishers, 2005).

15 Glenn D. Paige, *Nonkilling Global Political Science* (Honolulu, Hawaii: Center for Global Nonkilling, 2009), p. 1.

16 Ibid.

17 Benjamin, "Strategic Counterterrorism," p. 7.

18 David Rapoport, "Fear and Trembling: Terrorism in Three Religious Traditions," *American Political Science Review* 78, no. 3 (1984): 658-77.

19 Mark Juergensmeyer, *Terror in the Mind of God: The Global Rise of Religious Violence* (Berkeley: University of California Press, 2003), p. 121.

20 Scott R. Appleby, *The Ambivalence of the Sacred: Religion, Violence and Reconciliation* (New York: Littlefield, 2001), p. 7.

21 Bruce Hoffman, *Inside Terrorism* (New York: Columbia University, 2006), pp. 88, 272.

22 Audrey Cronin, "Behind the Curve: Globalisation and International Terrorism," *International Security* 27, no. 3 (2003), p. 38.

23 Juergensmeyer, *Terror in the Mind of God*, p. 230.

24 Jeroen Gunning and Richard Jackson, "What's So 'Religious' about 'Religious Terrorism?'" *Critical Studies on Terrorism* 4, no. 3 (2011): 369-88.

25 Matthew Morgan, "The Origins of the New Terrorism," *Parameters* 34, no. 1 (2004): 30-31.

26 Daniel L. Byman, "Al-Qaeda as an Adversary: Do We Understand our Enemy?" *World Politics* 56, no. 1 (2003): 147.

27 Benjamin, "Strategic Terrorism," p. 2.

28 Hoffman, *Inside Terrorism*, p. 88.

29 Juergensmeyer, *Terror in the Mind of God*, pp. 149-150.

30 Gunning and Jackson, "What's So 'Religious' about 'Religious Terrorism?'"

31 Magnus Ranstorp, "Terrorism in the Name of Religion," *Journal of International Affairs* 50, no. 1 (1996): 54.

32 Gunning and Jackson, "What's So 'Religious' about 'Religious Terrorism?'"

33 Juergensmeyer, *Terror in the Mind of God,* p. 220.

34 Hoffman, *Inside Terrorism*, pp. 197-228, 288-90.

35 *Daily Trust*, April 25, 2011.

36 John Campbell and Asch Harwood, "Nigeria's Challenge," *The Atlantic*, June 24, 2011, http://www.theatlantic.com/international/archive/2011/06/nigeria-challenge/240961/.

37 Sani Umar, *The Discourses of Salafi Radicalism and Salafi Counter-Radicalism in Nigeria: A Case-Study of Boko Haram* (Evanston, IL: Northwestern University, 2011); Daniel E. Agbiboa, "Boko Haram and the Ongoing Campaign of Terror in Northern Nigeria: The End in Sight?" *Harvard Africa Policy Journal*, July 3, 2013, http://africa.harvard.edu/apj/boko-haram-and-the-ongoing-campaign-of-terror-in-northern-nigeria-the-end-in-sight/.

38 Alex Thurston, "Threat of Militancy in Nigeria," Commentary for Carnegie Endowment for International Peace, September 1, 2011, http://carnegieendowment.org/2011/09/01threat-of-militancy-in-nigeria/4yk8.

39 "Nigeria's 'Taliban' Enigma," *BBC News Africa*, July 31, 2009, http://news.bbc.co.uk/2/hi/8172270.stm.

40 "Nigeria: Boko Haram Sect Leader Ustaz Mohammed Vows Revenge," *Daily Trust*, July 27, 2009, http://www.nairaland.com/302352/islamists-yar-adua-want-total/6.

41 Human Rights Watch, "Spiraling Violence," p. 33.

42 Ibid.

43 Roland Marchal, "Boko Haram and the Resilience of Militant Islam in Northern Nigeria," *NOREF Report*, July 13, 2012, p. 3.

44 Daniel E. Agbiboa, "No Retreat, No Surrender: Understanding the Religious Terrorism of Boko Haram in Nigeria," *African Study Monograph* 34, no. 2 (2013): 65-84.

45 Human Rights Watch, "Spiraling Violence."

46 It would seem that the unwarranted attack on children is an attempt to weaken the education base of the north in line with the group's disdain for Western education. See Monica Mark, "Boko Haram Leader Calls for More School Attacks after Dorm Killings," *The Guardian*, July 15, 2013, http://www.guardian.co.uk/world/2013/jul/14/boko-haram-school-attacks-nigeria.

47 Bill Roggio, "Boko Haram Emir Praises al-Qaeda," *The Long War Journal*, November 30, 2012, http://www.longwarjournal.org/archives/2012/11/boko_haram_emir_prai.php.

48 "Boko Haram: Nigeria's Growing New Headache," *Strategic Comments* 17, no. 9 (2011): 1-3.

49 Ibid., pp. 2-3.

50 James J. Forest, *Confronting the Terrorism of Boko Haram in Nigeria* (Florida: The JSOU Press), p. 130.

51 Farouk Chothia, "Who Are Nigeria's Boko Haram," *BBC News Africa,* August 26, 2011, http://www.bbc.co.uk/news/world-africa-13809501.

52 Katherine Zimmerman, "From Somalia to Nigeria: Jihad," *The Weekly Standard*, June 18, 2011, http://www.weeklystandard.com/keyword/somalia.

53 Bill Roggio, "Boko Haram Suicide Bombs Kill 11 at Nigerian Military Church," *The Long War Journal*, November 25, 2012, http://www.longwarjournal.org/archives/2012/11/boko_haram_suicide_b.php.

54 Bill Roggio, "US Offers Rewards for Boko Haram, African Al-Qaeda's Leaders," *The Long War Journal*, June 4, 2013, http://www.longwarjournal.org/archives/2013/06/us_offers_rewards_fo.php.

55 Ibid.

56 Jeffrey R. Seul, "Ours Is the Way of God: Religion, Identity, and Intergroup Conflict," *Journal of Peace Research* 36, no. 5 (1999): 553.

57 Human Rights Watch, "Spiraling Violence."

58 Chris Kwaja, "Nigeria's Pernicious Drivers of Ethno-Religious Conflicts," *Africa Security Brief*, June 28, 2011, p. 1.

59 Freedom Onuoha, "Boko Haram: Nigeria's Extremist Islamic Sect," *Al Jazeera Center for Studies Report,* February 29, 2012, p. 2.

60 Marchal, "Boko Haram and the Resilience of Militant Islam," p. 2.

61 Ibid.

62 Ibid.

63 Ibid.

64 Nick Chiles, "After Rejecting Nigeria's Amnesty Offer: Boko Haram Continues to Kill," *Atlanta Blackstar*, April 23, 2013, http://atlantablackstar.com/2013/04/23/after-rejecting-nigerias-amnesty-offer-boko-haram-continues-to-kill/.

65 Ibid.

66 Ibid.

67 Agbiboa, "No Retreat, No Surrender."

68 Ibid., p. 65.

69 Ibid., p. 66.

70 Human Rights Watch, "Spiraling Violence."

71 Claude Ake, "What is the Problem of Ethnicity in Africa?" Keynote address at the Conference on Ethnicity, Society and Conflict, held in Natal, University of Natal, Pietermaritzburg Campus, South Africa. September 14-16, 1992, http://kznhass-history.net/ojs/index.php/transformation/article/viewFile/626/442.

72 Agbiboa, "No Retreat, No Surrender."

73 Human Rights Watch, "Spiraling Violence."

74 Ibid., p. 9.

75 Ibid., p. 59.

76 Chiles, "After Rejecting Nigeria's Amnesty Offer."

77 "Nigerian Forces 'Shell Fighter Camps'," *Al Jazeera*, May 17, 2013, http://www.aljazeera.com/news/africa/2013/05/20135171163037848.html.

78 See Benjamin, "Strategic Counterterrorism," p. 1.

79 "Boko Haram: We're winning war against Nigerian Army," *Press TV*, July 25, 2013. http://www.presstv.com/detail/2013/05/29/305978/boko-haram-were-winning-war-in-nigeria/

80 James Gow, Funmi Olonisakin and Ernst Dijxhoorn, "Deep History and International Security: Social Conditions and Competition, Militancy and Violence in West Africa," *Conflict, Security and Development* 13, no. 2 (2013): 240.

A Renewed, Sophisticated Containment Policy:
Mastering and Constraining War and Violent Conflict in World Society

Andreas Herberg-Rothe

Preventing Iran from attaining nuclear weapons contravenes a particular understanding of containment. However, a renewed and sophisticated containment policy understood as mastering and constraining great wars and mass violence, including combating the spread of WMD and the escalation of violent conflicts, should be the overarching political aim of the international community. The strategy of containment was successfully applied against the USSR and eventually led to the demise of that superpower. The question then arises how to adjust containment policy to make it an applicable and appropriate strategy for this globalized world.

Keywords: renewed containment, traditional containment, globalization, Clausewitz, just war theory, strategy, escalation of violence.

US President Obama has argued that traditional containment is not a reasonable policy towards Iran.[1] He emphasized that his policy is one of preventing Iran from producing a nuclear weapon, not merely containing a nuclear Iran. But in fact, by encircling China the US is pursuing a policy of traditional containment against the upcoming hegemonic power in East Asia. As the questioning of Chuck Hagel during his confirmation hearing showed, there are still some ambiguities worth mentioning concerning the strategy of the US government.[2] Perhaps these ambiguities could be systematically justified. From a different point of view, preventing Iran from obtaining a nuclear weapon is nothing less than part of a renewed

Dr. habil. Andreas Herberg-Rothe is a permanent lecturer at the Faculty of Social and Cultural Studies at the University of Applied Sciences, Fulda.

and sophisticated containment policy: the containment of the spread of weapons of mass destruction and especially nuclear bombs. Only on the basis of such a renewed containment policy, which is aimed at containing great wars, mass violence that has the same effect on societies as cancer on the human body, and weapons of mass destruction, can one reasonably deny Iran the acquisition of a nuclear bomb. As the hearings of Chuck Hagel also showed, one cannot deny Iran the rights of a member of the United Nations. But from the point of view of a renewed containment policy, it can be argued that it is necessary to prevent any additional state from acquiring nuclear weapons. The thesis in this article, therefore, is that preventing Iran from obtaining a nuclear weapon is only in conflict with a particular understanding of containment. But a renewed and sophisticated containment policy understood as mastering and constraining great wars and mass violence, including combating the spread of WMD and the escalation of violent conflicts, should be the overarching political aim of the international community.

It must be recalled that the strategy of containment was successfully applied against the USSR and eventually led to the demise of that superpower. The question then arises how to adjust containment policy to make it an applicable and appropriate strategy for this globalized world.

We are witnessing a worldwide escalation of war and violence, which should be countered by a new containment policy, just as George Kennan emphasized as early as 1987: "And for these reasons we are going to have to develop a wider concept of what containment means... a concept, in other words, more responsive to the problems of our own time...than the one I so light-heartedly brought to expression, hacking away at my typewriter there in the northwest corner of the War College building in December of 1946."[3] Sixty years have already passed since George Kennan formulated his original vision of containment. Although his original concept would be altered in application by various administrations of the US government, in practice it has been incorporated within the concept and politics of common security, which has been the essential complement to pure military containment.[4] These ideas are still valid – and as Kennan himself already pointed out, they are more in need of explication and implementation than ever. Although Kennan could not foresee them, the developments in Iraq and Afghanistan have underscored the validity of his statement, demonstrating that the aim of gaining victory over one's opponent in a traditional manner is no longer applicable in a globalized world. Instead of such strategies of the past, we need one that focuses on transforming military achievements and success into a lasting political order.

This renewed containment policy is essentially not only a double strategy, but a "pentagon" of five interconnected strategies. The overall political perspective on which the concept of containing war and violence in world society rests, consists of the following elements of what can be called the "pentagon for containing war and violence":

a. The ability to deter and discourage any opponent from fighting a large scale war and, as a last resort, to conduct pinpoint military action;
b. The possibility of using and threatening[5] military force in order to limit and contain particularly excessive, large scale violence which has the potential to destroy societies;
c. The willingness to counter phenomena that incite or fuel violence, such as poverty and oppression, especially in the economic sphere, and the recognition of a pluralism of cultures and styles of life in world society;
d. The motivation to develop a culture of civil conflict management (concepts that can be summed up with the "civilizational hexagon"[6]), global governance, and democratic peace), based on the observation that the reduction of our action to military means has proved counterproductive and will ultimately overstretch military capabilities; and
e. The restriction on the possession and proliferation of weapons of mass destruction and their delivery systems, as well as small arms, because the proliferation of both categories of weapons is inherently destructive to social order.

The Escalation of Violence and a New Containment Policy

The triumphant advance of democracy and free markets in the wake of the Soviet collapse once seemed unstoppable, to the point that it appeared for a time as if the twenty-first century would be an age defined by economics and thus, to a great extent, peace. However, these expectations were soon dashed, not only because of ongoing massacres and genocide in Sub-Saharan Africa, but also by the return of war to Europe (primarily in the former Yugoslavia), the attacks of September 11, 2001 in the US, and the Iraq war with its ongoing, violent consequences. A struggle against a new totalitarianism of an Islamic type appears to have emerged, one in which war and violence are commonly perceived as having an unavoidable role. This violence is also perceived as having become more "unbounded" than ever before – in both a spatial sense, for terrorist attacks are potentially ever-present, and a temporal sense, as no end to these attacks is in sight. One can also speak of a new dimension to violence with respect to its extent and brutality, as exemplified by the extreme violence of the ongoing civil wars in Africa. Additionally, we are facing completely new types of threats, such as the possession of weapons of mass destruction by terrorist organizations and the development of atomic bombs by "problematic" states like Iran and North Korea. The potential emergence of a new superpower, China, and perhaps of new "great" powers like India, may lead to a new arms race, presumably with a nuclear dimension as well. In the consciousness of many, violence appears to be slipping through the leash of rational control, an image the media has not hesitated to foster, especially with respect to Sub-Saharan Africa.

Since the 1990s various influential authors have argued that Clausewitz's theory of war is no longer applicable, neither in relation to contemporary conflicts nor in general. Some have suggested that it is harmful and even self-destructive to continue to use this theory as the basis for understanding current warfare and as a guide to political action, given the revolutionary changes in war and violent action taking place throughout the world. Clausewitz, it is proposed, was concerned only with war between states employing regular armies, whereas conflict today mainly involves non-state actors. Both claims are overstatements, however, with respect to the core of Clausewitz's theory as well as the unique characteristics of today's "new wars." With the exception of much of Africa and some very old conflicts at the fringes of the former empires, existing states, alongside hierarchically organized political-religious groups like Hizbollah and Hamas, are still the decisive, if no longer the sole, actors in war. Will there be "another bloody century," as Colin Gray has proposed?[7]

The wars in Iraq and Afghanistan taught us the terrible lesson that in a globalized world winning a campaign does not necessary imply winning the war. According to Emile Simpson, the key point is that winning the war in a military manner means winning it in relation to the enemy, but increasingly now, audiences other than the enemy matter, and the narrative needs to address what they think as well as what the enemy and one's own side thinks. If the strategic narrative of the battle space in the twenty-first century is not only about winning the war in a merely military manner, then what is it about?[8] I would like to propose three different yet interconnected topics: the legitimacy of using force, the conduct during war, and the mutual recognition of the fighting communities after the war.

Before explaining this conceptualization in more detail, for purposes of clarity I will describe its basic ideas. The proposition stems firstly from my interpretation of Clausewitz's trinity, which is quite different from the so-called Trinitarian War. The latter is not a concept directly attributable to Clausewitz but, rather, an argument posed by Harry Summers, Martin van Creveld, and Mary Kaldor.[9] In my view, each war is composed of three aspects in differing combinations: the application of force, the struggle or fight of the armed forces, and the fighting community to which the warring forces belong. One can easily relate the legitimacy of using force, the conduct of war, and the mutual recognition of the fighting forces after the war to these three aspects of my interpretation of Clausewitz.

The second basic idea underlying my approach is related to the just war tradition, but not in the way that it was integrated into the doctrine of Responsibility to Protect (R2P), for example. In the just war tradition it is customary to differentiate among *jus ad bellum, jus in bello*, and *jus post bellum*. These three Latin terms may be characterized respectively as the right to wage a just war, the maintenance of rights and justice during war, and the orientation of warfare toward a just peace after the war. My thesis is that in a globalized world these three narratives are closely intertwined. The two most important European traditions grasping the meaning of war, namely, the notion of a just war and the notion of the right in war in the case of state-to-state wars, contributed initially to a tremendous limitation on violence.

Following the latter tradition, the acknowledgement of the foe as an equal with the same rights was the precondition for limiting the war after the disaster of the Thirty Years War, according to Carl Schmitt. Both conceptions succeeded in limiting warlike violence between European opponents at first. Yet at times the irregular methods of using force were simply pushed to the margins of the European world. During the crusades of the Middle Ages and in the course of colonial conquest from the sixteenth to the eighteenth centuries, non-European opponents were not merely fought but often downright annihilated. In both cases, the regular and bounded intra-European ways of employing force, which were practiced in the beginning of both eras, eventually ended in disaster.

The idea of a just war, which contributed to a limitation on war and violence for long periods during the Middles Ages, ultimately resulted in the religious battles of the sixteenth century and the Thirty Years War. The European style of state-to-state war in the "Westphalian Area," which was based upon a right to war between equal opponents and which in the eighteenth and nineteenth centuries led to a significant limitation on violence during war, resulted in the catastrophe of two world wars. One should not idealize the model of a limited European state-to-state war in reference to the forms they took at their origin in the seventeenth and eighteenth centuries, because this same model (together with the industrialization of war and new nationalistic and totalitarian ideologies) ultimately resulted in the two world wars. Similarly, there are no grounds for dismissing the notion of the just war tradition simply in view of the religious wars and the Thirty Years War. Rather, the curbing and protecting effects of war during long periods of the Middle Ages should be borne in mind.

The teaching of just war should not promote military violence, but rather hinder it or at least help to limit it. It is appropriately understood only against the background of fundamental reservations against war for the purpose of peace. That is, the threat and employment of military violence can only be justified conditionally – as instruments for preventing, limiting, and moderating violence. Despite this ideal definition of just war, three fundamental problems of this conception have appeared in the course of history: the unleashing of violence through the notion that the war is just, the stigmatization of the opponent as a criminal, and the restriction of one's own possible actions to violent measures because of the immediate connection between morality and politics.

I am not completely sure about the following proposition; it is more of a trial balloon. The notion of a just peace after the war is by no means free of problems. For example, the Nazis sought perfect harmony within German society and therefore excluded all those who seemed to them to disturb the concept of the perfect harmony of a unified German nation through the creation of a homogenous race. Perhaps this criticism of the notion of a just peace is not very convincing at first, but it is embedded in the problem of every strategy – whether the ends in war sanctify the means applied. In order to avoid these problems by pursuing only one of these three concepts, it is necessary to conceive of the containment of war and violence as an overarching political aim embedded in the various actions of national and international communities. Containment of war and violent conflict is based on the maintenance of a balance of all three tendencies.

During the past twenty years, we have witnessed the promises of the revolution in military affairs (RMA) and the appearance of seemingly new kinds of warfare, the so-called new wars. The RMA promised to present meaningful technological solutions to conflicts. Warfare and "military operations other than war" seemed to be legitimate if they easily led to victory. The costs would remain limited and the adversary could be presented as an outlaw of the international community in a classical view, as a dictator or warlord who would receive no support from the majority of the populace. All three propositions proved fatally wrong in Afghanistan and Iraq. For a brief moment, this understanding of the current battle space was revived in the campaign against Libya and the interpretation of the Arab Spring through Western eyes, which customarily view communities as composed of individuals, whereas in most parts of the world society is viewed as a community of communities. The conflict in Syria is reburying this technical world view.

Containing war, violent conflict, and mass violence does not necessarily mean conducting only limited warfare, but also setting limits on the escalation of violence in actual conflicts. This becomes more important with the more technical opportunities that are to be expected in warfare of the twenty-first century. To put it bluntly, the evolving battle space of the twenty-first century is about ethics and the morality of using force, its legitimacy. The more we develop technical opportunities in warfare, the more the morality of its use comes to the fore.

Let us consider an example. The US military places great emphasis on developing robotic warfare and warfare that could be conducted by artificial intelligence. Of course at first sight this development seems to be an ingenious way of saving humans from the outcomes of warfare. And in fact it is ingenious when used in defense against criminals and barbarians. Yet what if the opponent is no criminal or barbarian, but an innocent civilian? The moral problem is obvious, is it not? What are the implications of a robot equipped with artificial intelligence killing human beings? This problem leads us to the second topic, the conduct of warfare.

We can witness the importance of *jus in bello* in the current Syrian crisis. What makes weapons of mass destruction a particularly salient topic in light of the distinction between combatants and non-combatants? Recent events in Syria indicate the unjust and unfair consequences of the use of these weapons. This sentiment against unjust conduct in war is deeply embedded in the history of warfare as well as human consciousness. During the past twenty years, the concept of asymmetrical warfare has gained momentum. It has been used to describe the apparently new wars, which could be characterized according to Herfried Münkler as entailing asymmetry of weakness.[10] The weaker side turns to asymmetrical forms of warfare precisely because of its weakness in fighting a regular form of warfare.

Terrorism, partisan warfare, and attacking the populace of the adversary are typical examples of such asymmetrical warfare. But there is another kind of asymmetrical warfare, in which the superior side seeks to conduct warfare in such a way that the opponent does not stand a chance. This attempt to gain an asymmetrical advantage is at the core of the RMA debate. It is astonishing that the inherent connections between these two types of asymmetrical warfare are not, to the best of my knowledge, discussed as openly as they deserve to be. The prevalent view seems to be to give one's opponent no chance in warfare, in order to force him not to wage a war at all or to abandon the fight if he does. But there is another possibility for the weaker adversary: to turn to asymmetric warfare. The problem then arises that the more one gains an asymmetrical advantage over the opponent based on technical strength, which is perceived as unjust and unfair by the opponent, the more the latter will turn to the asymmetrical warfare that is typical of the weaker side, such as terrorism or partisan war.

This brings us to the last of my three propositions, the recognition of the warring parties after the war in order to bring about a just peace. Of course it is hard if not impossible to recognize criminals, terrorists, warlords, drug dealers, religious hard-liners, war criminals, or gangsters and mobsters as equal and legitimate combatants. These actors have only been prevalent in the last decade of the past century. We can still witness such privatized conflicts in most parts of Sub-Saharan Africa and at the fringes of the former empires. Most conflicts in today's world, however, are political in essence, and thus the above characterization of the actors involved does not apply to the overall trend these days. In this context, I am a Clausewitz scholar and adhere completely to his proposition that "The escalation in war would be endless if the calculation in the meaning of strategy would be 'uninfluenced by any previous estimate of the political situation it would bring about.'"[11]

Hence my conclusion is that we need a renewed strategy of containment, which must be different from that of the Cold War but based on some similar principles.

In contrast to the Cold War era, today there is no longer an exclusive actor to be contained, as the Soviet Union was. Even if one were to anticipate China's emergence as a new superpower in the next twenty years, it would not be reasonable, in advance of this actually happening, to develop a strategy of military containment against China similar to that against the Soviet Union in the 1950s and 1960s, as doing so might well provoke the type of crises and conflicts that such a strategy was intended to avoid.[12]

The second difference is that current developments in the strategic environment display fundamentally conflicting tendencies: between globalization and struggles over identities, locational advantages, and interests;[13] between high-tech wars and combat with knives and machetes or suicide bombers; between symmetrical and asymmetrical warfare; between the privatization of war and violence[14] and their re-politicization and re-ideologization, as well as wars over "world order";[15] between the formation of new regional power centers and the imperial-hegemonic dominance of the only superpower; between international organized crime and the institutionalization of regional and global institutions and communities; and between increasing violations of international law and human rights on the one hand and their expansion on the other. A strategy designed to counter only one of these conflicting tendencies may be problematic with respect to the others. I therefore stress the necessity of striking a balance among competing possibilities.

The third difference is that the traditional containment was perceived mainly as military deterrence of the Soviet Union, although in its original formulation by George Kennan it was quite different from such a reductionist approach. Our main and decisive assumption is that a new containment policy must combine traditional, military containment on the one hand with a range of opportunities for cooperation on the other. This is necessary not only with respect to China, but also to political Islam, in order to reduce the appeal of militant Islamic movements to millions of Muslim youth.

The idea of curbing war and violence in world society implies the expansion of non-military zones to which the Kantian conception of democratic peace applies, as well as the active containment and limitation of the expansion of war and violence. Such an overarching perspective has to be self-evident, little more than common sense, because it has to be accepted by quite different political leaders and peoples. The self-evidence of this concept could be so accepted that one might ask why we are discussing it. At the same time, such a concept must be distinguishable from competing concepts. It should also be regarded as an appropriate concept to counter contemporary developments. Finally it should to some extent only be an expression of what the international community is already doing anyway. "Other states are instrumental in interrupting the flow of finances from one institution to another, in restricting the movements of terrorists, in eliminating their save havens, in tracking down and arresting their principal leaders and in driving a wedge between the terrorist groups and the various populations they purport to champion."[16] What strategy are these states already pursuing? Nothing other than a strategy of containment!

The question of course remains of how to deter the true believers, members of terrorist networks or people like the former president of Iran, for whom even self-destruction might be a means of hastening millenarian goals. Of course, the true-believers or "hard-core" terrorists can hardly be deterred. But this is precisely the reason why containment should not be reduced to a strategy of deterrence. The real task even in these cases, therefore, is to act politically and militarily, in a manner that would enable separating the true believers from the mere believers and the latter from the followers. This strategy can include military actions and credible threats, but at the same time it should be based on a dual strategy of offering a choice between alternatives, whereas the resort to military means would only intensify violent resistance. Additionally, even true believers could be presented with the choice of either exclusion from their social and religious environment or reduction of their millenarian aspirations (and continued acceptance).

Of course in following this strategy there is no guarantee that every terrorist attack could be averted, but this is not the real question. Assuming that the goal of the millenarian Islamists is to provoke an over-reaction of the West in order to ignite an all-out war between the West and the Islamic world, there is no choice other than trying to separate them from their political, social, and religious environment.

Competing Concepts

The function of this conception can be clarified through the example of democratization. The limitation of war and violence lays the foundations of democracy. If the single counter-strategy to the proliferation of violence were a general, worldwide democratization – in the sense of implementing democratic elections, a necessary but not sufficient precondition of establishing real democratic societies – implemented (as would be necessary) through force, this would almost certainly lead to counterproductive results. This is particularly clear in those cases where fully developed constitutional democracies are not yet present, but states and societies are undergoing the initial process of transformation. It is more justifiable to speak of the antinomies of democratic peace in the latter cases than when referring to developed democracies.

Thus it is possible that a one-sided demand for democratic processes without regard to local conditions in individual cases might even contribute to the creation of totalitarian movements. The historical experience that corresponds to the change from democratic to totalitarian processes is embodied in developments during and after World War I. In nearly all of the defeated states there was initially a process of democratization, including, in some cases, democratic revolutions. Yet almost all ended in dictatorships. In Eastern Europe and the Balkans, the "right of national self-determination" proclaimed by US President Wilson was interpreted in a nationalist rather than democratic way, so that it entailed the exclusion of entire populations and even the first genocide of the twentieth century, committed against the Armenians, which already began during World War I.[17]

The so-called Arab Spring seemed at first to be a reversal of this development. But the current developments in Egypt, Syria, and Libya amplify the tendency described above, as all three are shaken by some form of civil war and are on their way to becoming failed states. Clearly, this situation does not exclude the possibility that the processes of democratization promoted from the outside might involve the use of violence. Historically speaking, one must remember that after World War II there were a number of democratization processes following militarily disastrous defeats, for instance in Germany and Japan, and later in Serbia after the Kosovo war. From the overarching perspective of the containment of war and violence, however, it can be reasonable in particular cases to renounce democratization in favor of disarmament.

The central approach developed here, in contrast to other theoretical conceptions of peace, can be described as follows: conceptions of democratic peace following Kant, those belonging to theories of equilibrium, and conceptions of hegemony and empire have all been used to bring about a limitation on war and violence in world society. But these means have often become ends in themselves. In my approach, the containment of war and violence itself becomes the overarching aim of political and communal action. Proceeding from this *political aim*, one can then judge *which* goal and *which* action are the most appropriate.

The Re-Ideologization and Re-Politicization of War

One can point to developments in Afghanistan as an example of the re-ideologization and re-politicization of war and violent conflict. After the victory over the Soviet army, a civil war between warlords and tribes began at the end of the 1980s. The conflict was re-ideologized, and the Taliban seized power. We see from this example that civil wars do not always become increasingly privatized until the smallest possible communities wield Kalashnikovs – communities that are only held together by the violence itself – and the fighting becomes independent of any purpose.[18] There have also been a number of cases in which civil wars have been ended by re-ideologization and re-politicization. Afghanistan is a good example because it illustrates the new quality of privatization of war and violence, and at the same time it reveals very clearly the re-ideologization and re-politicization of the conflict with the rise and eventual victory of the Taliban. Claiming that the privatization of the war in Afghanistan proves the emergence and nature of the new wars in general therefore leads to a paradox if the claim has to be restricted to the period up until the Taliban victory in 1996. This case, therefore, cannot be used to demonstrate a general shift towards the privatization of war. In fact, what it shows is that this development, though genuine, lasted for only a limited period (at least in this case). A new phase, the phase of world order wars, began in 1996.

One can supplement the periodization I am proposing by adding a geographical-hierarchical classification of the two phases. The privatization of violence can be observed in many parts of sub-Saharan Africa and in traditional conflict regions such as the Balkans and the Caucasus. The development of world order conflicts can be seen in the conflict between the West and militant Islam, and in the future it can be anticipated in relations with China and, perhaps, with Russia. It follows that events are moving away from the level of interstate war and conflicts in two directions simultaneously: downwards towards privatized war, and upwards towards supra-state war, world order wars. This distinction is more fundamental than the attempt to distinguish between privatized, "new" wars and those fragmented wars arising in the course of globalization, and the attempt to use this distinction as a way of challenging the legitimacy of the first set of concepts.[19] War that is waged to promote values[20] and as a way of ordering the world (whether this order is conceived as universal or particular) is quite different from privatized and fragmented wars. In practice, of course, these two levels are interlinked with one another and also with inter-state wars, but the analytic distinction is a significant one. States do still wage wars; however, for the most part they now do so not in pursuit of their particular interests but for reasons related to world order, as can be seen in the use of concepts like US empire[21] and American hegemony.

Processes such as the technological, economic, and communicational saturation of the world intensify this dual movement dramatically because they often link spaces of action directly with one another. During the civil war in Somalia, for example, bands of fighters could be seen using computers to buy and sell their Wall Street shares. The decisive factor, though, is the contradictory dual movement towards the privatization of violence and simultaneously towards existing, as well as future, world order wars and conflicts that can be either global or regional. Although it may not at first glance appear to do so, globalization does in fact re-politicize conflicts about world order.[22]

The Concept of Containment and Contemporary Warfare

The advantage of my concept can be further demonstrated by considering the nature of the end state for which the war on terror should be fought: trying to find terrorists and rooting all of them out, as Donald Rumsfeld stated?[23] Another question is how to fight organizations, which are not hierarchically structured, but as often noted, function like networks?

I conclude that the goal of the war on terror should not be to gain victory, because no one can explain what victory would mean with regard to this type of war. Moreover, trying to gain a decisive victory over terrorists would result in the production of more of them. An additional problem is not only how we ourselves conceive of the concept of victory, but even more important, how low-tech enemies (for example) define victory and defeat. This is an exercise that requires cultural and historical knowledge much more than impressive technology.[24] Instead, one could argue, the goal is containment of terror, which is of course quite different from appeasement. An essential limitation of the dangers posed by terrorist organizations could be based on three aspects: first, a struggle of political ideas for the hearts and minds of the millions of young people; second, an attempt to curb the exchanges of knowledge, financial support, and communication among the various networks, with the aim of isolating them on a local level; and finally, but only as one of these three tasks, to destroy what the Israelis call the terrorist infrastructure. In my understanding, trying to achieve victory in a traditional military manner would not only fail, but would perhaps greatly increase terrorism in the foreseeable future.

The concept of the center of gravity in warfare provides another illustration of the way in which my conception makes a difference. Clausewitz defines war as an act of violence to compel our enemy to do our will. This definition suits our understanding of war between equal opponents, between opponents in which one side does not seek to annihilate the other or his political, ethnic, or tribal body. But in conflicts between opponents with different cultures or ethnic backgrounds, the imposition of one's will on the other is often perceived as an attempt to annihilate the other's community and identity. Hence, for democratic societies, the only alternative is to perceive war as an act of violence in which, rather than compelling our own will on the opponent, our opponent is rendered unable to pursue his own will violently, unable to use his full power to impose his will on us or others. Consequently the abilities of his power must be limited, such that he is no longer able to threaten or fight us in order to compel us to do his will.

The purpose of containing war and violence, therefore, is to remove from the belligerent adversary his physical and moral freedom of action, but without attacking the sources of his power and the order of his society. The key to mastering violence in this sense is to control certain operational domains, territory, mass movement, and armaments, as well as information and humanitarian operations. But this task of mastering violence should no longer be perceived as being directed against the center of gravity, but rather towards the gravitational field lines. Instead of increasing the imposition of one's own will on the adversary up to the point of controlling his mind, as the protagonists of Strategic Information Warfare put it,[25] the only way of ending conflict in the globalized twenty-first century is by containing the escalation of war and violence while simultaneously providing space for action within these boundaries.

The position I have put forward is oriented towards a basically peaceful global policy and treats the progressive limitation of war and violence as both an indefinite, ongoing process and an end it itself. The lasting and progressive containment of war and violence in world society is therefore necessary for the self-preservation, and even survival, of states and of the civility of individual societies and world society.

Notes

[1] A previous version of this paper was published as "A New Containment-Policy: The Curbing of War and Violent Conflict in World Society," S. Rajaratnam School of International Studies, Singapore, May 2, 2013.

[2] See Tim Mark, "Chuck Hagel Stumbles on Iran Questioning," *Politico*, January 31, 2013, http://www.politico.com/story/2013/01/chuck-hagel-stumbles-on-iran-question-87001.html.

[3] George, F. Kennan, "Containment: 40 Years Later," in *Containment: Concept and Policy*, eds. Terry L. Deibel and John Lewis Gaddis (Washington: National Defense University Press, 1986), pp. 23-31.

[4] Charles W. Kegley, Jr. "The New Containment Myth: Realism and the Anomaly of European Integration," *Ethics & International Affairs* 5 (1991): 99-115.

[5] See Nathan K. Finney, "Using the Threat of Violence to Contain Syria: An External Approach," *Infinity* 3 (Summer 2013): 13-16.

[6] Dieter Senghaas, *On Perpetual Peace: A Timely Assessment* (New York: Berghahn Books, 2007).

[7] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld and Nicholson, 2005), p.9.

[8] Emile Simpson, *War from the Ground Up* (London: Hurst Publishers, 2012).

[9] Andreas Herberg-Rothe, *Clausewitz's Puzzle: The Political Theory of War* (Oxford: Oxford University Press, 2007). The following is taken from Andreas Herberg-Rothe, "The Evolving Battle Space of the Twenty-First Century," Lecture at Nanyang University, Singapore, September 19, 2013.

[10] Herman Münkler, *The New Wars* (New York: Polity Press, 2004).

11 Carl con Cluasewitz, *On War* (Princeton: Princeton University Press, 1984), p. 78.

12 See, for example, "US Denies New Containment Policy against China," *People's Daily Online,* http://english.people.com.cn/200511/24/eng20051124_223692.html, November 24, 2005.

13 Zygmunt Bauman has labelled these contrasting tendencies as "Glocalisation," meaning a combination of "Globalisation" and "Localisation." Zygmunt Bauman, "Glokalisierung oder: Was für die einen Globalisierung, ist für die anderen Lokalisierung," *Das Argument* 217 (1996): 653-664; Zygmunt Bauman, *Globalization* (London: Polity Press, 1998) (German).

14 Münkler, *The New Wars*; Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era* (Stanford: Stanford University Press, 1999).

15 I have put forward the thesis that after the breakdown of an empire, after a demise of a system of world order, there has nearly always been a tendency towards a privatization of war and violence, to a level beneath that of the previous situation, as happened after the fall of the Soviet Union and the bipolar order of the Cold War. But in the long run, in my estimation, the importance of politics and ideology even increases; see Andreas Herberg-Rothe, "Privatized Wars and World Order Conflicts," *Theoria* 53, no. 110 (2006): 1-22.

16 Antulio Echevarria, *Fourth-Generation Warfare and Other Myths* (Carlisle, PA: Strategic Studies Institute, 2005), pp. 5-6.

17 Dan Diner, *Das Jahrhundert verstehen,* (Frankfurt: Fischer, 2000) (German).

18 This image symbolizes the "new wars" discourse better than any other, and also symbolizes Thomas Hobbes's war of all against all.

19 Sven Chojnacki, "Wandel der Kriegsformen – Ein Kritischer Literaturbericht," Leviathan, 32, no. 3 (2004): 402-24.

20 Hans Joas 2000, *Kriege und Werte: Studien zur Gewaltgeschichte des 20. Jahrhunderts* (Weilerswist: Velbert, 2000.

21 Michael Walzer, Just and Unjust Wars: A Moral Argument with Historical Illustrations(New York: Basic Books, 2000); Michael Walzer, "Die Politik der Rettung" Berliner Debatte Initial 6, 1995, pp. 47-54.

22 Antulio Echevarria, "Globalization and the Clausewitzian Nature of War," The European Legacy 8, no. 3 (2003): 317-32.

23 nterview with Donald Rumsfeld, "You Can Only Defend by Finding Terrorists and Rooting Them Out," *The Daily Telegraph*, February 25, 2002.

24 Robert D Kaplan, "The Story of a War," *Atlantic Monthly*, November 2003.

25 David Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), p. 208.

Integrating Technologies to Protect the Home Front against Ballistic Threats and Cruise Missiles

Yossi Arazi and Gal Perel

This article discusses active protection in response to the rocket threat to Israel's home front. The defense establishment anticipates that in an all-out war, the home front would be attacked for about thirty days, and that every day there would be about one thousand rocket and missile hits that would cause thousands of casualties as well as damage to infrastructures and strategic sites. Israel has an active protection system with five layers of interceptor missiles, and in cooperation with the United States, it developed Nautilus, a chemical-laser-based defense system from which the Skyguard system is derived. In 2007, the Iron Dome system, whose missiles are more expensive, was chosen over it for reasons both economic and operational. Yet only an integrated response that includes anti-missile defense systems and chemical laser systems will offer a comprehensive solution for active protection against all threats, without causing any significant economic difficulties.

Keywords: Iron Dome, active protection, high trajectory weapons, Skyguard system, Operation Pillar of Defense

Background

Operation Pillar of Defense took place in November 2012 and highlighted once again the growing rocket threat to the State of Israel. Although there has been a significant reduction in the threat of ground maneuvers against

Colonel (ret.) Yossi Arazi was a pilot in the Israeli air force and an electronic engineer involved in the development of weapons systems. Gal Perel is a research assistant at INSS.

Israel by neighboring enemy states, the operation showed that there is a real threat to the country's population centers.[1] As Lieutenant General (ret.) Gabi Ashkenazi said at the time, "He who creates an advantage in this fighting succeeds in preparing first for the next threat."[2]

The Israeli defense establishment anticipates that in an all-out conflict, an attack on the home front by Syria, Hizbollah, and Hamas would last for some thirty days. The expectation is that the Israeli civilian front would be struck by approximately 1,000 missiles, rockets, and cruise missiles every day,[3] some of them GPS guided and accurate to within several meters. The estimated harm caused would be thousands wounded, destruction of infrastructures, and damage to strategic sites. To counter this threat, Israel is developing and implementing a defensive system that would operate from the moment the missiles or rockets are launched until they hit the ground. This system is based on five layers of missile defense: Iron Dome, Magic Wand, Arrow 2, Arrow 3, and Patriot. The working assumption is that the Defense Ministry is planning to complete the development processes, including for radar and communications systems, and that it will acquire the various defensive missiles in quantities sufficient for several days of fighting.

In the mid-1990s, the government of Israel, in close industrial and operational cooperation with the United States, began to develop Nautilus, an anti-Katyusha defense system based on a high-energy chemical laser. Nautilus was intended to protect Kiryat Shmonah, where it was planned to be positioned prior to the withdrawal from Lebanon. From 2000 to 2004, there were 46 tests of the system against various ballistic threats, including mortars, different rockets, and artillery shells. All of them, without exception, were intercepted. At the same time, the planning of the Skyguard system – the immediate derivative of Nautilus – was completed and ready for production. In early 2007, the Nagel Committee concluded that the Iron Dome system was preferable to Skyguard for various reasons, one of which being the conclusion that the kinetic interception option has clear financial and operational advantages over laser interception. The development and testing of Skyguard was, therefore, stopped. Significantly, the 2008 state comptroller's report 59A criticized the manner in which the recommendation was formulated, as well as the fact that no operational need had been defined that delimits the operational gap or defines the requirements for an active defense system. This led to an expansion of the threat reference from Qassam rockets to all types of short-range high-trajectory fire.[4]

This article aims to show that only an integrated solution that includes anti-missile and anti-rocket defense systems together with high-energy chemical laser systems will result in the implementation of a comprehensive defense solution and protect the entire civilian front from all types of threats. This response would provide protection for the period of fighting regardless of how long it is, and could be implemented without significant economic difficulty. Furthermore, a system that is based only on defensive missiles is not practicable for financial reasons because it cannot provide protection in some of the operational scenarios.

The Threat Reference Scenario

Israel's security concept holds that if a future campaign presents a threat that is defined as a clear and present danger, Israel would have to carry out a preventative action as soon as possible and aim to shorten the fighting's duration to the extent feasible. This is due to the state's lack of strategic depth and its limited ability to absorb economic damage, as well as a large number of civilian casualties. Hence, the goal must be to defeat the enemy on its territory quickly and decisively in order to avoid battles that would take place near Israel's civilian population.[5] From the offensive standpoint, the Israeli Defense Force (IDF) has prepared for this by means of a combat doctrine that rests on three pillars: "(1) a destructive strike of firepower against the enemy's core assets; (2) a quick maneuver to damage the enemy and paralyze its launching capabilities in the area of the maneuver; and (3) stamina and defensive capabilities on the civilian front."[6] This doctrine is based on the assumption that in the case of a military conflict on the scale of the Second Lebanon War or Operation Cast Lead, Israel will not have great latitude in time, space, or legitimacy for the use of force regardless of the intensity and severity of hundreds of rockets and missiles being fired on the state every day. A better solution for Israel would be to strike the enemy, as in the attack on Hizbollah's headquarters in Beirut during the 2006 Second Lebanon War in order to achieve the *Dahiya* effect and deter the enemy.[7] As Lieutenant General Benny Gantz said, "In reality, when we seriously damage the enemy's launching capability, and when our achievements on the ground are clear, and the other side begs for a ceasefire, there will be no doubt as to who is the victor and who the vanquished."[8]

The drive to shorten the combat's duration does not, however, insure that the battle will indeed be short.[9] An examination of the Second Lebanon War, in which the IDF fought against Hizbollah for 34 days, shows that in the course of the fighting, the organization fired some 4,000 rockets of various kinds at the Israeli home front – close to 250 rockets a day toward the end of the war – thus bringing everyday life to a halt for the residents of northern Israel.[10] The defense establishment, therefore, anticipates that in the future, the fighting against Syria, Hizbollah, and Hamas will continue for up to 30 days.

The threat to the State of Israel is evolving and ongoing in every aspect.[11] The weaponry is becoming much more destructive and precise in its hits, and the threat is expanding in range. Today's high-trajectory weapons threaten the entire country, unlike in the past, when they only threatened Israel's northern border. The launching sites have also expanded to include the Gaza Strip, the Sinai Peninsula, and Iran, and cover an area ranging from hundreds of meters from the border for mortar shells to distances of 1,500 kilometers or more for Iranian Shihab missiles. The amount of weaponry in the possession of the enemy is also increasing,[12] and currently they have between several thousands and hundreds of thousands of missiles and rockets. These include mortar shells for ranges of up to several kilometers, which are one of the main threats to the Gaza perimeter communities; Qassam and Grad rockets, which are fired to distances of between 3-40 kilometers; Fajr short-to-medium-range rockets that range some 60-90 kilometers; F110 and M600 rockets, which are fired to distances of 200-300 kilometers and have 200-kilogram warheads and GPS accuracy; and Scud missiles that reach distances of 200-700 kilometers and have warheads of hundreds of kilograms that could be armed with chemical or biological weapons. To this range of threats we can add the Iranian Shihab-3 and Shihab-4, which also have the potential to be armed with nuclear warheads, and Russian made P-800 cruise missiles (Yakhont) that are in Syrian possession, have GPS accuracy, and cruise at an altitude of 10-15 meters at a speed up to Mach 2.5. These missiles could potentially destroy all strategic targets in Israel as soon as the conflict begins.

As a basis for planning the defense system, this article relies on the defense establishment's assumption that a quantitative model should be developed for every type of threat that may be launched at Israel during a 30-day fighting period. It can be expected that as the fighting continues, the rate of missile fire will decrease, as in the case of Operation Cast Lead, where Hamas began by firing hundreds of rockets per day, a number that decreased to 13 rockets per day towards the end of the Operation.[13]

Nevertheless, this assessment holds that on any given day Israel will be attacked with hundreds of mortar shells, some 800 short-range rockets from the Qassam-1 to the enhanced Grad, about 100 short-to-medium-range threats (including Fajr rockets, the F110, and Zelzal missiles), approximately 100 medium-range or higher threats (including M600 rockets, Scud missiles, and Shihab missiles from Iran), and several dozen cruise missiles.[14]

Basic Requirements for an Optimal Defense System

The defense system required for this task would optimally be able to cope with a large quantity of high-trajectory threats and rockets of various kinds and destroy them before they reach the ground in a way that will be affected as little as possible by the duration of the conflict. Iron Dome, for example, was developed for short-range threats, Magic Wand for threats fired from ranges of 100-200 kilometers, and Arrow 3 is currently being developed as a response to threats fired from ranges of some 1,000 kilometers or more.

The ideal defense system, however, should be able to intercept all threats the enemy is capable of launching – including firing in volleys – and maintain this capability over time. The cost of destroying a threat should be as low as possible in order to avoid economic restrictions on the use of the system. It would need to be available for use against all types of ballistic threats and cruise missiles and in any type of weather, and its response time – from the moment the threat is launched or enters the security envelope to the moment it is destroyed – would be as short as possible in order to allow action against threats fired from especially short ranges. Finally, the system's rearming at the end of the fighting in preparation for the next conflict would not require a massive investment, and technological development would not be needed every time a new threat appeared on the scene. In this article, we examine and evaluate the various solutions available and their integration with a focus given to their ability to meet the requirements.

Advantages, Disadvantages, and Feasibility of a Missile Defense System

The main operational advantage of a system that is based only on defensive missiles is its ability to operate in all weather conditions, if it was designed accordingly. An additional advantage is that such systems are currently in different phases of implementation – from completed development (Iron Dome and Arrow 2) through initial development (Magic Wand and Arrow 3) to procurement (Iron Dome, Arrow 2, and Patriot) – which allows for more rapid procurement.

The problem with this type of system is that when a new threat appears, a defensive missile must be developed to counter it. In addition, a defensive system that relies only on defense missiles is fundamentally flawed, as budgeting for procurement of defensive missiles that could cope with the number of threats the enemy presents requires enormous funds the state cannot allocate for this purpose. In fact, Israel and the IDF will only have a relatively small quantity of anti-missile missiles, resulting in partial protection that will be reduced as the fighting continues.

Other problems arise from the failure of the systems to meet the operational requirements in the face of the threat. The Iron Dome system does not have the ability to cope with certain threats, such as the various Qassam rockets and the regular and enhanced Grad missiles, which are fired from short distances of about 3-15 kilometers,[15] as well as mortar shells, which means that protection for over 1 million people living up to 10-15 kilometers from the borders is deficient.[16] The various types of defensive missiles lack the ability to contend with cruise missiles, particularly the Russian made P-800. Increasing the accuracy of the rockets will cause the collapse of the "selective fire" concept – not intercepting threats that fall in open areas will make it necessary to intercept all threats. This will surely have a severe economic impact. When the fighting ends, it will be necessary to replenish the supply of all defensive missiles fired during the conflict, a process that would take many years to accomplish, be very expensive, and leave Israel exposed to threats until it is completed.

Proponents of the system hold, as GOC Northern Command Gadi Eizenkot stated, that the system "must be directed first and foremost at preserving the IDF's offensive capability and not at defending civilians" and that it should protect Israel's critical infrastructures, IDF bases, and military forces' gathering points. Within approximately three days, an offensive move carried out by the IDF would lead to a significant reduction in the firing and extensive damage that would result in a ceasefire.[17] Hence, the system would not be required to cope with a large quantity of rockets. According to Brigadier General (ret.) Danny Gold, former head of the Research and Development Department in the Ministry of Defense, the existing system is proof of Israel's willingness to protect its civilians and their property and enable the economy to continue functioning during a time of war.[18] This system also allows the political echelon greater room to maneuver during a military operation.[19] A study by former head of the Wall Missile Defense Program Uzi Rubin indicates that while in the Second Lebanon War Hizbollah needed to fire an average of 75 rockets to kill one person, the Iron Dome system raised the ratio so that it now takes 375 rockets to kill one person.[20]

Advantages, Disadvantages, and Feasibility of Defense Based on High-Energy Chemical Lasers: Ground and Airborne Skyguard

Ground-Based Laser Systems: Nautilus and Skyguard

Development of the Nautilus system began in June 1996 and ended in June 2000, with two successful tests that included the destruction of rockets in mid-flight. Dozens of additional tests were conducted from June 2000 to November 2004, in which the system intercepted all 46 of the threats that were launched against it: 31 Katyushas and other rockets, five 152-mm. artillery shells, and 10 mortar shells, three of which were shot in one volley.[21]

The Skyguard system is a direct development of the Nautilus. Its detailed engineering design was carried out between 2000 and 2005 and was presented to the US army and representatives of Israel's Ministry of Defense in August 2005. Skyguard is four times smaller than Nautilus[22] and directs four to five times more energy against the target. This increases the system's effective range by some 10 kilometers (15 with adaptive optics). Hence, with eight Skyguard systems operating, all of the Gaza perimeter communities would be protected; with 26 systems, the entire northern part of Israel (from Kiryat Shmonah to the Haifa-Afula-Beit Shean line) could be protected; and with a total of 80 systems, all 40 large population centers and strategic sites in Israel could be protected.[23] Northrop Grumman, the company that developed the system, has committed to meet the full military standards of availability, reliability, maintainability, and transportability.

The Skyguard system consumes five different types of gases – nitrogen fluoride, hydrogen, ethylene, helium, and oxygen – along with jet aircraft fuel. All materials are sold in the open market and are inert, non-toxic, and non-explosive (though they could ignite if directly hit). The by-products of lasing – that is, a steady transfer of laser energy to the target in order to destroy it – include hydrogen fluoride and deuterium fluoride, which are hazardous to health. The required safety zone is 100 meters, which can be reduced to 20-30 meters if a special filter is installed on the system. Next to every Skyguard ground unit there are two tanks (the size of a standard fuel-supply tank), which contain the gases and the fuel required for 40 seconds of continuous lasing (suitable for the destruction of 20 threats on average). Switching from one tank to another takes a number of seconds, while replacing an empty tank with a full one takes about two-three minutes.

When the company completed the engineering design,[24] it committed to supply the Skyguard systems to the Ministry of Defense 18 months after the decision was made and at a fixed price. The company also agreed to pay fines for falling behind schedule.

The ground-based Skyguard system has advantages in the basic concepts of firing. Missing a target is not possible due to the system's use of a laser beam that locks on to the reflected energy of the target. The system is able to destroy any target that enters its 10-15 kilometers cover range, and actually has a perpetual and accessible magazine of the fuels and gases required for its operation, which can be supplied in the same way that air force planes are refueled.

As was proven in tests, the system will be effective against mortar shells, various types of missiles and rockets, such as Shihab 4 missiles that are fired from ranges of up to 2,000 kilometers, and will also respond to the threat of cruise missiles. The average rate of target destruction is about one per three seconds, which includes the time it takes to move on to the next target and allows the destruction of volleys of missiles fired simultaneously. For example, it takes about 38 seconds for an enhanced Grad rocket fired at a distance of 40 kilometers from the moment it enters the effective range of Skyguard (15 kilometers) until it hits the ground. One system can destroy a volley of about eleven such rockets fired simultaneously. Since the system works at the speed of light, it will not be necessary to upgrade it when more advanced threats appear. It enables interception of the target immediately after its discovery and does not require reevaluation of the target's interception point. Hence, threats can be destroyed within less than five seconds from the moment they are launched or enter Skyguard's effective range.

The cost of interception is very low, some 1,000 to 3,000 dollars[25] (the price of the gases and fuel used to create the laser beam varies depending on the range). In comparison, the cost for two Iron Dome missiles to hit one target starts at hundreds of thousands of dollars and can go up to several million dollars for two missiles such as Magic Wand or Arrow. The system has the ability to defend itself against any ballistic threat fired at it. The technology is available and has been proven in dozens of tests, and an official request from the government of Israel to the US government could lead to a resumption of activity on the issue.

The main drawback of the Skyguard system is that the effective range of the laser beam decreases significantly when it needs to penetrate thick, dense clouds (from 5/8 and up), in which case defensive missiles would be relied on. Nevertheless, the Skyguard system can still intercept ballistic threats when they are below the cloud base. In that case, the laser beam "waits" for the threat until it is exposed again.

The Airborne Skyguard System

In the early 1990s, the United States started developing the Airborne Laser (ABL), a high-energy laser system, which was installed on Boeing 747 planes. Its mission was defined as destroying ballistic missiles during the boost phase of flight at ranges of hundreds of kilometers from the interceptor aircraft. In February 2010, after a lengthy development process, the first system test was carried out, and two ballistic missiles were intercepted at a range of nearly 100 kilometers from the ABL aircraft.[26] The test was significantly successful: for the first time in history, ballistic missiles were destroyed in the air and at very long ranges, proving the technological feasibility of the system.

Threats can also be destroyed at the penetration phase, of course. The interceptions take place above the clouds and therefore above weather effects. Any missile that is launched at ranges of 30 kilometers or more reaches heights exceeding 40,000 feet. The greater the range the missile is launched from, the greater the height it reaches. The airborne Skyguard system is designed to destroy any threat that is launched from ranges between 30 to 2,000 kilometers, which is the maximum range from which Israel is threatened.

The start of the interception will be at very large ranges from the interceptor aircraft, which will be able to destroy fragmentation warheads with each fragment being intercepted separately. In 2003, Northrop Grumman made a proposal to the Israeli defense ministry to install the "regular" Skyguard system on a medium transport aircraft. This configuration enabled destruction of threats at ranges of about 130-150 kilometers from the interceptor plane, and was called ARIEL.

This article proposes that an examination of the airborne Skyguard system's enhanced configuration takes place, as was done on the ABL, and increase the output to 3 megawatts and the optical diameter to 1.5 meters. If installed on a large aircraft like the Boeing 747-300, the system would be able to carry an ample quantity of fuel and gases in order to perform a number of interceptions. A few aircraft flying around the clock could intercept any ballistic threat in combination with the defensive layers of anti-missile missiles.

Similar to ABL, the enhanced ARIEL system's anticipated capability is its ability to intercept ballistic threats that are found at a range of some 400 kilometers from it and above 30,000 feet. Initial calculations show that lasing can be produced approximately 200 or more times before the aircraft needs to be refueled with the gases and fuel that are needed for lasing. Thermal calculations show that for Shihab and Scud D missiles, we can assume a required lasing time of some five seconds to destroy the threat and approximately another two seconds to move to the next threat. For the other threats, like Scud C, the required lasing time is about three seconds, with another two seconds to move to the next threat. The gross interception times will be seven seconds and five seconds, respectively. ARIEL aircraft will be able to intercept any ballistic threat launched from a range exceeding about 30 kilometers and in dense volleys. The other tactical rockets, from a regular Grad to smaller threats, do not exceed an altitude of 30,00 feet during flight and will be intercepted by the ground-based Skyguard systems and Iron Dome missiles.[27]

Work on the ABL system was stopped in 2011 due to the system's lack of sufficient power to enable an aircraft to operate outside the borders of Iran, as explained by former US Defense Secretary Robert Gates.[28] This limitation is not relevant to Israel, however, as the aircraft would remain in the air over the country and intercept threats at the penetration phase, when they are at a distance of approximately 400 kilometers or less from the target.[29]

Budgetary Scenario

Basic Assumptions

- The fighting scenario is as described in the Threat Reference Scenario section.
- The defense establishment will continue to invest in missile defense systems.
- The cost estimate for procurement of defensive missiles only is based on the assumptions that inventory will be prepared for 40 days of fighting and that missiles fired in the course of 30 days of fighting will be replaced. In order to have a reasonable chance of success in intercepting a threat, two defensive missiles will be needed. The cost of an Iron Dome missile is 100,000 dollars,[30] of a Magic Wand missile, 1.25 million dollars, and an Arrow 2 or Arrow 3 missile, about 3 million dollars.
- The expected cost of the airborne and ground-based laser element in the integrated system will be presented, that is, five airborne Skyguard systems and 80 ground-based Skyguard systems. The radar and communication infrastructures for missile defense systems will also support the laser systems.
- The investment required for procurement of defensive missiles alone (not including launchers, support systems, and infrastructures) is as follows: to intercept 250 short-range rockets every day that are likely to fall in various premises (out of the 800 that will be fired), 500 Iron Dome missiles will be required. The cost of preparing for 40 days of fighting will reach approximately 2 billion dollars. Interception of the 100 medium-range missiles and rockets will require the use of 200 Magic Wand missiles per day at a total cost of 10 billion dollars for 40 days of fighting. The cost of 200 Arrow and Patriot missiles to intercept long-range threats every day will reach 24 billion dollars. For 40 days of fighting then, the total sum of 36 billion dollars will be needed for procuring inventory. The cost of just “pressing the trigger” on one day of fighting will get to approximately 900 million dollars. Following the fighting, the cost of procuring inventory to replace the missiles fired during 30 days of fighting will reach 27 billion dollars (3/4 of the cost

of procurement for 40 days). The total cost of preparing an inventory of missiles alone for 40 days and replacing inventory after 30 days of fighting will reach up to 63 billion dollars. These are prohibitive sums that will never be allocated.

Investment in Ground-Based and Airborne Skyguard Systems

Ground-Based Systems

The specification submitted by Northrop Grumman in a letter sent in 2007 quotes the following prices:

- 310 million dollars for the first three systems.
- 40-50 million dollars for a system in production (depending on the quantity ordered). The price includes communications and also unique radar for each Skyguard system, which costs approximately 15 million dollars. One radar will feed four or five systems, so it can be assumed that some 30 million dollars would be necessary for a Skyguard system in serial production. The price of the 77 remaining systems will be approximately 2.3 billion dollars.

In addition, the following will be required:

- 200 million dollars (estimated) for fueling infrastructures.
- 300 million dollars (estimated) for administrative and maintenance infrastructures and spare parts.

The total cost is estimated at about 3.1 billion dollars for 80 ground-based Skyguard systems to protect all critical sites and population centers in Israel.

Airborne Laser Systems

The figures given in the letter from Northrop Grumman quote the price of 177 million dollars for the first ground-based Skyguard system. Based on this figure, it can be assumed that the development phase for airborne systems will require an estimated 100 billion dollars for the purchase of a used Boeing 747 and some 250 million dollars to build a prototype of the first airborne Skyguard systems. The airborne system is simple to implement compared to the ground-based system due to the low atmospheric pressure that exists at an altitude of 40,000 feet and is required for production of the laser beam. An additional 100 million dollars will be added for purposes of planning and implementing installation in the aircraft and another 100 million dollars for testing. In addition, about 100 million dollars will be needed for infrastructures, maintenance, and refueling of the laser systems on the ground, and another 50 million for other expenses. This is a total of some 700 million dollars for the development phase and production of the first aircraft. Procurement of another four airborne Skyguard systems, including their installation, will cost about 120 million dollars per aircraft, 50 million dollars for the laser system (20 million more than for the ground-based Skyguard system), and approximately another 20 million dollars for spare parts, maintenance support, and other expenses. The total price of one aircraft will be approximately 190 million dollars, and the price of the four additional aircraft will be about 760 million dollars. The overall price of procurement of the ground-based and airborne laser systems, including maintenance support, operational auxiliary systems, and the like is expected to reach up to 4.6 billion dollars, an investment that will be spread over about eight years and is economically feasible.

Cost of 30 Days of Fighting with Skyguard Systems Alone

Cost of one day of fighting

- 1,000 lasing to destroy all 1,000 threats – 2 million dollars
- 72 flight hours (3 aircraft in a row at 15,000 dollars an hour) – 11 million dollars

The total cost comes to 13 million dollars per day, compared to 900 million dollars per day for partial protection with missile defense systems. The cost of 30 days of fighting would be some 400 million dollars, compared to a cost of 63 billion dollars for the defensive missiles alone.

Effectiveness of the Integrated Solution

The integrated solution makes it possible to economically and operationally implement a comprehensive system of protection that is effective and efficient at protecting the entire home front. As concluded above, an investment of about 4.6 billion dollars in ground-based and airborne laser systems will make it possible to save more than 55 billion dollars over the cost of missile defense alone, and create a feasible system. The integrated system would include about five high-energy laser aircraft (ARIEL), five defensive layers of anti-missile missiles (Iron Dome, Magic Wand, Arrow 2, Arrow 3, and Patriot) in quantities and deployment to be determined by the defense establishment, and 80 ground-based Skyguard systems. This combination meets all the necessary requirements for the ultimate, ideal

Table 1. Comparison – Performance and Cost[31]

Interceptor/Type of Threat, Characteristics, and Costs	Iron Dome	Magic Wand	Arrow 2	Arrow 3	Ground-Based Skyguard System	Airborne Skyguard System	Comments
Mortar Shells	/	/	/	/	V[1]	/	[1] Destroys a threat every 3 seconds.
P-800 Cruise Missiles	/	/	/	/	V[1] Volley of 4-5 missiles	/	
Qassams and Grads up to 12-15 kilometers	/	/	/	/	V[1]	/	
Grads to a range of 15-40 kilometers	V	/	/	/	V[1] Volley of 10-12 missiles	V[1,2] Volley of 10-30 missiles	[2] Firing from a range of over 30 kilometers
Fajr-3, Fajr-5	V	Maybe	/	/	V[1] Volley of 9-10 missiles	V[1,3] Volley of 15-23 missiles	[3] Threats will be intercepted under a range of 400 kilometers and over 30,000 feet
Zelzal, M600, F110	/	V	Maybe	/	V[1] Volley of 4-5 missiles	V[1,3] Volley of 18-52 missiles	
Scud B, C	/	Maybe	V	Maybe	V[1] Volley of 2-3 missiles	V[3,4] Volley of 56-64 missiles	[4] Estimated lasing time 3-5 seconds
Scud D, Shihab 3, 4	/	/	/	V	V[1] Volley of 1-2 missiles	V[3,4] Volley of 15-33 missiles	
Cost of 1 interception (2 missiles)	200,000 dollars	2.5 million dollars	6 million dollars	6 million dollars	Up to 3,000 dollars	Up to 5,000 dollars	
Cost of 1 day of fighting	50 million dollars (250 interceptions)	250 million dollars (100 interceptions)	300 million dollars (50 interceptions)	300 million dollars (50 interceptions)	2-3 million dollars	2-3 million dollars, including 72 flight hours	

system, which will provide protection against mortar shells and cruise missiles, defend communities near the border, and allow a dual defensive response in most cases using the laser system and defensive missiles. As a general rule, it is always preferable to use the laser system due to its low cost. Defensive missiles will be a backup for the ground-based laser system in the event of bad weather and when it is necessary to defend against especially dense missile volleys. The radar, communications, and control systems that are intended to support defensive missiles will also support laser systems, both ground based and airborne.

Operation Pillar of Defense – Protection from All Threats Fired from the Gaza Strip as a Case Study

Operation Pillar of Defense is unique in the sense that it was the first conflict in which the State of Israel used an active defense system – Iron Dome – rather extensively. At the recommendation of the military and political echelons, the operation began as a planned and orderly move whose objectives were to strengthen deterrence, to strike a hard blow at the rocket array, to inflict a painful blow on Hamas and the other terrorist organizations involved, and to stop the rocket fire directed at Israel from Gaza.[32] The start of the operation included an aerial attack to assassinate Ahmed Jabari, commander of Hamas's military wing in the Gaza Strip, and another aerial attack whose targets were warehouses and missile-launching pits for Fajr-5 rockets ranging some 75 kilometers. The IDF was working to shorten the duration of the fighting, which was reflected in the political echelon's pursuit of a mechanism for ending the operation[33] and in the directive by Chief of Staff Benny Gantz "to continue to attack with every bit of force and to step up the pace,"[34] in accordance with the approach of achieving the objectives quickly.

There is no doubt that during the fighting the system made a significant contribution to the home front's morale. And indeed, the more effective the defensive system is, the greater the home front's morale, as well as its ability to cope with the situation. In the course of the operation, Hamas fired 1,506 rockets at Israel, but only 479 of them were fired at populated areas. Iron Dome succeeded in intercepting 421 rockets, achieving the success rate of 84 percent.[35]

It is important to examine the limitations and disadvantages of using a system that is based on defensive missiles alone versus the advantages of combining two technologies – defensive missiles and a high-energy laser – in an integrated defense system. Within this discussion, there are two main points: the inability of defensive missile systems to protect communities near the border and the cost of defensive missiles, which limits the number of missiles that can be purchased.

Two Israeli governments have recognized Iron Dome's limitations in protecting sites near the border. In early 2008, after Iron Dome's limitations were made clear, the Olmert government decided to secure all homes up to 4.5 kilometers from the border, which were, at the time, threatened by the somewhat slow Qassams. The current government decided in mid-2012 to secure all homes up to 7 kilometers from the border. Minister Matan Vilnai even stated in November 2011 that all communities up to a distance of 15 kilometers from the border would be fully secured.[36] But the system's limitations were revealed during Operation Pillar of Defense. Aside from isolated instances in the Sderot area, when rockets fired from southern Gaza were indeed intercepted by Iron Dome– possibly due to the large distance that allowed the interception – Sderot and the Gaza perimeter communities were, for the most part, not actually protected. Though Iron Dome protected communities far from the border such as Beersheba, Ashdod, and Ashkelon, the protection was not thorough. The fact is that Operation Pillar of Defense ended before all the IDF's Tamir interceptor missiles had been launched. Nevertheless, it is easy to imagine what would have happened if the operation had gone on for another few days and the IDF had reached the "bottom of the barrel" in the inventory of defensive missiles. There is no question that both the government of Israel and the IDF command were forced to face very significant pressures to end the operation before all the missiles ran out. This surely would have affected any negotiations connected to ending the fighting. Even worse, if the fighting had not been stopped in time, it is easy to imagine how despondent Israelis would have been and what a great blow this would have been to their morale, in addition to the physical damage.

We cannot ignore the Property Tax report that presents the list of damage during the operation in cities protected by Iron Dome. Hundreds of buildings and cars were damaged. A report from the Israeli Police notes that sappers from the police in the southern region handled 109 rocket hits in populated areas. The conclusion is that the protection provided by the Iron Dome system was not sufficient.

The Skyguard system could be much more thorough than the Iron Dome system in defending against the threat from Gaza. The Gaza Strip has no strategic depth: its width, almost along its entire length, is about 7 kilometers, aside for its southern part, whose width is about 13 kilometers. Figure I shows the operational coverage of eight Skyguard systems placed around the Gaza Strip at a distance of about 1 kilometer from the border

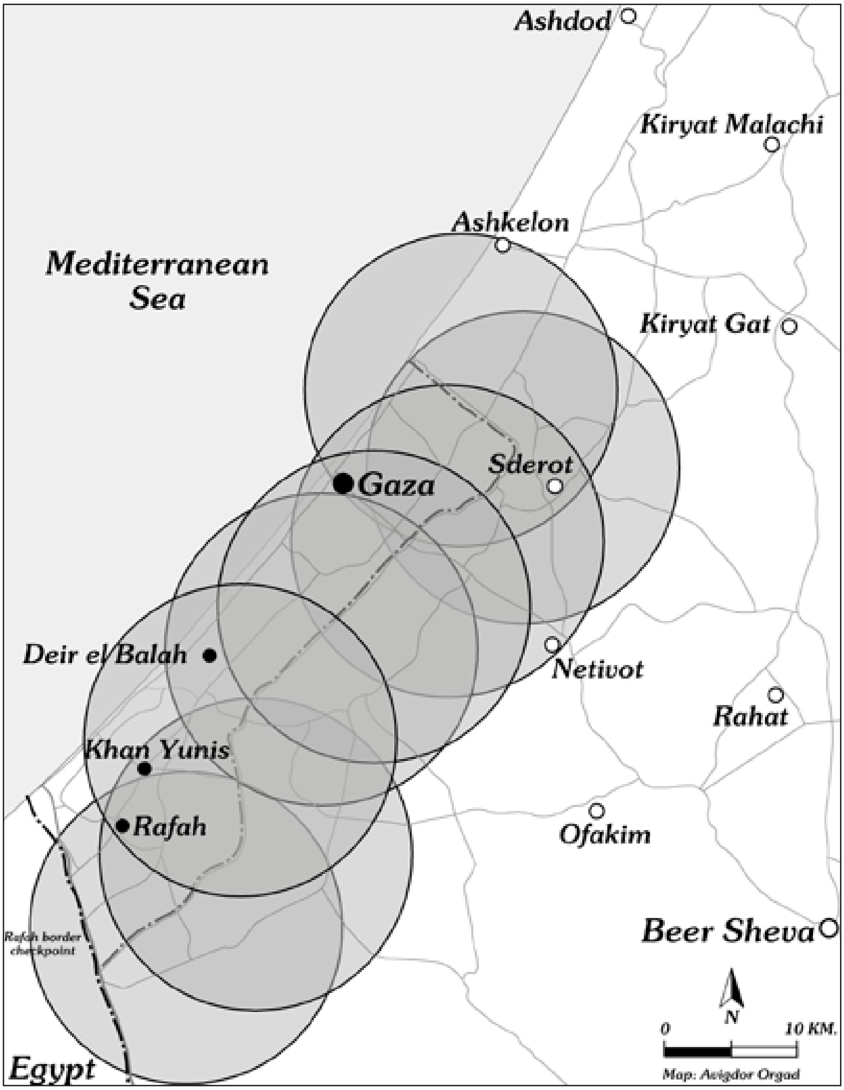


Figure 1. Operational Coverage of the Gaza Perimeter by Eight Skyguard Systems

(behind folds of land, in order to prevent direct fire on them). With the exception of a limited area, all launch points are covered by the Skyguard systems.

The Skyguard system does not require estimation processes. The vector to the target is received within one-two seconds from the moment the threat is fired, and will be destroyed within another two-three seconds, usually while still over the Gaza Strip and regardless of where it was originally directed.

Because of the short distances involved, the fire at Gaza perimeter communities is almost entirely flat-trajectory fire. Unlike the threat of Qassam 1, an enhanced Grad, with a range of 15 kilometers, usually reaches a maximum altitude of about 550 meters. This is under the typical cloud base, which begins at about 600 meters. The conclusion is that even in difficult weather conditions, the Skyguard systems will protect the Gaza perimeter communities. In fact, the laser systems surround the Gaza Strip with a kind of "defensive shield" that will intercept any threat fired from the strip at any target in Israel. This also includes the Fajr rockets, which have a range of about 70 kilometers.

The investment required for the incorporation of the Skyguard systems into Israel's security system is approximately 500 million dollars. Delivery would take about two years, and the system's integration with the Iron Dome systems could be elementary. The Iron Dome systems would be placed in locations that are relatively far from the border and which they are able to protect. The initial interception of all threats would be done with the Skyguard systems, which, as noted, have a perpetual magazine, and any threat that gets through, would be handled by the Iron Dome system. This combination would give optimal protection, and would provide the decision makers and government of Israel with breathing room to consider various decisions, knowing that the home front is well protected.

The Irrelevance of Defense Systems Based on Solid-State Lasers

Both the Nautilus and Skyguard chemical-laser systems are currently available and have proven capabilities. Postponing their implementation just because of the expectation for a more advanced solid-state laser has no basis in any technical reality.[37] Solid-state lasers also have a number of significant limitations. First, there is the limitation of output. The highest output that has been achieved with this technology – only about 100 kilowatts, which Northrop Grumman produced in February 2009 by means of plate technology – is about one-tenth of what is needed to intercept a missile. Reaching an output of 1 megawatt or more would require a technological breakthrough that does not appear to be feasible. Second, the efficiency of the laser system based on solid-state technology is only slightly greater than 10 percent. Creating a beam with the necessary output of at least 1 megawatt then requires an investment of some 9 megawatts of electric output, about 8 of which will turn into heat, which must be dispersed during lasing, that is, in two-three seconds. There is no cooling technology capable of doing this, and therefore, no chance to implement the system in the foreseeable future. Third, the system is hypersensitive to the effects of weather because of the length of the short wave on which these lasers operate (about 1 micron, vs. 3.8 microns for the Nautilus/Skyguard). Attenuation of the beam during passage through the atmosphere will be very great compared with the chemical-laser systems. In addition, there is a danger of blindness from reflected light, which stems from the same wavelength. These limitations are a technological barrier that will prevent implementation of a high-energy laser system based on solid-state technology.[38] There is no forecast that would indicate a date for completion of development of such a system, which would make it possible to protect population centers and strategic sites.

Conclusion

Precision ballistic weapons and cruise missiles have the potential to destroy critical infrastructures in Israel and to threaten the lives of many of its citizens. A system that is based on defensive missiles alone is not applicable to Israel's security needs because of the expenditures involved in procurement and due to the system's failure to meet some of the operational objectives required for basic protection. Nevertheless, the current attempts to build five layers of defense based on defensive missiles should continue in order to bring about an integration of these technologies with high-energy laser systems. An investment of about 4.6 billion dollars in Skyguard systems – 80 ground based and five airborne – continuing for about eight years would lead to creation of an integrated system that would possess all the components of a missile-defense system. This system would meet all the requirements of an ideal system by protecting against all threats at any time, under any type of weather, for as long as necessary, at minimal cost, and with significant savings.

The government of Israel should go back to the drawing board. It should recognize the advantages of the integrated system and act accordingly – especially toward the US government, with regard to restarting activity on the Skyguard system – lest Israel be forced to cope with a serious crisis in future conflicts.

Notes

[1] Amos Harel, "Chico Tamir Thinks Gantz Plan Could Lead to Disaster," *Ha'aretz*, July 18, 2013.

[2] Amir Rapoport, "Golani Guy," *Ma'ariv*, January 28, 2004.

[3] Zeev Klein and Hezi Sternlicht, "Matan Vilnai: We'll be Attacked with 1,000 Missiles a Day," *Israel Hayom*, June 3, 2011, http://www.israelhayom.co.il/site/newsletter_article.php?id=11489.

[4] State Comptroller, *Annual Report 59a for 2008* (Jerusalem: State Comptroller's Office, 2009), pp. 13-20.

[5] Yehuda Wegman, "Why Is It Hard for the IDF to Succeed?" *Maarachot* 419 (2008): 11.

[6] Gabriel Siboni, "From the Second Intifada through the Second Lebanon War to Operation Cast Lead: Puzzle Pieces of a Single Campaign," *Military and Strategic Affairs* 1, no. 1 (2009).

[7] Giora Eiland, "Operation Pillar of Defense: Strategic Perspectives," in *In the Aftermath* of *Operation Pillar of Defense*: *The Gaza Strip*, *November 2012*, ed. Shlomo Brom, Memorandum No. 124 (Tel Aviv: Institute for National Security Studies, 2012).

[8] Ran Dagoni, "Deputy Chief of Staff Benny Gantz: 'We'll Win Third Lebanon War; When We Take Horses out of Stable, Lebanon Will Be Hurting Badly,'" *Globes*, June 2, 2010, http://www.globes.co.il/news/article.aspx?did=1000563836.

[9] Gadi Eizenkot, "A Changed Threat? The Response on the Northern Arena," *Military and Strategic Affairs* 2, no. 1 (2010).

[10] Ofer Shelah and Yoav Limor, *Captives in Lebanon* (Tel Aviv: Yediot Books, 2007), p. 221.

[11] Klein and Sternlicht, "Matan Vilnai."

[12] Eizenkot, "A Changed Threat?"

[13] Amos Harel, "Major General Gantz: 'I'm Satisfied with Israel's Capability vis-à-vis Iran; We're in a Good Place, and We'll be in a Better Place,'" *Ha'aretz*, December 31, 2010, http://www.haaretz.co.il/news/politics/1.1238152.

[14] The scenario was formulated on the basis of all threats fired at Israel during the Second Lebanon War and Operation Cast Lead.

15 Letter from Magen LaOref ("Home-front Shield," a non-profit organization): "Anticipated Performance of Iron Dome," December 15, 2009

16 Yiftah Shapir, "Iron Dome: The Queen of Battle," in *In the Aftermath* of *Operation Pillar of Defense*: *The Gaza Strip*, *November 2012*, ed. Shlomo Brom, Memorandum No. 124 (Tel Aviv: Institute for National Security Studies, 2012).

17 Gadi Eizenkot, "The Characteristics of a Possible Conflict in the Northern Arena and the Home Front," Seminar in Memory of Soldiers Killed in Second Lebanon War, University of Haifa, October 30, 2010, http://www.youtube.com/watch?v=l0xkjirjvCI.

18 Uzi Rubin, "Iron Dome in Action: A Preliminary Evaluation," *Perspectives* 151, Begin-Sadat Center for Strategic Studies, Bar Ilan University, October 24, 2011, http://www.biu.ac.il/SOC/besa/perspectives151.html.

19 Noam Barkan, "They Reign Supreme," *Yediot Ahronot*, April 11, 2011.

20 Yuval Azoulay, "The Price in Blood: How Many Rockets Does It Take to Kill One Israeli?" *Globes*, April 27, 2012.

21 Isaac Ben-Israel interview with Yoaz Hendel, *Makor Rishon*, December 29, 2006.

22 Northrop Grumman presentation to Ministry of Defense, January 2007.

23 For purposes of redundancy, the intention is to have two Skyguard systems to protect each site. This would lead, inter alia, to the interception of twice as many threats. If the threat arrival rate is less than 1.5 seconds on average, all threats will be destroyed. See Table of Comparison: Performance and Cost.

24 Josef Shwartz, *2008 Multinational Ballistic Missile Defense Conference* (Honolulu: Northrop Grumman, September 2008).

25 Isaac Ben-Israel interview with Yoaz Hendel.

26 "ABL's Successful Shootdown," *DT Defense Tech*, February 12, 2010, http://defensetech.org/2010/02/12/abls-successful-shootdown/.

27 It should be noted that all the data and the assumptions presented above require a careful feasibility study that will also include flight tests.

28 Subrata Ghoshroy, "Coming Not So Soon to a Theater Near You: Laser Weapons for Missile Defense," *Bulletin of the Atomic Scientists*, November 1, 2011, p. 35.

29 See Table 1.

30 Yoav Zeitun, "Lapid Cuts Defense: 'Concerns about Adverse Effects on Tank Reinforcement,'" *Ynet*, March 28, 2013, http://www.ynet.co.il/articles/0,7340,L-4361962,00.html.

31 Superscript numbers refer to comments in table. For security reasons, no assessments of the capabilities of defensive missiles against missile volleys are presented.

32 Amos Yadlin, "Conclusion," in *In the Aftermath* of *Operation Pillar of Defense*: *The Gaza Strip*, *November 2012*, ed. Shlomo Brom, Memorandum No. 124 (Tel Aviv: Institute for National Security Studies, 2012).

33 Benjamin S. Lambeth, "Israel's Second Lebanon War Reconsidered," *Military and Strategic Affairs* 4, no. 3 (2012).

34 Amir Buhbut and Nir Yahav, "Gantz: We Must Continue to Attack with All our Strength, Step up the Pace," *Walla*, November 17, 2012, http://news.walla.co.il/?w=/551/2587039.

35 Shapir, "Iron Dome: The Queen of Battle."

36 Klein and Sternlicht, "Matan Vilnai."

37 Yosef Arazi, "The Skyguard System: The Only Means of Protecting Gaza Perimeter Communities from Rockets and Mortar Shells," *Magen LaOref*, October 16, 2012.

38 D. L. Carroll, "Overview of High Energy Lasers: Past, Present and Future," *42nd AIAA Plasmadynamics and Lasers Conference* (Honolulu: June 2011), AIAA Paper 2011-3101.

New Security Threats, Unilateral Use of Force, and the International Legal Order

Afeno Super Odomovo

The emergence of new security threats to the international community has led to a fundamental reevaluation of the contemporary international legal order. The events of September 11, 2001 in particular heralded the beginning of an age of terror, characterized by the fear that terrorist groups could acquire and use weapons of mass destruction (WMD) against their targets. The ensuing war against transnational terrorism and proliferation of WMD is a new type of warfare, posing unique threats and unparalleled security challenges to the international community. No doubt the war against terrorism incorporates a number of innovations into the existing international legal framework. One such innovation has to do with the rules regulating the use of force in inter-state engagements. In spite of the normative *jus ad bellum* doctrines of self-defense and necessity, there have been instances where the imperatives of political, humanitarian, and strategic considerations leave no choice but for states to act outside the law. Unilateral and unauthorized use of force has the potential to undermine the universal system of collective security and erode the current international legal framework, as it sets a bad legal precedent. This paper places contemporary provisions for the use of force in their historical and legal contexts, examines the extent to which they diverge from the current international legal order, and considers whether they create the need for a new international legal order.

Key Words: international legal order, weapons of mass destruction, terrorism, preemptive self-defense, use of force

Afeno Super Odomovo is a junior research fellow at the French Institute for Research in Africa (IFRA-Nigeria) and Assistant Project Coordinator, Nigeria Watch/IFRA-Nigeria, University of Ibadan, Nigeria.

Introduction

The circumstances under which the use of force is justified in international law have remained at the forefront of political and legal debates since early times. In this context, the creation of the United Nations resulted in the most fundamental modification of international law of the twentieth century, by outlawing the use of force in international relations. The prohibition against the use of force is a treaty-based rule that is enshrined in both the UN Charter and treaties of regional scope such as the North Atlantic Treaty and the Inter-American Treaty of Reciprocal Assistance. These provisions are the most fundamental *jus cogens* norm of contemporary international law that encompasses the primary value of collective security.

However, contemporary international law has been inundated with new security problems. In the past few years, the international community has witnessed an upsurge in threats of terrorism and has realized the danger posed by the production and proliferation of WMD. Most importantly, the changing nature of armed conflict has exposed the international community to new security challenges, as inter-state conflicts and threats from failed states and armed non-state actors have been proven to affect the law regulating the use of force. These new security threats have led to demands for a fundamental reevaluation of the relevance of the current international law. The thinking among some members of the international community is that existing international laws are hopelessly outdated in light of new security threats, and they therefore call for a radical overhaul of the current international legal order.

This paper examines the use of force under customary international law and the legal framework established at the end of the Second World War to protect the international community from threats to international peace and security, and the capacity of this framework to respond to threats that were not contemplated by the drafters of the UN Charter. In particular, it examines the relevance of the existing international legal order in the face of new security threats and the recent tendency to resort to unilateral and unauthorized use of force. The paper first explores the use of force under customary international law. Second, it considers the use of force under the UN Charter. Third, the paper examines the prospect of a new international legal order in the face of a changing world. Fourth, the nature of the international legal order in the post-9/11 world is examined.

Preemptive Use of Force under Customary International Law

The conduct of war is customarily governed by a large body of international humanitarian law. This body of law evolved over centuries and draws greatly on past conventions, particularly the Geneva and Hague Conventions.[1] While the Geneva and the Hague Conventions were primarily associated with *jus in bello* (laws of war), the focus of customary international law was mainly on the rules relating to *jus ad bellum* (justification for war). The rules governing the use of force together with other fundamental humanitarian principles have long provided the framework for formally organized international relations and coexistence of states.

Until contemporary times, customary international law regarded the right to use force and the power to go to war as essential attributes of statehood and, consequently, the right of every state. As Charles Cheney Hyde, a foremost expert in international law put it, "It always lies within the power of a state to endeavor to obtain redress for wrongs or to gain political or other advantages over another, not merely by the employment of force, but also by direct recourse to war."[2] Within this context, customary international law also recognized self-defense as a legitimate basis for the use of force. Hence, Hyde affirmed:

> An act of self-defense is that form of self-protection which is directed against an aggressor or contemplated aggressor. No act can be so described which is not occasioned by attack or fear of attack. When acts of self-preservation on the part of a state are strictly acts of self-defense, they are permitted by the law of nations, and are justified on principle, even though they may conflict the... rights of other states.[3]

Apparently, customary international law recognized the use of force against an aggressor under the self-defense provision even before the aggressor actually attacks. Traditionally, the recognized right of a state to use force for purposes of self-defense include the preemptive use of force.

The precedent classically cited by states and international law scholars for preemptive self-defense was the formulation of the right of preemptive attack by then United States (US) Secretary of State Daniel Webster in connection with the famous *Caroline* incident. During the 1837 insurrection against British rule in colonial Canada, the ship *Caroline* was believed to be conveying supplies to insurgents on Navy Island who were attacking British vessels on the Canadian riverside. British forces crossed the border into the US, seized the *Caroline,* set her on fire, and sent her over the Niagara Falls. The British government claimed to have acted in self-defense because the US had not prevented the rebellious activities on its territory. The US protested, and in the course of the diplomatic exchanges that followed, Secretary of State Daniel Webster articulated the two conditions essential to the legitimacy of pre-emptive use of force under customary international law.

Webster asserted that an intrusion into the territory of another state can be justified as an act of self-defense only in those "cases in which the necessity of that self-defense is instant, overwhelming, and leaving no choice of means and no moment for deliberation."[4] In another remark Webster asserted that the force used in such circumstances has to be proportional to the threat.[5] Therefore, under customary international law the preemptive use of force for self-defense is limited such that it has to be necessary and proportional,[6] and for an act to be necessary, any measure short of armed force (diplomatic efforts, economic sanctions, embargoes, and so on) would have to be, or have proven to be, inadequate.

The Use of Force under the United Nations Charter

The rules that govern the use of force for preemptive self-defense encompass a number of treaties, international agreements, and conventions, the most fundamental of which is the UN Charter, as the source of the organizing principles of the existing international legal order. The prohibition on the use of force is a fundamental principle of contemporary international law and is enshrined in the UN Charter. The Charter creates a system of collective security in which the Security Council is authorized to "determine the existence of any threat to the peace, breach of the peace, or act of aggression," and to "decide what measures shall be taken... to maintain international peace and security."[7] The Charter obliges member states to "settle their international disputes by peaceful means"[8] and to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[9]

Although it nominally outlaws the use of force in international relations, the UN Charter recognizes the right of nations to use force for the purpose of self-defense. Article 51 of the Charter provides: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[10] The right acknowledged under this article is traditionally referred to as the "inherent right" of every state to self-defense. Nevertheless, the language of Article 51 indicates that resort to self-defense is intended to be an interim measure, permitted "until the Security Council has taken measures necessary to maintain international peace and security."[11] Unfortunately, the collective decision-making process of the Security Council has been rendered ineffective as a result of strategic voting among its permanent members.

In particular, the veto right of permanent member states has rendered the Security Council largely limited in authorizing the use of force under Article 42 of the Charter. Nevertheless, there are exceptions to the veto right of the permanent members of the Security Council. Specifically, UN General Assembly Resolution 377 of 1950, titled "Uniting for Peace," empowers the General Assembly to make appropriate recommendations to members for collective measures, including the use of force "if the Security Council, because of lack of unanimity of the permanent members, fails to exercise its primary responsibility for the maintenance of international peace and security."[12]

Read literally, Article 51's articulation of the right of self-defense apparently precludes the preemptive use of force by individual states or groupings of states and reserves the right to authorize such use of force exclusively for the Security Council. Measures taken in self-defense, according to this understanding, are legitimate only after an armed attack has already started.[13] Unfortunately, to interpret Article 51 literally, "is to protect the aggressor's right to the first strike."[14] Clearly it would be a betrayal of the purpose of the Charter to oblige a state, in the face of potential radiological, chemical, biological, or nuclear attack, "to allow its assailant to deliver the first and perhaps fatal blow."[15] This predicament reflects the fact that the position of the UN Charter concerning the condition under which the use of force is legitimate has been overtaken by new security threats and modern weapons technology.

Indeed, both the literal and nominal interpretations of Article 51 are controversial. The crux of the controversy is whether the phrase "if an armed attack occurs" rules out preemptive self-defense. That is, does international law as embodied in Article 51 of the UN Charter confer on states an anticipatory right of self-defense? In an attempt to avoid this controversy over nominal and literal interpretations, some scholars assert that Article 51 recognizes the "inherent right of individual or collective self-defence" as it was developed in customary international law prior to the adoption of the Charter and preserves it intact.[16]

In essence, contemporary international law has never satisfactorily clarified whether any form of anticipatory defense is allowed under the self-defense clause (Article 51) of the UN Charter. However, in both theory and practice it has generally been accepted that states do not have to wait to be attacked before responding with force if there is overwhelming evidence of an impending attack.[17] This position has a foundation of support in the words of Elihu Root, US Secretary of War (1899-1904), who once defined self-defense as "the right of every sovereign state to protect itself by preventing a condition of affairs in which it will be too late to protect itself."[18] Therefore, unlike customary international law, the Charter regime of international law is limited by its lack of clarity regarding anticipatory self-defense.

This weakness has created a problem of compliance with the Charter's provisions and has consequently led to instances of unilateral and unauthorized use of force by states in the face of new security threats. In the case of the 2003 US-led intervention in Iraq, military force was used without explicit UN Security Council authorization, yet the US and its allies justified their action as legitimate on the basis of Iraq's non-compliance with UN Security Council Resolution 1441 of 2002, which had found Iraq to be in "material breach" of its disarmament obligations.[19] Some Security Council members, such as China and Russia, "were strongly of the view that this resolution did not provide automatic authority for the use of force, and that it would be for the Council (and not individual member states) to decide whether Iraq was in breach of the provisions of Resolution 1441."[20] Indeed, the UN Charter's provisions regulating the use of force give rise to a general problem of compliance in the face of modern security threats.

Technological Advancement and Modern Security Threats

Technological revolutions in military affairs over the last fifty years have fundamentally transformed the nature of armed conflict at a pace beyond the capacity of current international law to handle. The introduction of WMD, ballistic missiles, the Internet, and information warfare has reduced the time necessary to carry out deadly attacks and greatly multiplied the security costs of non-anticipatory defense strategies. According to William Bradford:

> [Breakthroughs in] technological development, proliferation of WMD, and radicalization of international relations have so enhanced the magnitude of the threats to civilian populations and the speed with which enemies can attack that the *Caroline* standard for 'imminence,' developed in the pre-WMD era, is no longer sufficient to simultaneously restrain states while guaranteeing their survival.[21]

In other words, the emergence of more elusive and deadly threats posed by the convergence of terrorism and WMD has rendered dangerous such restrictive standards of international law as "imminence" because the threat of nuclear attack is always imminent. Biotechnological advancement has made it easier to enrich nuclear materials and informal networks facilitate the transfer of the technology required to convert nuclear materials into WMD. In 2004, there were reports of illicit transfer of nuclear weapons technology to Pakistan, North Korea, and possibly Iran and Libya through the informal networks of a Pakistani scientist, Abdul Qadeer Khan.[22] Moreover, unlike state actors, non-state armed groups can detonate WMD without fear of a devastating nuclear retaliation. In June 1990, the rebel group Tamil Tigers seized cylinders of chlorine from a paper mill and released the gas into a fort controlled by the Sri Lankan Armed Forces.[23] Evidently the existing international nuclear nonproliferation regulatory regime cannot handle modern nuclear and biotechnological security threats.

International Law and the Use of Force in the Post-9/11 World

The US reaction to al-Qaeda's terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001 was expressed in terms of recourse to military force. The US and its allies initiated military actions against al-Qaeda's terrorist training camps and the military installations of the Taliban regime in Afghanistan in exercise of its inherent right of individual and collective self-defense.[24] Although the invasion was widely perceived as legitimate on the basis of self-defense under the UN Charter,[25] there was no specific UN Security Council resolution authorizing the invasion. Consequently, the invasion set a legal precedent capable of undermining the provisions of existing international law regulating the use of force among states.

It has been argued by various international jurists and legal luminaries[26] that the law relating to the use of force is concerned mainly with state relations, and that its scope does not include the activities of non-state entities. Confusion over the status of non-state actors and the responsibility under the Charter of states on whose territory non-state aggressors are located has been exploited by certain states to launch military attacks against other states. The problem emanating from this development centers mainly on the question of whether contemporary international law recognizes an attack by a non-state armed group to be an armed attack within the scope of Article 51, which would justify the use of force against that group and any third state in which the group is located.

It is remarkable that most of the forceful counter-terrorist measures by the US against other states after 9/11 have received considerably less opposition from the international community. The UN Security Council expressed its unanimous support for the US-led military intervention against the Taliban regime in Afghanistan. In Resolutions 1368 and 1373 of 2001,[27] the Security Council reaffirmed the inherent right of individual and collective self-defense against non-state actors. But then, mere failure to condemn the US should not be taken as acceptance of a legal doctrine permitting the use of force in these circumstances. Nevertheless, it indicates a trend of increasing tolerance, which has recently resulted in recognition of states' right of self-defense against non-state armed groups.

Moreover, use of force is contemplated beyond circumstances of self-defense and extends to a number of situations that do not fit within the existing regime governing the use of force in international law. For instance, the US extends the law regulating the use of force a step beyond the doctrine of pre-emptive self-defense. The proposed Bush doctrine of preventive war claims the right of self-defense "even if uncertainty remains as to the time and place of the enemy's attack."[28] In other words, advocates of the doctrine (especially the US) justify the use of force that is not necessarily based on imminent attack but forms part of a long-term risk prevention strategy. This was basically the argument put forward by the US for attacking Iraq in 2003.[29]

In response to the 9/11 attacks, the US has pushed for a revision of outmoded standards for evaluating the lawfulness of self-defense by using the Bush doctrine, which is adapted to the capabilities and objectives of today's adversaries. The Bush doctrine is a signal that the US and other states, like Israel, will no longer wait for threats to fully materialize but will take preventive action when necessary to protect their citizens. The Bush doctrine of preventive war is indeed a "militant and highly transformative assertion"[30] that clearly transcends the bounds of anticipatory self-defense.

Closely related to the Bush doctrine is a recent conceptualization of imminence that supports US drone strikes. A confidential Department of Justice white paper justified the lawfulness of the US government's use of deadly force in a foreign country against a US citizen who is a "senior operational leader of al-Qa'ida or an associated force" if such an individual poses an "imminent threat of violent attack against the United States" and his or her "capture is infeasible," provided such use of deadly force is "conducted in a manner consistent with applicable law of war principles."[31] Though not a legal document, this white paper justifies governmental authority to carry out extrajudicial killing of citizens who pose an imminent threat of violent attack against the country.

Historically, there are a number of instances of military aggression in the guise of anticipatory self-defense, including the Japanese invasion of Manchuria in 1931 and the German invasion of Poland in 1939. Perhaps, justifying their actions as anticipatory self-defense rather than aggression, states like China, North Korea, Pakistan, and members of the Arab League might claim this legal entitlement to attack Taiwan, South Korea, India, and the state of Israel, respectively, in light of the volatile nature of their geopolitical regions. For instance, in response to the September 2004 school siege by Chechen terrorists in southern Russia, the argument put forward by the Russian government for the use of military force against the terrorists was that the strikes were carried out in order to liquidate terrorism in the region.[32]

In particular, the terrorist incidents of 9/11 have created a new world order characterized by unilateral and unauthorized use of force in interstate relations and have "set in motion a significant loosening of the legal constraints on the use of force."[33] The strong support for the US-led extraterritorial use of force against Afghanistan by members of the international community, coupled with heightened concerns about transnational terrorism, has reinforced the authority of the UN Security Council to approve the use of force for individual or collective self-defense.

Although the initial invasion of Afghanistan in October 2011 was conducted without specific UN Security Council authorization, the language of Resolutions 1368 and 1373[34] enabled the US to claim legitimacy for its actions. This is a clear demonstration that international law is changing in response to contemporary threats facing the international community.

International Law in a Changing World: Towards a New Legal Order

The existing rules of international law regulating the conduct of war were drawn up when war was primarily the business of nation-states. Moreover, the UN system was established to regulate inter-state relations, "including the declaration of war between states."[35] But the current security situation is more complex than that of previous decades. Now, more states as well as non-state armed groups capable of inflicting large-scale harm are seeking to procure and produce weapons of mass destruction, thereby threatening both regional and global security. Chemical, biological, radiological, and nuclear weapons that are within the reach or in the hands of terrorist groups are among the greatest security threats in contemporary times. Thus the problem is that "in today's security climate, yesterday's exceptions are becoming today's rules."[36]

The evolving security environment necessitates new rules for regulation of the use of force in self-defense. New developments in the international environment require reformulation of the laws of war and, in fact, the entire international legal system to reflect the changed nature of security threats, in order to incorporate contemporary realities into the international legal framework. As it is continuously faced with new situations, the current international legal regime is constantly challenged, and international law is gradually being modified to incorporate these changes. These new developments include the emergence of international terrorist organizations; the increasing number of non-state actors in armed conflicts, such as drug cartels, rebel groups, and pirates; and the growing number of failed states that threaten international peace and security.

Non-State Actors and International Law: The UN system was undoubtedly created to regulate the use of force and relations between nation-states. The Charter regime did not recognize non-state entities as actors on the international scene. In fact, self-defense was justified only against states. Accordingly, the target was specified: the aggressor state. And the purpose was clear: to repel the aggression.[37] Conversely, contemporary security threats are fuzzy, "altering the definition of vulnerabilities, threats, and dangers and catapulting a variety of non-state actors into strategic visibility."[38] In the current security environment, threats that used to originate from interstate disputes now emerge from intrastate conflicts sponsored by non-state actors outside the territorial state.

Today, terrorism is considered one of the greatest threats to international peace and security. The fact that terrorist groups are non-state actors, and are difficult to pinpoint in a particular state, necessitates the establishment of legal means of determining the responsibility under international law of the state on whose territory such terrorist groups operate. Accordingly, the doctrine of the "Responsibility of States for Internationally Wrongful Acts"[39] provides legal clarifications on the responsibility of failed states and non-state actors in international law. In addition, secondary legislation – the UN Security Council resolutions – partly fills this legal vacuum by establishing that terrorists may be considered agents of governments that harbor them.[40] Nevertheless, these rules still leave unanswered the question of whether the war on states that sponsor terrorism is legal under the self-defense clause of the UN Charter.

The apparent void in the UN Charter in relation to non-state actors pertains basically to non-state actors that are not in any way established or partly governed by states. The situation is complicated by the absence of structures that enable diplomatic relations among some non-state actors.[41] Non-state actors such as drug cartels, pirates, and terrorist organizations pursue goals that are arguably illegal and pose security threats not only to the territory from which they operate, but also to the wider international community.[42] For instance, recent developments off the coast of Somalia have resulted in a UN Security Council resolution (Resolution 1816 of 2008) describing pirate activities as a threat to international peace and security.[43] This resolution is a confirmation that threats from non-state actors can be of such magnitude as to constitute a security threat to the international community, even though piracy was hitherto considered a mere criminal act on the high seas.

Rogue States, Failed States, and the International Legal Order: The concepts of rogue states and failed states have emerged in the lexicon of international relations, with both branded as threats to international peace and security because these states are largely seen as vulnerable to terrorist networks.

The existence of failed or failing states has further complicated the problem of identifying and holding responsible those states that sponsor terrorism. Rogue states and failed or failing states constitute a great threat to international peace and security as they serve as breeding grounds for terrorists and similar groups, and such states are very likely to sponsor and fund terrorist activities against their enemies, whether real or imagined.

UN Security Council Resolution 748 of 1992 affirmed that "every state has the duty to refrain from instigating, assisting, or participating in terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when such acts involve a threat or use of force."[44] But can a failed or failing state be held responsible for the actions of terrorist groups within its territory? Put differently, what is the obligation of a failed state under international law? For instance, can Somalia, an African failed state, be held responsible under international law for its inability to prevent actions of terrorist groups who hold sway and operate in parts of the country? Does the inability of the state of Somalia to stop these acts constitute acquiescence to these terrorist activities? Limitations inherent in the existing international legal framework in relation to non-state entities have made this question difficult, if not impossible, to answer within the scope of the Charter framework.

Although the UN's core principles of non-interference, respect for the territorial integrity of member states, and prohibition of unilateral use of force "provide the cornerstone for international order,"[45] international law has other provisions[46] that recognize the rights and responsibilities of failed states and non-state actors. International human rights and humanitarian laws recognized failed states and non-state actors as members of the international legal system with corresponding rights and responsibilities. The notion that all actors are bound by international humanitarian law was supported by the UN Security Council with reference to Liberia and Somalia.[47] However, human rights laws may be suspended in a failed state in the absence of legally recognized governmental authority.

Indeed, it would be a questionable practice to hold a failed state responsible for the violation of its international obligations during a period of total collapse. Hence, the "Responsibility of States for Internationally Wrongful Acts" regards the conduct of non-state entities as acts of a state only if these entities are exercising "elements of governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of these elements of authority."[48] Although the doctrine provides legal clarifications regarding the problem of attribution in a failed state, it is applicable only where a functioning state structure and governmental authority exist.

Collective and Unilateral Humanitarian Intervention: The duty of other states to protect civilian population in states where the government poses a humanitarian threat to its citizens has emerged as a challenge to state sovereignty under international law.[49] In particular, unilateral humanitarian intervention to relieve a population from gross human rights abuses is a big challenge to state sovereignty in customary international law. This is a considerable security challenge given the fact that such intervention mostly results in armed confrontations between the intervening state and the territorial state. Apparently, the 1999 NATO military intervention in Kosovo for humanitarian reasons broke new legal ground and resulted in the debate about the need for a new humanitarian war doctrine. Subsequently, the principle that military interventions to achieve humanitarian objectives did not require the UN Security Council's specific authorization seems to have been established.[50]

According to the Independent International Commission on Kosovo,[51] NATO military intervention was "illegal but legitimate" because it was undertaken without specific authorization from the UN Security Council but was justifiable as legitimate on humanitarian grounds and on the basis of the understanding that all diplomatic avenues were exhausted before the invasion. Yet Article 2(7) of the UN Charter states, "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require Members to submit such matters to settlement under the present Charter." That is to say, "No other State and no international organisation may scrutinise what is happening inside a State except with the full consent of the territorial State."[52]

Even though the UN Security Council passed a resolution authorizing "all necessary measures to protect civilians under threat of attack,"[53] the NATO military intervention in Libya to protect civilians from human rights violations by military forces loyal to former dictator Muammar Qaddafi exceeded the authorization of the Security Council resolution. Moreover, the legality of this military intervention is questionable because NATO implemented the resolution not only for civilian protection but "to justify pursuing general support for the rebels and attacking Libya government military assets."[54] In consideration of the controversy surrounding NATO military intervention in Libya, what circumstances justify external intervention under international law? Put another way, at what point is unilateral use of force for humanitarian objectives legal? Clearly, these are very difficult questions, partly because – aside from international law and the doctrine of Responsibility to Protect (R2P)[55] – economic, political, and strategic interests have evolved as important factors justifying the use of force on humanitarian grounds.

Recent military actions "all bend or break the law of war as it has traditionally been understood."[56] New security threats have made major world powers regard international law as secondary to projection of military power. Naturally, states that are skeptical about the ability of international law to regulate state and non-state behavior will hardly worry about the damage to the international legal system. The cumulative effect of these developments is apparently that the Charter's provisions regulating the use of force are no longer regarded as binding international law.[57] It is becoming difficult to determine where diplomacy ends and where the use of force becomes necessary.

Conclusion

Although state recourse to preemptive use of force has occurred before 2001, the recent resort to anticipatory use of force by states is largely a development that resulted from the fear of threats posed by terrorism and the lethality of WMD and, especially, the 9/11 terrorist attack. The threats of WMD are linked not only to changes in the international environment, but also to the process of economic globalization, which has reduced the effectiveness of traditional nonproliferation regimes. International law as embodied in the UN Charter is concerned more with the maintenance of peace and security and less with the legal rules of the use of force. The Charter's provisions regarding the use of force are legally obscure. Thus, in the process of responding to new threats, international law is often amended by state practice in violation of the current international legal framework. Although these changes still lack the status of binding international law, as they are at the level of individual state practice, they have set a legal precedent to which other states would lay claim in the future.

Indeed, violations of international law by states serve as a legal precedent and have the capacity to indirectly reform the law, particularly when the violator receives widespread support for its actions. However, the international community has to be careful to ensure that such renovations do not, in seeking to address new security challenges, shift the balance too far in another direction, in order not to become a destabilizing force in the current delicate constellation of international affairs. The use of force, except in self-defense, when explicit and confirmed threats have been recognized, or in pursuit of other legitimate ends recognized as such by the larger international community, often instills insecurity and resentment of the existing legal order by less powerful states.

On the whole, without meaningful reforms incorporating a more flexible and holistic view of states' right of self-defense against terrorism and WMD, international law regulating the use of force will become irrelevant in the face of emerging security threats. Nor will a gradual modification of the existing body of the law of war work, as the entire legal structure is in danger of collapsing under the weight of new threats. Likewise, the recognition of a new legal order will not necessarily prevent the emergence of new threats to the international community. Moreover, it is difficult to predict the effect of a new legal order on future international stability. To be effective and binding, the rules of a new legal order must have enough built-in flexibility for states to exercise force when necessary without undermining or destroying the credibility and legitimacy of the international legal order.

Notes

[1] Tomas Valasek, "New Threats, New Rules: Revisiting the Law of War," *World Policy Journal* 20, no. 1 (Spring 2003): 17-24.

[2] Charles Cheney Hyde, *International Law Chiefly as Interpreted and Applied by the United States,* Vol. 3 (Boston: Little, Brown & Co., 1945), p. 168.

[3] Ibid., p. 234.

[4] John Bassett, "Letter from Secretary of State Daniel Webster to Lord Ashburton of August 6, 1842," *A Digest of International Law* Vol. 2 (1906), p. 412.

[5] David Ackerman, "International Law and the Preemptive Use of Force against Iraq," *Congressional Research Service Report* No. RS21314, April 11, 2003, p. 2.

6 See "Legality of the Threat of Use of Nuclear Weapons," Advisory Opinion of the International Court of Justice, *I.C.J. Reports* (1996), p. 245, para. 41, http://www.icj-cij.org/docket/files/95/7495.pdf.

7 UN Charter, Article 39.

8 Ibid., Article 2(3).

9 Ibid., Article 2(4).

10 Ibid., Article 51.

11 Ibid.

12 UN Doc. A/RES/377 (V) A (1950), http://www.kentlaw.edu/faculty/bbrown/classes/IntlOrgSp07/CourseDocs/VUnitingforPeaceResolution.pdf.

13 "Legality of the Threat of Use of Nuclear Weapons," *I.C.J. Reports*, p. 245.

14 Humphrey Waldock, cited in Guy Roberts, "The Counterproliferation Self-Help Paradigm: A Legal Regime for Enforcing the Norm Prohibiting the Proliferation of Weapons of Mass Destruction," *Denver Journal of International Law and Policy* 27, no. 3 (1999): 483.

15 Ibid., p. 513.

16 Bruno Simma, *The Charter of the United Nations: A Commentary* (Oxford: Oxford University Press, 1994), p. 51.

17 Valasek, "New Threats, New Rules: Revisiting the Law of War," p. 18.

18 Elihu Root, "The Real Monroe Doctrine," *American Journal of International Law* 8, no. 3 (1914).

19 UN Doc. S/RES 1441 (2002), http://www.un.org/depts/unmovic/documents/1441.pdf.

20 Justin Morris and Nicholas Wheeler, "The Security Council's Crisis of Legitimacy and the Use of Force," *International Politics* 44, no. 2/3 (2007): 214-31.

21 William Bradford, "The Duty to Defend Them: A Natural Law Justification for the Bush Doctrine of Preventive War," *Notre Dame Law Review* 79, no. 4 (2004).

22 Michael Laufer, "A.Q. Khan Nuclear Chronology," *Proliferation Brief* No.8, September 7, 2005, http://carnegieendowment.org/2005/09/07/a,-q.-khan-nuclear-chronology/6jq.

23 Jonathan Tucker, "The Future of Chemical Weapons," *The New Atlantis* (Fall 2009/Winter 2010): 3-29.

24 Dan Balz and Bob Woodward, "America's Chaotic Road to War," *Washington Post*, January 27, 2002.

25 UN Charter, Article 51.

26 See Michael Byers, "Terrorism, the Use of Force and International Law after 11 September," *International Relations* 16, no.2 (2002): 155-70; Thomas Franck, "What Happens Now? The United Nations after Iraq," *American Journal of International Law* 97 (2003); Antonio Cassese, "Terrorism Is Also Disrupting Some Crucial Legal Categories of International Law," *European Journal of International Law* 12, no. 5 (2001): 993-1001; Michael Glennon, "How War Left the Law Behind," *New York Times*, November 21, 2002.

27 See UN Doc. S/RES 1368 (2001); UN Doc. S/RES 1373 (2001), http://www.un.org/en/sc/documents/resolutions/2001.shtml.

28 Devika Hovell, "Chinks in the Armour: International Law, Terrorism and the Use of Force," *UNSW Law Journal* 27, no. 2 (2004): 398-427.

29 Ibid.

30 Franck, "What Happens Now? The United Nations after Iraq."

31 "Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al-Qa'ida or An Associated Force," US Department of Justice White Paper, 2011 (released by NBC February 4, 2013), http://users.polisci.wisc.edu/kmayer/408/020413_DOJ_White_Paper.pdf.

32 Nicholas Kralev, "Russia Vows Pre-emptive Terror Hits," *Washington Post*, September 9, 2004.

33 Byers, "Terrorism, the Use of Force and International Law after 11 September," p. 165.

34 See note 27.

35 Valasek, "New Threats, New Rules: Revisiting the Law of War," p. 18.

36 Ibid., p. 19.

37 Cassese, "Terrorism Is Also Disrupting Some Crucial Legal Categories of International Law."

38 David Kennedy, "International Symposium on the International Legal Order," *Leiden Journal of International Law* 16 (2003): 841.

39 Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10 (2001), http://www.un.org/documents/ga/docs/56/a5610.pdf.

40 Valasek, "New Threats, New Rules: Revisiting the Law of War," 18.

41 Cherif Bassiouni, "The New Wars and the Crisis of Compliance with the Law of Armed Conflict by Non-state Actors," *Journal of Criminal Law and Criminology* 98 (2008): 711-810.

42 Ian Brownlie, *Principles of Public International Law*, 6th ed. (New York: Oxford University Press, 2003), pp. 713-714.

43 UN Doc. S/RES 1816 (2008), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1816(2008).

44 UN Doc. S/RES 748 (1992), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/748(1992).

45 Morris and Wheeler, "The Security Council's Crisis of Legitimacy and the Use of Force," p. 222.

46 Universal Declaration of Human Rights, UN Doc. A/819 (1948), http://www.un.org/en/documents/udhr/; see also Responsibility of States for Internationally Wrongful Acts.

47 UN Doc. S/RES 788 (1992) https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/788(1992); see also UN Doc. S/RES 814 (1993), https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/814(1993).

48 Responsibility of States for Internationally Wrongful Acts, Article 9.

49 Bradford, "The Duty to Defend Them: A Natural Law Justification for the Bush Doctrine of Preventive War"; see also Anthony Arend, "International

Law and Rogue States: The Future of the Charter Framework," *New England Law Review* 36 (2002).

50 Valasek, "New Threats, New Rules: Revisiting the Law of War," p. 21.

51 Independent International Commission on Kosovo, *The Kosovo Report: Executive Summary,* 2000, http://www.cfr.org/kosovo/independent-international-commission-kosovo-kosovo-report-executive-summary/p25962.

52 Ingrid Detter, *The Law of War*, 2nd ed. (Cambridge: Cambridge University Press, 2000), p. 34.

53 UN Doc. S/RES 1973 (2011), https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1973(2011).

54 Ben Smith, Vaughne Miller, and Arabella Lang, "Military Interventions: Some Comparisons," *Commons Library Standard Note*, August 29, 2013, http://www.parliament.uk/business/publications/research/briefing-papers/SN06715/military-interventions-some-comparisons.

55 *The Responsibility to Protect*, Report of the International Commission on Intervention and State Sovereignty, 2001, http://responsibilitytoprotect.org/ICISS%20Report.pdf.

56 Valasek, "New Threats, New Rules: Revisiting the Law of War," 18.

57 Michael Glennon, "The Fog of War: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter," *Harvard Journal of Law* 25, no. 2 (2002): 539-59.

Cyber Defense from "Reduction in Asymmetrical Information" Strategies

Guy-Philippe Goldstein

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

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

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

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

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

Introduction: A Regional Scenario

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

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

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

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

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

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

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

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

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

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

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

Perfect deterrence theory posits that "response in kind" is an optimal strategy.[3] It demonstrates that the defender has a credible retaliatory threat. At the same time, it signals that Country X is not necessarily seeking escalation – what Huth describes as a "firm-but-flexible" negotiation style.[4] Additionally, not to commit to full-fledged escalation but to engage in firm response allows opening up options without exercising them. This is the position most favored by politicians as well as financiers. It is also an optimal situation with regard to the decision laws of cybernetics. But in the current predicament for Country X, response in kind is not possible. First, there is a major obstacle: Country X does not know against whom to respond in kind. It is faced with an attribution issue.[5] But even if it knew with certainty, Country X would still face a second major obstacle: it may not know exactly how to respond in kind.

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

At this stage, there are no good retaliatory options for Country X. If attacks have reached certain damage thresholds and Country X feels otherwise threatened by its geopolitical situation, then it may want to intimate to neighboring countries that attacks will have consequences. It will then try to respond in kind imperfectly by highlighting its most capable and credible non-cyber, kinetic threat, for example by flexing muscles through a show of air or ground forces. This measure will have adverse diplomatic consequences if attribution is not well established, and it could backfire if cyber attacks continue, actually raising the credibility stakes for Country X now that it has exposed its conventional forces. However, if a cyber attack does not seem to exact too high a price and if its origins remain efficiently obfuscated, then Country X may want to defuse tensions and lower the stakes. Difficulties could be attributed to non-state or technical origins. Then Country X could accept the help from Country B via the software security firm. Of course, as noted, this help would come at a price.

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

An Evaluation Framework

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

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

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

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

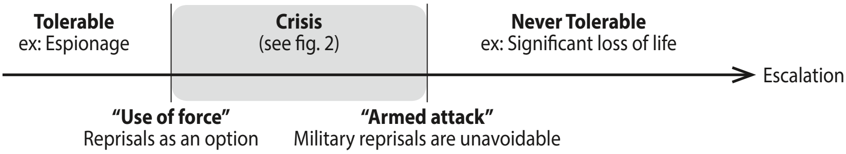
What is never tolerable, what would automatically elicit military reprisals, is action leading directly to significant loss of life among non-combatants. In general, this action would be interpreted as a voluntary breach of the laws of armed conflict with regard to *jus ad bellum* as expressed in the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

With regard to large-scale violence capabilities, some weapons are essential: first and foremost the nation's survivable second strike force, but also any weapon systems deployed so widely that malfunctions would significantly hamper the defense of the sanctuary. These include the specific networked communication systems and sensors required for the proper use of those weapons. They also include the intergovernmental communication systems necessary for the head of state and staff to command and control these capabilities, as well as for heads of states to communicate. Such provisions were agreed upon by the two superpowers during the Cold War. The 1971 Accident Measures Agreement and Hotline Modernization Agreement established protection of satellite communications essential to US-USSR communications in times of crisis, as well as the communication facilities for missile warning systems.[18] In addition, attempts at first responder forces and at medical assets that limit significant loss of life constitute red lines. Elements reflecting this understanding were agreed upon by Russian and American diplomats in 2011 and were included in the *Tallinn Manual*, as a way to more generally align the conduct of cyber operations with the current laws of armed conflict.[19] These measures include assets and communication systems for command and control for medical and first responder forces, including with the head of state. Protecting the communication systems does mean preserving data from external corruption: if data cannot be protected then, de facto, the communication systems as means of sending the right instructions are being sabotaged.

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

In this framework, those effects that are never tolerable hurt so severely that they are easily and blatantly recognizable as such. In the *Tallinn Manual*, attacks yielding such effects are construed as "armed attacks."[23] At this threshold, military reprisals are a certainty. If the identity of the attacker is known, then it is subject to the idiom of military action established among states. The rules of this idiom apply, ensuring what Thomas Schelling has called the diplomacy of violence.[24] States are entering a game of escalation, from conventional retaliation to potentially strategic reprisals. Cyber weaponry becomes an adjunct to other weapon systems.[25] States can credibly respond in kind with non-cyber weaponry. This will bring clarity and recognizable accents to this dialogue, as illustrated in figure 1.

Figure 1. Decision Framework with Tolerance for Effects



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

In the area between the tolerable and the never tolerable exists the territory of crises and its many shades of gray. The harm is conspicuous enough to be construed as a use of force but its severity is not elevated enough to identify it with certainty as an armed attack.[30] According to the International Court of Justice, as cited in the *Tallinn Manual*, "not every use of force rises to the level of an armed attack."[31] The crisis can be kept outside of the public eye – a default option to avoid tying one's hands too much within the unchartered waters of cyberspace. Still, the crisis will be real. Uncertainty here has many sources. The never-tolerable effects may not be observable yet, but they could be perceived as an imminent outcome: if online banking problems spread and last a few weeks, would they lead to financial panic? Could losses be easily recovered? The same questions apply if the energy grid is breached. On Day 2, it might be hard to tell. Additionally, not only might direct effects be hard to assess; the meaning of the enemy's military actions in cyberspace, its "virtual mobilization," might also be difficult to evaluate. The last point is critical because, following the rules of warfare first described by Sun Tzu, surprise is the key to victory[32]: the better warrior will not create patterns or precedents. His or her moves will be difficult to evaluate.

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

a. What is not benign, but reflects self-limitation in escalation: the attack is limited in intensity and cannot be construed as threatening non-combatants; it is limited in scope: only one type of targets is being attacked; it is limited in its temporal dimension: it happens only once or a few times, or has a date of termination. These attacks can be labeled as limited.

b. What is not benign and can be construed as potentially escalating: the intensity or scope of the attack seems not to be self-constrained and could be escalating; or there is repetition and acceleration along the temporal dimension, without a distinct termination date. These attacks can be labeled as escalating attacks.

For example, if GlobalWorm was recognizably set to alter the functioning of only very specific software or equipment, if the software or equipment specifically targeted by GlobalWorm was only for military use or dual-activities, if the effects did not lead to significant collateral damage among civilian personnel or civilian life, and if GlobalWorm had a recognizable date of expiration – for example with digital certificates protecting it and it was due to expire at a certain time – then the GlobalWorm attack against Country X would be a limited attack. This does not seem to be the situation in the Country X case. Effects are not limited and circumscribed to specific equipment, but are escalating. They are also hard to recognize: what may be the secondary effects of 48 hours without online banking?

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

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

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

An Evaluation Process

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

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

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

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

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

Attribution

Because cyberspace consists of three pillars – hardware (calculation, memory, or communication devices), software, and brainware[39] – intelligence work must investigate and develop hypotheses for each of these three sources. Clues as different as IP traffic patterns, styles of coding, and methods of actions should feed an attribution matrix. It should also include classical human intelligence on hackers themselves and their political sponsors. These investigative activities should adhere to the best practices in elucidation, with emphasis on deductive methods applied to intelligence as suggested by Ben-Israel.[40] As one methodology in the context of general intelligence works suggests,[41] attribution hypotheses could be laid out in different buckets (for example, "Hypothesis #1: Country Y is the aggressor"; "Hypothesis #2: Country Z..."). Then, empirical data refuting each hypothesis could be set against each bucket. Stacking data against attribution hypotheses would be a first step toward identifying which country is most liable to be the originator.[42] This would require advance identification and simulation of the multiple models of necessary preparations required to launch a massive cyber attack for each country. These models of preparation would of course include additional defensive hardening efforts and obfuscation efforts. Ideally, then, deductive A/B tests in the manner of controlled experiments launched against possible culprits could be set to confirm or infirm attribution hypotheses. For example, taking a page from the strategies used by fictional character George Smiley, by simulating unexpected effects of the malware, the true place of origination could inadvertently reveal a surge in unease and embarrassment.[43] The detection of this unease would help with attribution.

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

In cyberspace, truth is power, as it is for any other information domain, such as traditional intelligence.[44] The means and methods of establishing a quasi-incontrovertible truth are key instruments of power. As such, they can become instruments of influence. One day, the cyber-diplomatic scene could resemble the civilian internet mainstream scene, where some of the largest search engines or reference content providers (such as Wikipedia) are already vying for the highest relevance in terms of content. After all, the most important feature of any information system is the ability to distinguish the right signal.

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

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

A crucial initial observation is appropriate here: in addition to forcing attribution via the arsonist principle, this approach can actually establish it formally. In diplomatic terms, it can deny the offender the option of plausible deniability. Establishing attribution is as much an intelligence investigation as a diplomatic process. Other nations must be convinced. First, the credibility of the truth is best established when other observers (or testers) can confirm or infirm the attribution hypothesis. This social process is well established, from the two-witness rule governing the trials of treason as early as the Elizabethan era in England,[48] prefiguring Hooper's rule on concurrent testimony[49] to modern statistics where confidence in predictions is increased by the number of observations. To create a public test is to force other nations and their people to become observers. Second, a diplomatic process ensures higher coordination and thus strengthens the cyber blockade required to pressure suspicious states. The strength of the blockade is vital for the threat to be capable. If it can be significantly evaded, as Western powers managed to do during the Berlin Crisis of 1948 against the Russian blockade, then the threatening country fails.[50] If the blockade cannot be evaded, then the threatened country is forced to decide between escalation and backing down – and if the stakes are too high, it may back down as Russia did during the Cuban Missile Crisis. In addition, carrying out the attribution process first with close allies, then with a wider group of nations, might foster goodwill, rapprochement, and greater understanding toward the defending state. That, in turn, frees up political margins of maneuverability if the defending state is to move toward additional diplomatic, economic, or military sanctions beyond cyberspace and a cyber blockade. It lends further credibility to what is essentially a compellence strategy, as described by Schelling: "a threat intended to make an adversary do something."[51] Suspected states are compelled to collaborate or else they will continue not only to suffer from the cyber blockade, but also to single themselves out. In that new context, countries wanting to prove their goodwill will genuinely cooperate. Perhaps they may even share their own intelligence with regard to attribution, as a further proof of goodwill. Countries that do not cooperate will de facto reveal their true intent.

In addition, cooperation is all the more easily compelled when it means that cooperating countries do not have to lose face. Taking a page from Rattray and Healey's model of public health for cyber security,[52] the metaphor of World Health Organization (WHO) investigation teams at times of pandemics can be used. National governments do not have to be nominally accused – they do not have to be held initially responsible for the pandemics. Officially, the blame is placed on the malware or the nefarious teams of hackers behind it. Using the public lack of attribution for the sake of the compellence action, the coalition of defenders can then request the heads of the suspected states to cooperate. A cyber blockade can still be implemented, analogous to WHO quarantining regions or countries during pandemics. Thus the cost of not cooperating still weighs on the offenders – and it will grow as other states cooperate and the offending state becomes ever more isolated. Conversely, the cost of cooperating is lessened because there is no loss of face. And still, there is a genuine threat, that is, a cost for having launched the operation in the first place: finally accepting cooperation, the offending capabilities (servers, codes, hackers) will be publicly branded. They will be rendered inoperative. Ongoing cooperation – and the additional intelligence it will provide – will help maintain this calculus. This is the end game. Defecting nations are forced to cooperate again. Their investment in defection capabilities is nullified. But there is not necessarily the audience cost attached to backing down. This makes renewed cooperation acceptable, and thus potentially stable. Additionally, the difficult task of a formal, public attribution, requiring a very high degree of certainty because of its public format, is rendered unnecessary.

Strategies and Requirements for Joint Compellence

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

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

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

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

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

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

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

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

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

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

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

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

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

Notes

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

2 This article can be viewed as a follow-up to the issues of destabilization in cyberspace discussed in Guy-Philippe Goldstein, "Cyber Weapons and International Stability," *Military and Strategic Affairs* 5, no. 2 (2013): 121-39.

3 See Frank C. Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge Studies in International Relations, 2000), pp. 296-301.

4 Paul K. Huth, *Extended Deterrence and the Prevention of War* (New Haven: Yale University Press, 1988), cited in Zagare and Kilgour, *Perfect Deterrence*, pp. 296-301.

5 For further details on this issue and introductory literature, see for example Goldstein, "Cyber Weapons and International Stability."

6 For further details on this issue and introductory literature, see for example Goldstein, "Cyber Weapons and International Stability."

7 William W. Kaufmann, *The Requirements of Deterrence* (Princeton: Center of International Studies, Princeton University, 1954). See also the discussion in Fred Kaplan, *The Wizards of Armageddon* (Stanford: Stanford University Press, 1983), pp. 193-200.

8 See discussion in Goldstein, "Cyber Weapons and International Stability" with reference to Schelling's definitions of red lines in Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), p. 137.

9 See discussion in Goldstein, "Cyber Weapons and International Stability," with reference to the concept of "curve of credibility" in Carey B. Joynt and Percey E. Corbett, *Theory and Reality in World Politics* (Pittsburgh: University of Pittsburgh Press, 1978), p. 94-95.

10 See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), p. 88: "The international Group of Experts achieved no consensus as to whether non-destructive but severe cyber operations satisfy the intensity criterion." See also pp. 82-83, comments #14 and #15.

11 See Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," in *The Virtual Battlefield: Perspective on Cyber Warfare*, eds. Christian Czosseck and Kenneth Geers (Amsterdam: IOS Press, 2009) for a discussion of cyber warfare in the context of effect-based warfare. More explicitly, the *Tallinn Manual* states that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (Rule 11) and that "a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death

to persons or damage or destruction to objects" (Rule 30). The ensuing discussion does highlight that "'acts of violence' should not be understood as limited to activities that release kinetic force. This is well settled in the law of armed conflict. In this regard, note that chemical, biological or radiological attacks do not usually have a kinetic effect on their designated target, but it is universally agreed that they constitute attacks as a matter of law." See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013). What matters is the direct effect on civilian populations or on properties, whatever the way – kinetic or not – these direct effects have been caused.

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

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

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

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

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

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

18 See Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between The United States of America and The Union of Soviet

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

19 See Karl Frederick Rauscher and Andrey Korotkov, *The Russia-US Bilateral on Critical Infrastructure Protection: Working Towards Rules for Governing Cyber Conflict* (New York: East-West Institute, 2011). See also Part II, Chapter 3 ("The law of armed conflict generally"), in particular Rule 20 ("Applicability of the law of armed conflict"), and Chapter 4 ("Conduct of hostilities"), in particular Rule 29 ("Civilians") and Section 3 ("Attacks against persons"), in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

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

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

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

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

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

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

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

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

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

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

[30] See Rule 11 in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

[31] See Rule 13, comment #5, citing the *Nicaragua* judgment, para. 191, in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 55.

[32] "All warfare is based on deception" quoted in Sun Tzu, *The Art of War*, transl. Samuel B. Griffith (New York and Oxford: Oxford University Press, 1963), p. 66.

[33] Herman Kahn, *On Escalation* (London: Pall Mall Press Ltd., 1965).

[34] The observation of effects should be complemented by a technical analysis of the malware itself. However, this could take too much time. For example, Stuxnet was identified by Virusblokada in June 2010 but only significantly analyzed by November 2010. See Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32. Stuxnet Dossier* (Symantec, 2010). Hence the requirement for up-to-date information alerts from all military and civilian activity centers to a cyber intelligence collection point will make it possible to reinterpret cyber incident data points to form a coherent national picture for use by national security institutions.

[35] See Rule 30, comment #5, in Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, p. 106.

[36] See John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (1995).

[37] See James N. Mattis, "USJFCOM Commander's Guidance for Effects-based Operations," *Joint Force Quarterly,* no. 51 (2008); see also criticism of USJFCOM decision by USAF officers in Paul M. Carpenter and William F. Andrews, "Effects-based Operations Combat Proven," *Joint Force Quarterly*, no. 52 (2009).

[38] On the rise of corporate APIs, see Robin Vasan, "Business Process API-ification: The LEGO Promise Fulfilled," *GigaOm*, October 6, 2012, http://gigaom.com/2012/10/06/business-process-api-ification-the-lego-promise-fulfilled/ and Mark Boyd, "Getting C-Level Buy-In: Demonstrating the Business Value of APIs," *ProgrammableWeb*, September 11, 2013, http://blog.programmableweb.com/2013/09/11/getting-c-level-buy-in-demonstrating-the-business-value-of-apis/.

[39] See discussion in Goldstein, "Cyber Weapons and International Stability," for main components of cyberspace.

40 Isaac Ben-Israel, *Philosophie du renseignement* (Paris : Editions de l'Eclat, 2004).

41 Ibid.

42 This example is directly inspired by the 1973 Yom Kippur War post-mortem analysis described in Ben-Israel, *Philosophie du renseignement*.

43 To reveal the identity of "Gerald," the mole working for the USSR, Smiley has a message sent to the head of the "Circus" that forces "Gerald" to seek an emergency meeting with his Soviet handler at an already identified safe house. This is the test that allows Smiley to identify "Gerald" while breaking into the safe house. In John Le Carré, *Tinker Taylor Soldier Spy* (London: Hodder & Stoughton, 1974).

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

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

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

47 Ibid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

69 By the mid-2000s, the mood had been reversed on AI and there was talk of a "spring" in AI. See for example John Markoff, "Behind Artificial Intelligence, a Squadron of Bright Real People," *New York Times*, October 14, 2005.

70 See the discussion on rules relaxation and lengthening the game in Zagare, *The Dynamics of Deterrence*, pp. 48-56.

71 See the discussion on the "shadow of the future" in Axelrod, *The Evolution of Cooperation*, p. 13.

72 See Goldstein, "Cyber Weapons and International Stability."

73 Zagare and Kilgour, *Perfect Deterrence*, pp. 293-96.

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 6000 words (including citations and footnotes). Please include an abstract of 120 words and a list of up to 10 keywords. Previous issues of the journal may be accessed on the INSS site at: http://www.inss.org.il/.

For further information, please contact:
Daniel Cohen
Coordinator, *Military & Strategic Affairs*
Cyber Warfare Program
Tel: +972-3-6400400/ext. 488
Cell: +972-50-5772338
danielc@inss.org.il