# Cyber, Intelligence, and Security

Volume 1 | No. 2 | June 2017

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

# Cyber, Intelligence, and Security

Volume 1 | No. 2 | June 2017

## Contents

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

# Cyber, Intelligence, and Security

The purpose of *Cyber, Intelligence, and Security* is to stimulate and enrich the public debate on related issues.

*Cyber, Intelligence, and Security* is a refereed journal published three times a year within the framework of the Cyber Security 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.

**Editor in Chief:** Amos Yadlin
**Editor:** Gabi Siboni
**Journal Coordinator:** Hadas Klein
**Asst. Coordinator:** Gal Perl Finkel

**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

*Cyber, Intelligence, and Security* is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

ISSN 2519-6677 (print) • E-ISSN 2519-6685 (online)

# Imposing and Evading Cyber Borders: The Sovereignty Dilemma

Alessandro Guarino and Emilio Iasiello

The world's perception of cyberspace has evolved from the libertarian promises of the 1990s to the current situation, where nation-states seek to reestablish their sovereignty. This paper explores the history of our conceptions of cyberspace, from the enthusiastic utopias culminating in the so-called "declaration of independence of cyberspace" to the technological underpinnings and the legislative steps being taken by today's governments to assert more control. It will address efforts in the West and East to resolve diverse, multi-faceted, and ongoing challenges that range from supporting open cyberspace to being able to heavily monitor the threat activities and the various state and non-state actors operating in cyberspace. The paper will highlight the technical and regulatory difficulties in establishing borders in cyberspace, as well as the corresponding policy consequences, and reveal how actors are evading borders by using various techniques such as cryptography and data havens, to name a few. The main takeaway is that the balkanization of cyberspace is not only a reality, but also a course that may be too difficult to reverse, and raises the question of how do open societies balance sovereignty with individual freedoms in cyberspace? A proposal is offered, drawing from examples in which the sovereignty of nation-states is limited and in which borders are not a factor, such as the international body of law regulating global commons.

Alessandro Guarino is the principal consultant of StudioAG, an Italian information security and cybersecurity consultancy firm. Emilio Iasiello is a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, as well as the private sector.

**Keywords:** cybersecurity, internet governance, international relations, cyberwarfare, cyber conflict, China, privacy

## Introduction

The worldwide diffusion of a unique digital information-carrying infrastructure over the last decade of the twentieth century has deeply changed every facet of life and society, from social interactions to the global economy. Availability of internet access is—at least in developed nations—considered almost a "given" right. Cyberspace, however, is not a natural phenomenon, but a historical and political one, and as such, is subject to influence by social and political entities. Among political entities, nation-states are of paramount importance. The US government has been instrumental in the development of the internet since its inception, beginning as a research project of the Department of Defense Agency for Advanced Projects (DARPA). The international community, as well as several supranational organizations, are also interested in the internet's regulation and use. Recently, for very solid political and strategic reasons, NATO declared cyberspace an autonomous warfare domain, endorsing a position not universally shared among scholars. Since the internet's opening to commercial entities in the 1990s, private sector actors, ranging from network operators to service providers, have achieved a prominent position in the regulation debate itself—a borderless cyberspace that offers advantages to internet companies, but that would invariably put them into conflict with sovereign states. On the other side of the spectrum, individual citizens (e.g., operators, content providers, citizens, experts, journalists, or simply users) would form their own perception of what cyberspace is now and how (and if) it should be governed and regulated.

## History

The conceptions of cyberspace cannot be properly understood without a solid understanding of its historical background. It should not sound strange studying a "history" that is only decades old; rather, the rapid rate of change and developments in the cyber realm makes looking back not only possible, but necessary to begin the debate on solid grounds.

The sudden and widespread diffusion of the internet was the result of a series of converging political and technical factors. It is likely that none of the actors involved predicted exactly what would happen and how disruptive an innovation the internet was going to be. In a short period, the internet transitioned from being a mostly academic and military network, connecting tens of sites and usable only via command line interfaces, to a world-wide resource accessed by millions of people using a point-and-click interface—the web browser.

Voice telecommunications in the 1970s and 1980s were a world apart from the data networking world, involving computer-to-computer data exchange and communications. Telecommunications companies (Telcos) operating in this market enjoyed monopolistic or quasi-monopolistic dominant positions in their markets and the stable cash-flow that went with them. In the United States, however, with its tradition of anti-trust legislation dating to the nineteenth century, an ongoing process of deregulation and competition took place that included breaking existing monopolies and companies, with AT&T being a prominent example. The direct effect of this process was a push for innovation in the infrastructure. In addition to the liberalization of the telecommunication market, which enabled the United States to expand, to some extent, to the rest of the developed world, the other important policy was the decision by the US Federal Communications Commission to reclassify "data processing"—machine-to-machine digital communications—as a "value-added" enhanced service in contrast to the basic voice services.[1] The consequence was the creation of an unregulated and open market for digital services, even beyond trade barriers.[2] At the time, information services made up a tiny fraction of telecommunication companies' revenues, allowing this market to remain non-regulated. This was probably seen as a small price to pay compared to voice-services. Those policies paved the way for a global digital information network of networks.

Alongside high-level policies, several technical aspects contributed to the explosion of the internet to include the way data communication is managed on the internet. The network was based on packet-switching technology, allowing two nodes to exchange information without having to establish a fixed, or even predetermined path between them. The data is divided into small-size "packets" and transmitted separately, possibly even on different paths, and in a different order than the original one. The whole is rebuilt at the destination by the networking software. This is in sharp

[1] Milton L. Mueller, *Network and States* (Cambridge: MIT Press, 2010).

[2] Ibid.

contrast to the circuit-switched technology of the telephone networks, where a dedicated “circuit”—or path—is established each time a communication is initiated between two nodes. The packet-switching architecture allowed for decentralized management because the routing decisions about packets could be made at the local level without the need for detailed information on the network. This was coupled with the fact that the particular communication protocols used at the time—the TCP/IP suite—were standardized and public, an engineering design choice made decades before the rapid growth of the internet by allowing whole pre-existing networks to be added. In fact, until then, the word “internet” meant just that; the interconnection of two or more computer networks (later it acquired the capital “I” and became the Internet). Also among the technical contributions, the maturation of the free software movement facilitated the availability of several robust elements, which—also for economic reasons—contributed to the building of many internet companies and servers; GNU/Linux and the apache web server are two prominent examples. Not to be underestimated is also the introduction of the xDSL technologies, which brought relatively high bandwidth connections to the public.

## The Tension of Governance

The debate on governance has polarized around two opposite views. On one hand, there is the view that— as an entity—cyberspace is completely separated from the “physical” world, where information flows freely and neither distance nor ordinary law is binding. The opposing view is that each nation is responsible for its sovereign piece of the global internet and is justified in implementing any legal mechanisms in place to ensure the security of online activities traversing its network space. To date, there is neither consensus nor compromise on these opposing factions, leaving the status quo for the time being; nevertheless, how the internet should be governed remains hotly contested.

According to the hypothesis that cyberspace stands apart from the physical world, nation states would not and could not regulate anything that happened on the internet, meaning that cyberspace is not subject to “ordinary” laws, sovereignty, or borders. This sentiment is articulated memorably by John Perry Barlow, who states, “Governments of the Industrial world, you weary giants […], I come from Cyberspace, the new home of Mind […], You have no sovereignty where we gather."[3] Supporting this view, the technical traits of the internet are what gives the system its independence from the physical world and the sovereignty of nation states: decentralization (thanks to IP protocols) and the easily transportable nature of information. The infrastructure allows and favors the birth and growth of network organizations composed of peers and relationships completely independent of physical locations, jurisdictions, and borders. In these social constructs—be they civil society groups, special interest clubs, or social networks—the internal organization of the peers depends only on the information's flow. The basic tenet of what can be called "cyber libertarianism" is that there is no need for sovereign regulations and laws in cyberspace. Unfortunately, the power of networked organizations can also be used to establish criminal or terrorist groups who leverage the relative anonymity that cyberspace permits. The transnational nature of these groups enables members to function cohesively, despite operating from different geographical locations and jurisdictions.

The second viewpoint concerns state sovereignty in cyberspace. This argument contends that not only should the technological components of the internet be subject to state authority, but also the information that originates, crosses through, or enters its sovereign digital space. The potential for creating and maintaining transnational social networks with ease, flexibility, and relative anonymity has been seen as a threat both to state sovereignty as well as national security itself. This perception has increased since the beginning of this century, given the ongoing confrontation with organized terrorist networks; terrorism in Europe and America, however, is not the only powerful motivation behind the sovereign position. The social movements that led to the "Color Revolutions" and "Arab Spring" are indicative of what can happen if information goes unchecked. Moreover, nation-states have demonstrated a natural tendency to maintain and extend the limits of their power; cyberspace—with its potential as a channel for communications and warfare—is a natural extension of state power. Indeed, the control of financial fluxes and even currency policy is a trait of sovereignty under attack.  Opponents of sovereignty see it as a legitimizing vehicle for more authoritarian regimes to increase monitoring and control of their citizens.

[3] John Perry Barlow, "A Declaration of the Independence of Cyberspace," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge: MIT Press, 2001).

Dissidents and political oppositionists have often been the target of strict internal monitoring, and the West's perceived existential threat of terrorism has been the raison d'être of the surveillance state. Semi-democratic or autocratic states do not even need that kind of justification for imposing borders.

The tension between the two viewpoints informed the whole debate about "internet governance" in the 1990s, and especially since the beginning of the twenty-first century. Formally, it led to two governance models: one in which cyberspace is perceived as another international regime to be regulated by inter-state treaties and organizations— the International Telecommunication Union (ITU) is a prominent example—and the other advocating a network governance model (multi-stakeholder is the preferred term in official EU parlance). A governance network, formed by both government and non-governmental actors, is widely held to be the most appropriate for the internet and is actually the way that cyberspace currently works.[4] The vision of cyberspace as a global common is attractive but misleading: the cyber domain is entirely artificial and no part of it exists outside of some sovereignty (even deep-sea cables fall under a whole body of regulations and treaties dating back to the nineteenth century).[5]

Underscoring this tension is the fact that the network governance model was already in place when states began to realize the potential of cyberspace and to reestablish traditional sovereignty. The Internet Corporation for Assigned Names and Numbers (ICANN) and the decentralized management of the Domain Name System (DNS) are striking examples. Decentralized governance made the internet incredibly successful at various levels, and it is hard to argue to the contrary.

## State of the Art

Well into the twenty-first century, nation-states have been gaining control over cyberspace. This policy view is widespread outside Western countries where internet and cyberspace are perceived to be dominated by the "cyber hegemony" of the United States. Admonishing cyber hegemony may be a propaganda tool for China, but the United States and its close allies—especially

[4] Mueller, *Network and States*, ch. 3, p. 31.

[5] Alessandro Guarino, "Cyberspace Does Not Exist," *Strange Loops,* January 15, 2015, http://www.studioag.pro/en/2015/01/la-nuvola-non-esiste/.

their security agencies—have consistently held a quasi "neocolonial" attitude towards cyberspace. Patent examples include the development and deployment of cyber weapons: the effects of Stuxnet; the attack on the Belgian telecom company, Belgacom by British intelligence; the claim to worldwide validity of US laws and the disregarding of other jurisdictions; and the injunction requiring Microsoft to relinquish data stored in one of its data centers in Ireland. Viewed from this perspective, liberal democratic state practices do not appear different from those of less democratic countries. Moreover, sometimes they can be contradictory; for instance, attempts to create a "Digital Single Market" without borders inside the European Union go hand-in-hand with the creation and enforcement of external borders, in order to avoid perceived or real dumping practices by companies outside the European Union, e.g., tax evasion.

*Imposing Borders*

State policies and actions aimed at establishing and enforcing borders in cyberspace can meaningfully be classified by considering two variables. The first variable considers whether an action is "overt" or "covert." The use of the term "covert" here is somewhat loose, comprising in a strict sense the meaning of both "covert" and "clandestine"; where the first terms implies concealing the source, the second does not. The second intersecting variable considers whether policies are technical in nature or not; that is, legislative or political. The policy of overt non-technical state efforts is an attempt to bring internet governance back under state control, directly or through inter-governmental organizations. Other overt actions are those deriving from the physical nature of cyberspace. All network devices (servers, routers, cable backbones, satellite stations) are located in the sovereign territory of a nation-state and are subject to its laws, or well-developed international law in the case of transoceanic submarine cables. While it is difficult to monitor and control data flow, laws and regulations can be created and enforced on the physical side of the "cloud." Overt political actions can also enable overt technical actions, by supplying them with legal justification (at least for the country in question). China's so-called "Great Firewall" is a clear example. Policy decisions created a whole arsenal of technical measures bent on reestablishing China's sovereignty over its "national" portion of cyberspace. These range from deep packet inspection and packet filtering of the perimeter routers, to the blocking and blacklisting of websites, to the manipulation of the DNS inside China, as well as many others. Simply, control is easy at the physical level, but more difficult at a slightly higher level, such as with the TCP/IP protocol and routing. Contrary to a physical cable, packet-switching technology makes it hard to control its path (e.g., which national territories it crosses). The covert side of an ideal matrix classification comprises the technical level where states race to militarize global networks in an effort to gain the virtual "high ground" in order to steal information in the classic style of espionage and to be prepared for a futuristic "cyberwar." Readiness also means being able to defend the critical networks of a nation against intrusions. Examples of covert, non-technical measures are the monitoring of content on social networks and elsewhere online by intelligence and security agencies. Generally, covert policy decisions of the interested government enable the control of the information flow by internal security agencies. Another relevant example of covert, non-technical means is the "moral suasion" exerted by governments on private Internet Service Providers (ISPs) and other network operators in order to ensure their collaboration in controlling the information flow (for instance by installing government-operated interception equipment on their premises).[6]

### *Evading Borders*

States have several motivations for wanting cyberspace to either remain unobstructed and unhindered, or to restrict it with more control, oversight, and monitoring. States may naturally seek to evade borders whether seeking to promote commerce, communication, steal secrets, or disrupt systems. The legal environment, or lack thereof, is one key way for states to maintain the status quo.

Countries currently are working to define acceptable behavior in cyberspace. For example, the recent 2015 G-20 meeting resulted in senior-level representatives pledging not to engage in cyber economic espionage in support of their respective commercial interests.[7] Yet despite promising platitudes, cyber espionage remains an attractive means of engaging in information theft and in the surveillance of friends and foes alike. The

[6] James Bamford, *The Puzzle Palace* (New York: Penguin, 1982), pp. 302–305.

[7] Emilio Iasiello, "G20 - No Commercial Hacking by Anyone," *Dead Drop,* January14, 2016, http://deaddrop.threatpool.com/g20-no-commercial-hacking-by-anyone/.

ultimate result from this pact may be that states will need to obfuscate more carefully their activities, rather than cease them altogether. As governments seek to bolster economic ties with one another using cyber as a facilitating agent, the very cyber boundaries that countries like China and Russia want to solidify become increasingly difficult to distinguish. This leaves states in the unenviable position of trying to defend their respective shares of the internet while trying to increase their political and economic ties with global partners.

### *Technologies Facilitate Border Evasion*

There is no accepted global definition of cyberspace. The US Department of Defense defines cyberspace as a "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures."[8] Russia prefers to use the term "information space" instead of cyberspace. The term "information space" is broader and more inclusive than the American term, which focuses on the network architecture and processes that occur in the digital domain. In contrast, Russia identifies information space as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself."[9] Similarly, China views the information space holistically. The Chinese definition of it is as follows: "The main function of the information space is for people to acquire and process data . . . a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases and information, forming a 'landscape' huge, interconnected, with different ethnic and racial characteristics of the interaction, which is a three-dimensional space."[10] Despite their differences, all three definitions refer to the networked aspects of the cyber domain, which is completely

[8] US Department of Defense, *Joint Terminology for Cyberspace Operations -Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, and the Directors of the Joint Staff Directorates* (November 2010).

[9] Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English" (Tallinn: Fifth International Conference on Cyber Conflict, 2013).

[10] Emilio Iasiello, "Are Cyber Weapons Effective Military Tools?" *Military and Strategic Affairs* 7, no. 1 (March 2015): 27–28.

human-made. Such a complex environment is bound to include human error, among other vulnerabilities. Those who helped design this network over subsequent decades focused on the technical challenges of moving information quickly and reliably and did not anticipate that the internet's own users would ultimately use the network to attack one another.

While attack and exploitation efforts do not have to be advanced to be successful, the more proficient actors have demonstrated the ability to script unique tools and exploits against vulnerabilities and maintain persistence and invisibility in their operations. The following are various technical techniques through which actors evade the notional cyber borders of a nation-state:

*Encryption:* Actors leverage encryption to mask the data that they harvest and exfiltrate. In some instances, they hide it in innocent-looking files (steganography). Other tactics involve compression (reducing the size of files without removing information); chunking (breaking down data into smaller parts so that it better blends into normal traffic); and obfuscation (converting characters to hex code so that data can avoid detection). By encrypting the data, actors make it difficult for the exploited organizations to know what kind of information was stolen, thereby hindering post-breach investigative and recovery response as well as attribution efforts.

*Onion Routing*: Although there is some debate whether the Onion Router (Tor) is completely anonymous, it remains a popular way through which actors conduct their operations. The strength of Tor rests in the fact that it is theoretically impossible to know which computer requested the traffic, as a computer may have either initiated the connection or may just be acting as a relay to another Tor node. The Tor client picks a random path through Tor nodes to its ultimate destination. In this regard, Tor is a popular tool for users to bypass restrictions and censorship controls in a given country, as much as it is for hostile actors. An incident in 2014 demonstrated that the Tor network was leveraged for exploitation activity: a rogue Tor node was used to launch cyber espionage attacks on European governments.

*Pluggable Transports:* Pluggable transports disguise Tor traffic to look like traffic from other common services such as HTTPS or Skype, and to look like benign traffic by transforming the Tor traffic flow between the client and the bridge.

*Virtual Private Networks (VPNs) and Proxies*: VPNs and proxies shield users by encrypting all activity to and from a computer. As long as the computer remains connected to a VPN, the network operators will not have access to traffic (e.g., sites visited). Similarly, proxies are used as intermediaries between the client and the server, eliminating the need for direct communication between the two parties. They provide some level of enhanced security in protecting the identity of a browsing computer.

### *The Tribulations of Cyber Diplomacy*

The diplomatic environment for cyberspace continues to be a work in progress, a situation that favors hostile activity. The impasse in critical areas has left the legal environment in limbo; states continue to evade borders without any international legal repercussions and struggle to find consensus on definitions and key legal issues—such as cyber warfare and security terminology—while avoiding nation-state responsibilities. The same extends to cyber sovereignty. China, among others, continues to promote its cyber sovereignty as an extension of its natural sovereignty, a right afforded to them under the UN charter. The United States, as well as its allies to some extent, believes that the internet—as an interconnected global platform—should remain open. It must be noted that while this is an official US position, different views and cyber strategies exist within the US government itself, sometimes at odds with each other.

Internet governance is another major area of contention. At present, no single organization influences how the internet expands, which technologies are used, or what rules govern the global network. China and Russia would prefer an international government organization—such as the ITU (part of the UN system)—to oversee and manage all internet activities. In April 2016, India aligned with this position. The debate is important as both sides continue to try to find allies to put their positions at the forefront. The United States—at least officially—prefers a multi-stakeholder approach that includes not just governments, but also the private sector, academia, civil society, and the technical community.[11]

A third legal area that remains in flux concerns the definition of information weapons. In 2011, China and Russia proposed banning the use of all information weapons and related technologies in their initial code of conduct proposal to the UN General Assembly. The subsequent 2015 revision removed the

[11] US Department of State Fact Sheet, “Internet Governance,” August 2015, https://www.state.gov/documents/organization/255010.pdf.

term, as it implied the potential use of information as a subversive element for inciting civil instability as had occurred during the Arab Spring. The United States has traditionally been opposed to outlawing offensive cyber weapons. The leading Department of State representative for cyber issues does not believe that conventional military or diplomatic treaties can work in cyberspace, preferring the development of "norms" instead.[12] This is at odds with the results of ongoing research by legal scholars at the invitation of the NATO Cooperative Cyber Defense Center of Excellence.[13]

Even among "friendly" nations, finding common legal ground is difficult to achieve. Fundamental differences in the legal underpinnings of privacy between the United States and the European Union led to the repealing of the "Safe Harbor" agreement on data transfer between the two sides. The new "Privacy Shield" framework appears on shaky legal ground as well.

### *Political Environments*

Political environments also contribute to states' evasion of borders. Whether they consciously avoid establishing legislation in their own countries or choose selective enforcement of the law, some governments create a permissive environment that allows for commercial, criminal, disruptive, and other nefarious activities to pass through their spaces. These political environments are not exclusively the purview of specific types of regimes and political systems; rather they depend largely on the interests of the governments that allow them to continue.

Russia's political environment, for example, has shown tolerance to cyber criminals, as well as nationalistic hackers. According to Reporters Without Borders, Russia maintains a robust surveillance apparatus known as SORM. SORM-1 focused on intercepting telephone communications; SORM-2 focused on data transmitted via the internet, and SORM-3 can intercept any form of communication and includes long-term storage. Censorship is

[12] Kenneth Corbin, "State Department Argues Against Cyber Arms Treaty," *CIO*, May 26, 2016, http://www.cio.com/article/3075442/government/state-department-argues-against-cyber-arms-treaty.html.

[13] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

also routinely enforced.[14] When it comes to cybercrime, Russia's prolific cybercriminals seems to follow two basic rules: 1) Russians do not hack Russians; and 2) If Russian intelligence asks for help, they comply. Russian hackers have gained attention since their 2007 DDoS attacks against Estonia and their 2008 involvement in the Georgia conflict. During these incidents, nationalistic hackers engaged in cyberattacks in defense of Russian culture and nationalism, with some of the attacks originating in or traversing through Russian internet space. More recently, similar activity has occurred in Ukraine where a conflict rages between Ukraine and Russian separatists, and online attacks are frequent.

Unlike Russia, the United States' political environment does not implicitly condone or support the activities of nationalistic actors hacking on behalf of US interests. However, the fact that an American patriotic hacker known as "The Jester" conducts attacks against terrorists and other hacktivists without being investigated and arrested by law enforcement certainly suggests that he has approval to do so. Even more so, the political environment of the United States is one where the highest levels of government condone questionable global surveillance activity, which collects incredible amounts of data not only internationally, but also domestically without citizen knowledge or approval. In this context, the US government evades its own borders, using its robust technical surveillance capability to capture and store information against adversarial nations, friendly nations, as well as its own citizens.

### *Legal Jurisdiction*

While transnational cybercrime affects all countries in the world, many governments still do not have adequate, if any, cybercrime legislation to support criminal investigation and prosecution. Even in those that do, such legislation has not yet proven to deter such activities; for example, the United States has some of the stricter cybercrime laws in the world and an increasingly competent law enforcement element, yet it remains among the leaders in cybercrime activity.

International law enforcement collaboration is spotty at best, a reality that constantly forces law enforcement officials to play catch up with advanced

[14] "Russia: Control from the Top Down – FSB (The Federal Security Service of the Russian Federation)," *Reporters Without Borders*, March 11, 2014, https://12mars.rsf.org/2014-en/2014/03/11/russia-repression-from-the-top-down/.

cybercriminal actors. There is no internationally accepted cybercrime legislation, although the Council of Europe Convention on Cyber Crime—the first international treaty seeking to address internet crime—has made great strides in getting governments on board. There are times, however, when cooperation between states is limited or when jurisdictional problems hinder the progress of investigations. The fact remains that not all law enforcement entities are as advanced as their colleagues, and in some cases, one entity may simply refuse to help another.

Currently, only the Convention on Cyber Crime appears positioned to help address border evasion issues from a collaborative perspective, rather than by relying on case-by-case, state-by-state bilateral legal agreements. Signatories under the Convention agree to adopt laws outlawing specific types of cybercrime and to take appropriate legal action as required to ensure law enforcement cooperation. As of March 2016, forty-eight states have ratified the convention, while a further six states had signed the convention but not ratified it. China and Russia are noticeably absent on this list.

## China: A Case Study

Beijing first introduced its views on internet sovereignty in a 2010 White Paper entitled "The Internet in China."[15] The intimation was clear: Beijing sought to establish as clear lines of sovereignty in cyberspace as there were for land, sea, and air. Building on this at the 2015 World Internet Conference hosted in Wuzhen, senior Chinese government and business officials, as well as government officials from Kazakhstan, Kyrgyzstan, Pakistan, and Russia, met to discuss internet issues. In his opening remarks at the conference, President Xi Jinping highlighted the need for governments to respect the rights of individual countries in developing a cyber governing path for its own citizens.[16] This plays an important role supporting China's security concerns, which focus on keeping the Communist Party in power, protecting China's territorial interests, and preserving internal stability. In a time when

[15] Shannon Tiezzi, "China's Sovereign Internet," *Diplomat*, June 24, 2014, thediplomat.com/2014/06/chinas-sovereign-internet/.

[16] "China Allows No Compromise on Cyberspace Sovereignty," *China Daily*, December 17, 2015, http://www.chinadaily.com.cn/world/2015wic/2015-12/17/content_22735756.htm.

the internet connects all facets of society, China sees cyber sovereignty as a critical component to national sovereignty.[17]

Beijing views cyber sovereignty not only as a way of further securing its interests, but also as an important means of countering "cyber hegemonic" activities that seek to undermine the country's national security. Chinese authors have written about US attempts to control the global internet, a fear reinforced by Snowden's revelations in 2013 of global surveillance. The "absolute freedom" of cyberspace as championed by the United States is viewed as beneficial to it and its national security, while it creates insecurity for the rest of the world.

To promote cyber sovereignty, China has been leveraging the UN Charter as justification to extend the principle of sovereign equality to cyberspace. This achieves two important objectives for Beijing: it demonstrates China's intent on using existing applicable international law to support its proposal, and it shows China's desire to raise such issues to a government level and in an international forum. Leveraging the legal angle lends legitimacy to China's proposal. Using the United Nations as a venue demonstrates China's commitment to multilateral action. In December 2015, China successfully fought to include the word "multilateral" in a document created by the United Nations that would direct the policies of the internet in the future. The importance of this addition was to show that governments—and not civil groups or organizations—should be the ones responsible for framing the rules. While this is non-binding for member states, it does provide the necessary counterbalance to previously established and accepted guidance.

China is not moving forward alone, but is promoting cyber sovereignty in various international forums, such as the Brazil, Russia, India, China, and South Africa (BRICS) Consortium, the Shanghai Cooperative Organization, and the UN Group of Governmental Experts, to name a few.

Notably, Beijing has engaged in strengthening the protection of its core national security interests through a series of laws and draft legislation. Examples of this trend include:

[17] "Why Does Cyber Sovereignty Matter?" *China Daily*, December 16, 2015, http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm.

*2016 Cyber Security Law:* In November 2016, the Chinese government approved its "Cyber Security Law."[18] The law addresses the security of key internet and information systems, while it increases the government's powers to record and impede the dissemination of information deemed "illegal." Two key reoccurring themes are stressed: 1) the ability to monitor and control information; and 2) compliance of foreign enterprises with the rules set forth. Critics have cited this law as being a government attempt to tighten its control on civil society while making unreasonable demands on foreign businesses.[19]

*2016 Overseas Non-Government Organization Management Law:* All NGOs are required to get approval from a supervisory unit to operate in China. It further prohibits any Chinese organization from conducting activities on behalf of or with non-authorized NGOs. While the law is not specifically cyber related, it is safe to assume that NGOs properly registering with Chinese authorities would be required to comply with any acceptable technology use policies set forth by the Chinese government in other legislation.

*2015 National Security Law:* This law provides a framework for China's security considerations in the face of emerging threats. Overlapping security considerations demonstrates Beijing's perspective that national security is an inherently integrated process, creating "a national security path with Chinese characteristics."[20] Perhaps most notably, however, is that the law is not restrictive to China's borders, and it includes the polar beds, outer space, and cyberspace.

*2015 Anti-Terror Law:* Passed in December 2015, it compels technology companies to help decrypt information, giving Chinese authorities access to encrypted data. The law combines administrative, judicial, and military means to address Chinese anti-terrorism efforts, demonstrating a comprehensiveness that reflects Beijing's desire to integrate all facets of security under the

[18] "China Passes New National Security Law Extending Control Over the Internet," *Guardian*, July 1, 2015, http://www.theguardian.com/world/2015/jul/01/china-national-security-law-internet-regulation-cyberspace-xi-jinping.

[19] Bethany Allen-Ebrahimian, "The Chilling Effect of China's New Cybersecurity Regime," *Foreign Policy*, July 10, 2015, http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/.

[20] "China Focus: China Defines Overall National Security Outlook in Draft Law," *Xinhuanet*, April 20, 2015, http://news.xinhuanet.com/english/2015-04/20/c_134166428.htm.

umbrella of its new national security law. This idea resonates with the recent push by US security agencies to weaken encryption systems to allow government access.[21]

While these efforts can be viewed as Beijing's attempt to gain greater resiliency in the face of external influences and to reduce potential economic and/or diplomatic liabilities imposed by the United States (e.g., cyber sanctions, economic sanctions, indictments, and so forth), such measures further reinforce China's position that governments have the right to manage their own internal cyber affairs. Indeed, many of these laws have been criticized for promoting economic self-interests and the tightening of controls, despite Beijing's insistence that they all are well in accordance with UN charter dictates.

## Conclusions

The internet governance debate presently remains a contested issue among nation-states. As a result, the so-called "Balkanization" of cyberspace is already happening, spurred on by a combination of national security interests, perceived threats, and economic warfare in the Western world and by the desire of states to control and monitor public opinion and political discourse. Imposing borders, however, would ultimately lead to the loss of huge opportunities in terms of economic development, the free flow of information, and online freedoms. While it is true that the somewhat naive vision of cyberspace embodied in Barlow's "Declaration of Independence" was never actually realized, it is imperative now to find a balance between sovereignty and globalization, as well as between national security and freedom.

It is incumbent on liberal democracies and on the seemingly hegemonic United States to lead the effort in finding such a consensus. It is unrealistic to minimize governments' involvement in this process as much as it is to solely empower them to find resolutions that could lead to a loss of accountability. Therefore, a multilateral agreement—based upon the successful guidance set forth by the regulation of global commons models such as banning military activities in space, ensuring the freedom of navigation on the open seas, and prohibiting sovereign claims on Antarctica—could very well provide the

[21] Joseph Lorenzo Hall, "Issue Brief: A Backdoor to Encryption for Government Surveillance," *CDT*, March 3, 2016, https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/.

most viable solution. Building a long-term, networked governance in the context of which both nation-states and non-state parties can work together seems the only mutually beneficial way for governments to reap the benefits of cyberspace without endangering their respective security interests.

# Four Big “Ds” and a Little “r”: A New Model for Cyber Defense

Matthew Cohen, Chuck Freilich, Gabi Siboni

As with all emerging threats, the cyber realm represents new dangers, which will be difficult to address. This article argues that cyberthreats are not fundamentally different from other asymmetric threats, and it provides a conceptual model for developing a response by drawing on classic principles of military strategy, the “four Ds”—Detection, Deterrence, Defense, and Defeat—as well as resilience (the little “r”). We offer a model for how countries can create policies addressing each of these principles that will enhance the security of national cyber systems. The proposed framework will allow for the development of detailed strategies and plans to address the specific demands posed by cyberthreats, whether state-based, or by non-state actors, or individuals.

**Keywords:** cyber, detection, deterrence, defense, defeat, resilience

## Introduction

Cyberspace is a dangerous place for nations. In 2016 a group called the “Shadow Brokers” announced it had successfully stolen classified malware codes used by the United States’ highly secretive National Security Agency. Some of this code, which is used to conduct espionage, is currently available to download online, and the Shadow Brokers have offered to sell the rest

Matthew Cohen is a PhD candidate and lecturer in Political Science at Northeastern University. Dr. Chuck Freilich, a senior fellow at Harvard’s Belfer Center, is a former deputy national security adviser in Israel. Gabi Siboni is a senior research fellow and head of the Program on Military and Strategic Affairs and Program on Cyber Security at INSS.

of the information to anyone willing to pay their hefty asking price.[1] In 2015, the United States announced that hackers had infiltrated sensitive computer systems at the White House, calling it one of the most sophisticated cyberattacks ever launched on US government systems; Russia is the likely culprit.[2] That year, North Korea launched a cyberattack against South Korea's nuclear operator, raising concerns regarding the safety of its nuclear power plants.[3] In 2014, hackers attacked Sony servers, posted private emails, and issued violent threats against the company and against any theater screening a satirical movie about North Korea. The United States blamed North Korea for the attack, stating that it would respond in a "proportional manner," and shortly thereafter North Korea's internet service was disrupted for days.[4] These are just a small sample of recent cyberattacks.

This article argues that the cyberthreat does, indeed, have some particularly difficult characteristics, but that an effective response can and will be found. To do so will require that a conceptual model be formulated to frame and guide discussion of the severity of different cyberthreats, the technologies to be developed, and the necessary government policies. This article proposes such a conceptual model by drawing on the classic principles of military strategy, the "four Ds"—Deterrence, Detection, Defense, and Defeat—as well as the less well-known concept of resilience (the little "r"). It will further explore how governments, militaries, and private entities can work together within this framework to address threats in cyberspace.

The concept of the four Ds is widely known and applied by governments around the world, but is defined differently by various authors and nations. For example, the United States applied a four Ds model, "defeat, deny, diminish, and defend," to the threat of terrorism in its 2003 "National

[1] Paul Szoldra, "New Snowden Documents Prove the Hacked NSA Files are Real," *Business Insider*, August 19, 2016, http://www.businessinsider.com/snowden-confirm-hacked-nsa-files-2016-8.

[2] Evan Perez and Shimon Prokupecz, "How the U.S. Thinks Russians Hacked the White House," *CNN*, April 8, 2015, http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html.

[3] K.J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes," *CNN*, April 22, 2015, http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/index.html.

[4] Haroon Siddique, "North Korea Responds with Fury to US Sanctions Over Sony Pictures Hack," *Guardian,* January 5, 2015, http://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony.

Strategy for Combating Terrorism."[5] Another example is Israel, which based its national security strategy for decades on a three Ds model of detection, deterrence, and defeat,[6] and later introduced a fourth "D,"—defense—for cyberthreats, as well.[7]

To date, no study has applied a comprehensive strategy of four Ds to the cyberthreat, although studies have touched upon each of the Ds separately. Each study offers valuable insights into the cyber realm, but the four Ds and the concept of resilience have interconnecting components that may be missed by surveying them separately. Thus, a holistic analytical framework that examines them together can offer a more complete understanding of the cyberthreat, both for academic and policymaking purposes.

## Defining the Cyber Realm

Many terms regarding cyberspace lack clear and widely accepted definitions. For our purposes, a cyberattack is an offensive use of cyberspace that both uses and targets computers, networks, or other technologies for malevolent, destructive, or disruptive political or criminal purposes.[8] Politically motivated cyberattacks—like other forms of warfare—aim to provide a strategic, diplomatic, economic, or military advantage over an adversary, or to force it to take an action it does not want to take.[9] Cyberattacks can be launched

[5] US State Department, "National Strategy for Combating Terrorism," February 2003, https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

[6] Matthew S. Cohen, Chuck Freilich and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17 (2016): 307–321; Chuck D. Freilich, "Why Can't Israel Win Wars Anymore?" *Survival* 57, no. 2 (2015): 79–92.

[7] Chief of the General Staff, "The IDF Strategy," *Israel Defense Force*, July 2016, https://www.idfblog.com/s/Desktop/IDF%20Strategy.pdf.

[8] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation: Project Air Force, 2009); Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2012); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).

[9] Jeffrey Carr ed., *Inside Cyber Warfare* (Cambridge: O'Reilly, 2012); Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2011): 817–886; Valeriano and Maness, *Cyber War versus Cyber Realities*.

by nations, non-state organizations, or individuals. Cyber defense includes efforts to ensure the ability to maintain control of internet service providers (ISP) and incoming and outgoing traffic, and to halt ongoing attacks.[10] Cyber espionage refers to use of the cyber realm by the state or by national security agencies (NSA) (often via malware or hacking, such as spear-phishing) to steal or gather information, or make known the attackers' ability to penetrate networks.[11]

## Four Big "Ds" and a Little "r"

In this section, we argue that, with some adaptations, cyberthreats can be effectively addressed using fundamental principles of military strategy—the above-mentioned four Ds, and the newer concept of resilience.

*Deterrence*. In order to deter an adversary, the adversary must have an identifiable "return address" against which to retaliate, and attribution must be possible, which is especially difficult in the cyber realm. Deterrence is further complicated in the cybersphere by the fact that it is not always possible to tell when damage has been done; indeed, the target may not even know it has been attacked.[12]

Different levels of certainty of attribution determine the type of response the country should deploy. A comparatively low level of certainty is all that is required for behind-the-scenes diplomacy. In such cases, a country can accuse another of attempting to modify its behavior without definitive proof. A medium level of certainty would be necessary before making public accusations. The highest level of certainty is needed for undertaking legal or kinetic action.

In cases of cyberattacks in which attribution is possible, the type of actor (state, terrorist group, NSA, or individual) plays an important role in determining the nature of the deterrence policy. Deterrence of cyberattacks by state actors is not substantively different from deterrence in other conflicts. The state under attack can retaliate with the entire spectrum of capabilities at its disposal— cyber, diplomatic, kinetic, or economic.

[10] Chris C. Demchak, *Wars of Disruption and Resilience* (Athens: University of Georgia Press, 2011); Valeriano and Maness, *Cyber War versus Cyber Realities*.

[11] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014); Valeriano and Maness, *Cyber War versus Cyber Realities.*

[12] Libicki, *Cyberdeterrence and Cyberwar*.

Deterring cyberattacks by terrorist groups is similar to preventing physical attacks, again running the gamut of potential cyber and non-cyber forms of retaliation. Most terrorist organizations are not nihilistic and have values they wish to protect, although the importance they attach to these values and their tolerance for punishment may be different from that of states. The ability to retaliate would only be limited by the same considerations that apply to the decision to employ physical retaliation, including distance and vulnerability. Just as in the physical world in which deterring terrorists is highly challenging, it is difficult to deter terror groups from launching attacks in cyberspace.

The sheer number of potential non-state organizations and individual attackers (hackers and activists) dispersed around the globe presents a challenge to the monitoring and attribution capabilities needed for purposes of deterrence. The sophisticated cyber capabilities of the state can, however, make it more difficult for an organization or individual to hide their identity. The good news regarding non-state organizations and individuals is that they are less likely to have the resources required to launch crippling cyberattacks against advanced states, and publicity is often one of their primary motivations, thereby facilitating attribution. Additionally, developing better forensic tools—an effort already underway—will help determine who launched the attack.

*Detection*. Detection or early warning of impending attacks is as critical in the cyber realm as in the physical. Prevention is only possible if there is sufficient early warning, and it is also usually easier to defend against such an attack. Few states, let alone NSAs, have the capabilities required to successfully conduct a major cyberattack against a sophisticated state-defender. The true challenge of detecting cyberattacks lies not in the vast number of potential attackers around the globe, but rather in the limited number of highly sophisticated ones; in this case, the problem of detection becomes more manageable.

Complicating the picture is the increasingly interconnected nature of governmental, military, and private-sector networks. Private-sector networks can now be used as a gateway to attack some governmental and military networks, meaning that the private sector should now be considered a vulnerability. Thus, states face the need to provide early warning not just for governmental systems and critical infrastructure, but also for major organizations and companies. Nations have already begun employing increased intelligence-gathering efforts and have expanded information sharing with the private sector. Nevertheless, information sharing between governments and private companies remains a significant challenge. Encouraging such efforts will likely require legal, organizational, and political changes by both governments and companies.[13] Technology is a critical component of a nation's cyber detection systems. Such efforts will also be greatly strengthened by using traditional off-line intelligence gathering of potential attackers to supplement what is gathered online.[14]

Several factors work to the defender's advantage. Attackers often conduct "cyber-reconnaissance missions" to assess the weak points in the defender's systems.[15] The larger a planned or ongoing cyberattack is, the easier it is to intercept communications between the attackers and carry out defense. For many nations, the problem of detection is simplified by the small number of communications cables carrying internet traffic.

*Defense*. Defense addresses the prevention and mitigation of attacks on military, governmental, and critical infrastructure networks, as well as on private networks, businesses, and individuals. The source of the attack determines the best means of defending against it, as the various actors are capable of different types of attacks and levels of severity. As noted, it is generally more difficult to defend against attacks by states, whereas the technological capabilities of non-state organizations and individuals are typically less advanced and can be handled through simple technological solutions.

Technology plays a central role in defensive efforts, and states have already begun building programs to assist with the defense of networks and cyber systems. Developing a range of technologies capable of addressing all types of threats is, of course, ideal, but resource constraints will require states to prioritize which threats are the most pressing so that the states can focus their resources on them. This is another area in which governments and the private sector can work together. Doing so will boost their ability to

[13] Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing," *Military and Strategic Affairs* 6, no. 3 (2014): 59–77.

[14] Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* (Tel Aviv: Institute for National Security Studies, 2016).

[15] Ned Moran, "A Cyber Early Warning Model," in *Inside Cyber Warfare*, ed. Jeffrey Carr (Cambridge: O'Reilly, 2012).

identify the greatest threats and create new tools for defense. Governments can even benefit if private cybersecurity companies choose not to work with them by observing the threats the companies address and using that as a guide for the government's threat assessment efforts. Governments can additionally work with private entities to ensure that security systems on networks that connect to government systems are up-to-date.[16]

At the same time, cyberdefense cannot be conducted only online, but rather requires a multi-layered effort involving gathering intelligence, interrupting attacks, securing networks, undertaking legal measures, formulating new norms of behavior, and engaging in effective cooperation with foreign governments. Currently, no clear international norms or laws exist regarding behavior in cyberspace.[17] Treaties, laws, and norms could prove to be useful in limiting malicious actions by states in cyberspace. To be effective, states must agree on the types of activity to be addressed, the responsibilities of the state under the agreement, and the punishments for violations. In addition, states must establish international bodies to oversee compliance.[18]

International cooperation is also of great importance and states can benefit from deepening and expanding the number of nations they cooperate with on cybersecurity. Intelligence sharing, bilateral and multilateral agreements, and improved cooperation with law enforcement agencies in other countries can

[16] William J. Lynn, "Defending a New Domain," *Foreign Affairs*, October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Milton L. Mueller, Andreas Schmidt, and Brenden Kuerbis, "Internet Security and Networked Governance in International Relations," *International Studies Review* 15, no. 1 (2013): 86–104; Ido Naor, "ATMZombie: Banking Trojan in Israeli Waters," *SecureList*, February 29, 2016, https://securelist.com/blog/research/73866/atmzombie-banking-trojan-in-israeli-waters/; Teri Radichel, "Case Study: Critical Controls that Could Have Prevented Target Breach," *SANS Institute*, 2014, https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

[17] Abraham D. Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," *Proceedings of a Workshop on Deterring Cyber-Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: National Academies Press, 2010), http://www.nap.edu/catalog/12997.html; Valeriano and Maness, *Cyber War versus Cyber Realities.*

[18] Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

be of great value in planning defensive strategies.[19] Enhancing cooperation between states will be necessary to ensure that new laws and norms are enforced.[20]

*Defeat*. The concept of defeat in the cyber realm should not be viewed as completely preventing all cyberattacks. In both the physical and cyber realms, decisive defeats have been quite rare. Defeat of an adversary in the cyber realm should thus be understood as reducing the number and severity of attacks to a level that allows a society to maintain its way of life and to bounce back quickly from attacks (see below for more on resilience). To achieve defeat in the cyber realm, a nation must be able to show its opponents that it can prevent major cyberattacks; cyberattacks that a state cannot prevent will be futile, either because they will not cause significant damage or the state is capable of rapidly bouncing back; and that cyberattacks will be met with some form of retaliation. Overall, achieving defeat requires that states be capable of successfully implementing each of the four Ds and the little r.

States must also give cyberattacks the same importance they attach to physical attacks and—when appropriate—use similar methods and strategies, such as responding not just with cybertools, but also with kinetic capabilities.[21] Launching kinetic attacks is straightforward against attacking states, but is far more complicated against NSAs, and would require either gaining the permission of the host-state or risking a military escalation. Additionally, there is likely to be significant public backlash against the use of kinetic strikes in response to cyberattacks by an NSA.

Due to the highly diffuse nature of the threat, nations cannot expect to prevent every cyberattack from every individual and non-state organization around the world. A nation can defeat an opponent in cyberspace by minimizing the likelihood of a major attack capable of widespread disruption or damage. If an adversary cannot successfully execute a major attack, it has, in effect, been defeated. For the numerous NSAs and individual attacks, defense is

[19] Observer Research Foundation, "International Public Private Partnership in Cyber Governance (Panel)," in *CYFY Conference Report, 201*3, India Conference on Cyber Security and Cyber Governance, http://www.bic-trust.eu/files/2014/04/CYFY-2013-Report-WEB-version-15Apr14.pdf.

[20] Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

[21] Robert Hackett, "Let's Get Physical? United States Weighs Options When It Comes to Cyber Attacks," *Fortune*, May 12, 2015, http://fortune.com/2015/05/12/rogers-cyber-attacks-us-response/.

a more appropriate response and a better use of resources, particularly as they are unlikely to have the capabilities necessary to cause severe damage.[22] Enhanced international cooperation can improve the ability of states to defeat such actors by imposing legal and criminal penalties for cross-border attacks.[23] States can more realistically aspire to achieving cyber defeat of states, terrorist organizations, and major non-state organizations.

*Resilience*. If an attack succeeds, the question is then how to manage the damaged system and to recover as rapidly as possible, i.e., to build "resilient" systems. Different systems will require differing levels of resilience. Some networks only need to quickly return to their most minimal level of functioning, while others must return to their original level of functioning as soon as possible.

The process of building resilient systems in cyberspace starts by drafting various high probability but low-cost scenarios, as well as low probability but high cost ones. Once developed, it is then possible to build plans and tools to address them. This must take place before failures occur and should include technological measures, human resource development, training exercises and drills, and implementation measures.[24] Resilience in the context of the cyber realm must also include plans regarding how to recover from the physical effects of cyberattacks.

The inherent limit on resources means that it is critical to prioritize the systems that require resilience. For example, military systems and the power grid likely are far more important to a nation than other networks. Metrics can be developed to help determine which systems are most critical and thus where to invest technological resources.[25] The impact of a failed network or infrastructure on the public morale and the citizens' faith in their government to provide basic public goods is one important measure to consider.

Building resilience also requires working closely with the private sector. Private companies are often responsible for maintaining facilities, dealing with threats, and ensuring they continue to operate. Governments must work

[22] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4, no. 63 (2010): 63–86.

[23] Valeriano and Maness, *Cyber War versus Cyber Realities*.

[24] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014); Valeriano and Maness, *Cyber War versus Cyber Realities*.

[25] Ibid.

with, as well as regulate, the private sector to ensure that the facilities have proper plans in place for addressing failures.[26]

Reality is likely to present unexpected cyberdefense failures, with results that may be extreme; a resilient system could be the difference between relatively rapid recovery and severe consequences. Intelligence gathering of enemy plans or more generally their capabilities can be vital in planning the recovery.[27] Resilient systems make attacks far less consequential, thereby reducing the payoff for the attacker.[28] This, in turn, decreases the likelihood that an attack will occur in the first place.

Resilience can, however, only go so far, and eventually an attack will take down both a system and the response designed to deal with its failure. Nations must be prepared for this likelihood and should develop additional plans for living without the system for a more extended period. This will likely require redundancy and will require policymakers to develop plans that are not dependent upon technology.

## Policy Implications

In this section, we discuss specific policy recommendations drawn from the four big Ds and little r model. To achieve deterrence, nations must make it clear to their adversaries what their retaliatory capabilities may be and the penalties they are likely to pay. Deterrence postures and intentions can be made through public statements and/or confidential channels.[29] This is complicated by problems of determining attribution as it is not always clear who should be the target of these postures and intentions. This can be overcome, however, as attribution abilities improve. Improved attribution abilities will convince the target of the deterrence postures that they will

[26] Dana Pasquali, "3 Steps Towards Building Cyber Resilience into Critical Infrastructure," *Dark Reading*, August 2, 2016, http://www.darkreading.com/vulnerabilities---threats/3-steps-towards-building-cyber-resilience-into-critical-infrastructure/a/d-id/1326464; Jan Trobisch, *Challenges in Protection of US Critical Infrastructure in the Cyber Realm* (Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 2014), https://www.hsdl.org/?abstract&did=791151.

[27] Demchak, *Wars of Disruption and Resilience*.

[28] US Department of Defense, "The DoD Cyber Strategy," 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[29] Ibid.

suffer the penalties, in addition to helping states to target their policies more effectively to the relevant adversaries.

The nature of the government in the country from which a cyberattack originates and, specifically, its willingness to cooperate are both crucial factors. Here, retaliation is not possible, unless the attacked state is willing to breach the sovereignty of the country that hosted the cyberattackers. Instead, a nation may be able to achieve deterrence by working with the host government's intelligence and law enforcement agencies. In some cases, the likelihood of severe legal action might be a sufficient retaliatory deterrent. Today, this expectation is quite limited, thereby emboldening organizations and individuals to carry out cyberattacks. When attacks originate in countries that do not have cooperative or effective governments, the ability of a nation to deter through legal means is, of course, far more limited. The deterrent question then becomes similar to retaliation against a physical attack and revolves around whether the attacker has cyber capabilities or other values that are worth counterattacking and the feasibility of doing so.

The real problem in deterring NSAs in the cyber realm, as in the physical world, may be that the damage they cause—painful as it may be—is usually limited, while their tolerance for pain often exceeds what the responding state is willing to mete out as punishment. This is especially true of Western democracies. It is not that they are incapable of defeating NSA threats; rather, the effort required to defeat them—including the level of damage and cost in lives—typically has been perceived as incommensurate with the threat to the state's interests. The same holds true for cyberattacks. Should an NSA conduct a drastic cyberattack, or should there be convincing information about an impending one, the country under attack undoubtedly will be more willing to adopt severe deterrent measures. To achieve deterrence, states must be able to assign attribution for an attack. To this end, states must deploy and continuously improve technological and intelligence tools, including information gathering about the technological abilities and goals of potential adversaries.[30] This is an area in which private entities and governments

[30] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

should consider ways to work together, as private cybersecurity companies can identify malware and offer insights into its possible origins.[31]

A further complication is that cyberattacks may be routed through ISPs in third-party nations. It is possible for a government to work with or pressure the ISPs or their host governments to halt cyberattacks as they occur.[32] If adequate cooperation is not achieved, it may be possible to retaliate by publicly shaming the state, group, or individual that conducted the attack. This has the additional benefit of alerting security services around the world to the attacker, thus decreasing their ability to launch further attacks.

Efforts to improve the detection of cyberattacks should be based both on specially tailored means of gathering cyber intelligence and investing a greater portion of already existing human and electronic intelligence resources in the cyber realm. As much as cyber technology poses new problems of detection, it also provides new options for doing so.[33] The Australian national cyber strategy stresses this point and calls for improved detection through continuous online, real-time monitoring.[34] Although a vast number of cyberattacks can be launched simultaneously from different sources, cyber technology can detect and counter a similarly large number. One option, appropriate primarily for non-state and individual attackers, is to pose as fellow activists and members of the cyber networks in order to gain intelligence, skills, and tools.[35]

A difficulty in detecting attacks by both states and NSAs is that they can originate in friendly nations, which constrains the ability to spy on them without straining relations. Technology, however, can assist with this, since detection can be done from afar without violating a state's sovereignty.

[31] Grant McCool, "Computer Spying Malware Uncovered with 'Stealth' Features: Symantec," *Reuters*, November 23, 2014, http://www.reuters.com/article/us-symantec-malware-regin-idUSKCN0J70SH20141123.

[32] Clarke and Knake, *Cyber War*.

[33] Department of Homeland Security, "The National Strategy to Secure Cyberspace," February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[34] Commonwealth of Australia, "Australian Government Cyber Security Strategy," 2009, http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

[35] Microsoft, "Impersonation," http://technet.microsoft.com/en-us/library/cc961980.aspx.

Conversely, the need for heightened international cooperation and information sharing is clear.

In terms of defense, states wishing to bolster their capabilities can focus on improved use of technology. Defending the cyber realm demands that existing technologies be improved and new ones be created. The defense mechanism must also be appropriate for the situation. In the initial stages of an attack, before any real damage has been done or systems penetrated, efforts to disrupt or redirect the attack may be adequate. If the system has been penetrated, or damage done, the defense mechanism should seek to contain the attack, as well as prevent the attacker from knowing that the intrusion has been discovered and successfully stopped.[36]

Protecting networks in both the governmental and private sectors will require new legislation and regulations. New government agencies may need to be created to help draft specific requirements and to ensure that defense mechanisms are implemented. The US Cyber Command and Israel's National Cyber Bureau are examples of centralized organizations responsible for overseeing the creation and implementation of cyber-defense strategies, including efforts to work with the private sector.

Governments, private companies, and academics should collaborate to develop new defensive technical tools and strategies and to improve existing ones. Governments can offer monetary incentives to private entities, where appropriate, to help build robust defenses[37] Surprisingly simple measures might prove quite effective, such as requiring employees of government agencies and private entities connected to government networks to use strong passwords that are regularly changed, as well as mandatory training to identify and avoid cyberthreats.[38]

Defenders must also consider the supply chain used to design and manufacture their equipment. Hardware, firmware, and software are currently created and built around the world, which makes it difficult to ensure a product is secure. The companies and nations in which such equipment is designed and manufactured may include hidden codes enabling the devices to eventually be hacked. Governments should consider working in conjunction

[36] Siboni and Assaf, *Guidelines for a National Cyber Strategy*.

[37] Teri Radichel, "Case Study: Critical Controls that Could Have Prevented Target Breach," *SANS Institute*, 2014, https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

[38] Ibid.

with foreign companies and nations to develop an accreditation system that ensures the design and manufacturing processes are transparent.[39] Such a plan does pose dangers, however, particularly in that it might make it more difficult to protect intellectual property, raise the price of the equipment by adding an additional expense, and even stifle the pace of innovation.[40]

The creation of global laws, norms, and international agreements can be useful in bolstering cyber defense. Focusing on protecting critical infrastructure and civilians (for example, banning attacks or intrusions into hospitals) are areas that seem most likely to produce agreement.[41] States should attempt to play an active role in the creation of these laws and norms, as the more involved a state becomes, the greater its ability to protect its interests and shape the future system.[42] Attempting to build laws and norms is an inexpensive undertaking that could potentially improve cybersecurity for nations around the world. If successful they would be a means of bolstering not only defense, but also detection, deterrence, and defeat.[43]

The power of international norms and laws in cyberspace, however, have important limitations. It is unclear how effective international law and norms might be due to the decentralized nature of cyberspace.[44] Furthermore, states might be reluctant to craft agreements regarding uses of the cyber realm that they consider beneficial to their national interests, particularly as this is still a relatively unchartered area.[45] Finally, as noted, it can be difficult to tell when an attack has taken place or to assign attribution, meaning states may believe they can escape punishment.

[39] David Inserra and Steven Bucci, "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," *Heritage Foundation*, March 6, 2014, http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

[40] Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

[41] Clarke and Knake, *Cyber War*; Sofaer, Clark, and Diffie, "Cyber Security and International Agreements"; Valeriano and Maness, *Cyber War versus Cyber Realities*.

[42] Siboni and Assaf, *Guidelines for a National Cyber Strategy*.

[43] Observer Research Foundation, "International Public Private Partnership in Cyber Governance (Panel)."

[44] Valeriano and Maness, *Cyber War versus Cyber Realities*.

[45] Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

To heighten their ability to defeat attackers in the cyber realm, states can take several steps. They can seek to isolate attacking nations and adopt confrontational tools, such as economic or diplomatic sanctions, in effort to convince them that continued offensive action is too costly. The prospects of defeating an enemy in the cyber realm can be increased if states focus on ways to destroy the opponent's cyber capabilities due to the extensive planning and expensive equipment required to launch sophisticated attacks.[46]

In addition to heightened legal punishments, states can take steps to mitigate the threat from individuals. Isolating individual hackers from the broader community upon which they rely—by disrupting their internet connections or sharing information about the hacker that the community might not approve of—would limit their ability to plan or launch an attack.[47] In addition, states can try to convince some hackers to serve as informants, or penetrate the hackers' networks by planting agents within them. These strategies may also be effective against many NSAs whose members rely on similar communities for support. This strategy may pose risks under international (and domestic) law, but the lack of clearly applicable international law on actions in cyberspace lowers the legal risk.

To enhance resilience in the cyber realm, states should seek a diversity of equipment. Hardware and software should not all be supplied from one source or company. Diverse equipment will allow nations to more quickly isolate the problem, switch to a different company's equipment, and resume operations, although this may increase supply-chain risks. When designing networks, features aimed at improving resilience can be built-in to support the recovery process. To help build resilience for the most critical networks, nations can design cyber architecture that offers multiple pathways for controlling systems.[48] Physical overrides should be built-in to ensure other ways of regaining control of critical systems. Railways, for example, can

[46] Jonathan Silber, "Cyber Vandalism – Not Warfare," *Ynet*, January 26, 2012, http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

[47] Scott D. Applegate, "The Principle of Maneuver in Cyber Operation*s,"* in *Fourth International Conference on Cyber Conflict,* ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Talinn: NATO CCD COE, 2012), https://ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf.

[48] US Department of Defense, "The DoD Cyber Strategy."

be constructed with the ability to stop a hijacked train by using physical controls that do not depend on cyber systems.

## Conclusion

Cyberattacks are not fundamentally different from other threats and can be addressed by applying the classic principles of military strategy, the "four Ds," along with the concept of resilience. These principles may not provide a complete response—much as they do not when applied to other asymmetric and conventional threats—and modifications will certainly be required for the challenges posed by cyberthreats. In those areas in which they prove deficient, however, we are confident that new capabilities will be developed over time as has always been the case when new threats arise.

Research and development are key to the effort to develop these new capabilities across all four Ds and the r. Advanced states have largely managed to ensure that their defense mechanisms have outpaced the offensive capabilities of NSAs. There is, however, no inherent reason this will remain the case, particularly if states fail to take the threat seriously.

This article is a first holistic effort to apply the "four big Ds and a little r'" model to cyberthreats, with the objective of turning it into a conceptual framework that could guide state cyber strategies. Use of the basic framework allows for the development of more detailed plans designed to address the specific demands posed by cyberthreats. The article found that improved intelligence, more resilient cyber architecture, and heightened cooperation both internationally and between the government and private sector are central means for implementing the "four Ds." Further research can help determine additional ways in which the model can be applied or expanded to the cyber realm.

# Proportional Response to Cyberattacks

Jarno Limnéll

Analysis in recent years demonstrates that government responses to cyberattacks vary widely. Although there has been significant political pressure to "do something," past experiences illustrate that most policy responses are ad hoc. This indicates that 1) response to cyberattacks is still an exceedingly untested phenomenon; 2) cyber domain is a relatively new arena of conflict—especially for the policymakers—and, therefore, special attention should be directed towards it; and 3) more research is needed to understand how nation-states could best respond to cyber hostilities and which instruments should be used. This article analyzes comprehensively how cyberattacks should be treated as a political question and provides a rough framework upon which policymakers can build. The article presents five variables that policymakers need to consider when evaluating appropriate responses to cyber hostilities. Combining incident impact, policy options, and other variables, the framework outlines the different levers of cyberpolitics that can be applied in response to the escalating levels of cyber incidents. The response framework is also an integral part of the state's cyber deterrence.

**Keywords:** Cybersecurity, cyberattacks, cyber warfare, cyberstrategy, politics, cyberpolitics, response, security, hybrid warfare

## Introduction

The US Department of Homeland Security and the Office of the Director of National Intelligence made a major announcement in October 2016. They officially declared that the Russian government directed the attack on the

Professor Jarno Limnéll teaches cybersecurity at Aalto University, Finland.

emails of US persons and institutions, including political organizations,[1] and stated that "these thefts and disclosures [were] intended to interfere with the US election process."[2] The accusation is remarkable in two ways. First, there is the act itself. The intrusion adds a serious political spin to prior intrusions and was a clear attempt to affect and manipulate the US presidential elections by utilizing cyber methods. The hack is also a reminder of how cyberattacks can undermine the conception of sovereignty, create confusion among people, and blur the borders between war and peace. Second, there is the question of attribution. While absolute attribution is a difficult endeavor, in this case, the US intelligence community stated that it was confident that the hacks could have been authorized only at the highest levels of the Russian government.[3] This public and direct political accusation indicates a high level of certainty of the attribution. Russian officials, however, dismissed the attribution as "rubbish" designed to inflame anti-Russian hysteria.[4]

The most important and interesting question followed the two previous ones. What will be the US response to these hacks? As Barack Obama, the former president said, cyberspace is "uncharted waters" where "you don't have the kinds of protocols that have governed military issues, for example, and arms issues, where nations have a lot of experience in trying to negotiate what's acceptable and what's not."[5] Hillary Clinton made it clear that the

[1] In July 2016, the WikiLeaks website publicized embarrassing emails from the accounts of the Democratic National Committee (DNC). The hackers gained full access to the DNC network used by the election staff, including emails, memos, and research pertaining to Democrats running for Congress.

[2] Homeland Security, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, October 7, 2016. https://www.dhs.gov/node/23199.

[3] Intelligence Community Assessment, *Assessing Russia Activities and Intentions in Recent US Elections*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[4] Dmitry Solovyov, "Moscow says U.S. Cyber Attack Claims Fan 'Anti-Russian Hysteria,'" *Reuters*, October 8, 2016, http://www.reuters.com/article/us-usa-russia-cyber-ministry-idUSKCN1280DO.

[5] White House, *Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting*, June 8, 2013, https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-/.

"United States will treat cyberattacks just like any other attack."[6] Voices in the United States and in the Western world have urged the US administration to respond and make it clear to Russia that a cyberattack on the democratic process will be met with an appropriate response. President Obama confirmed that the United States had been weighing a "proportional response" and a range of responses were available.[7] What does "proportional response" mean in concrete actions? We do not know. The United States had stated that the response "will be at the time of our choosing, and under the circumstances that will have the greatest impact."[8] This is a new situation for the American national security establishment and policymakers. At the time of this writing, President Obama had ascertained that the United States would sanction nine Russian entities and individuals and expel thirty-five Russian diplomats in retaliation for the US election hacking. President Obama also said that the United States would "continue to take a variety of actions" at a time and place of its choosing, some of which will not be publicized.[9]

The interference of the US presidential elections and consideration of a proportional response to the cyberattack is just one example of the subject of this article, and it raises several questions: Why is it important to create a political response framework to cyber hostilities in today's world? What should be taken into consideration when deciding upon a proportional response to a cyberattack? The hacking of the US elections is also a reminder of the urgent need to develop international norms to reduce the possibility of cyberattacks and hostilities in an increasingly digitalizing world.

[6] Andrew Blake, "Hillary Clinton: U.S. Will Treat Cyberattacks 'Just Like any Other Attack,'" *Washington Times*, October 7, 2016, http://www.washingtontimes.com/news/2016/sep/1/clinton-us-will-treat-cyberattacks-just-any-other-/.

[7] Julie Davis and Gardiner Harris, "Obama Considers 'Proportional' Response to Russian Hacking in U.S. Election," *New York Times*, October 11, 2016, http://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html.

[8] David E. Sanger, "Biden Hints U.S. Response to Russia for Cyberattacks," *New York Times*, October 15, 2016, http://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html.

[9] White House, *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*, December 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

## Theoretical Basis

The security of cyberspace is an integral part of today's security, warfare, and politics; therefore, it is important to understand that cyberattacks and other activities in cyberspace should not be separated into a stand-alone area without the broader political, strategic, and geopolitical context. For example, in the ongoing war in Ukraine, the cyber component has been an integral part, which is usually understood as the continuation of politics by other means.[10]

Actions are often divided into five levels: policies and goals, strategies, operations (including campaigns), tactics, and tools.[11] Actions at all these levels are important, but security professionals too often concentrate only on tactics and tools in cybersecurity and—most pertinently—from a technological point of view. This article approaches cyber affairs primarily from the political perspective because of the increasing importance of cyber affairs in today's interconnected world and in international politics. For example, NATO has recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.[12] NATO has also created the ability to invoke Article 5 in response to cyberattacks, which is a political decision.

The analysis of cyberattacks in recent years demonstrates that governmental responses vary widely.[13] There has been significant political pressure to "do something," but experience shows that most policy responses are ad hoc. This indicates that 1) response to cyberattacks is still an exceedingly untested phenomenon; 2) the cyber domain is a relatively new arena of conflict, especially for the policymakers, and therefore it needs special attention;

[10] This Clausewitzian approach is controversial, but describes how politics and war are intertwined. See, for example, Mary Kaldor, "Inconclusive Wars: Is Clausewitz Still Relevant in these Global Times?" *Global Policy* 1, no. 3 (2010): 271–281.

[11] See, for example, Richard Bejtlich, "Strategic Defence in Cyberspace: Beyond Tools and Tactics," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCDCOE, 2015), pp. 159–170.

[12] NATO, *Warsaw Summit Communiqué*, July 9, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[13] See, for example, Sico Van der Meer, "Signaling as a Foreign Policy Instrument to Deter Cyber Aggression by State Actors," *Clingeldael*, December 2015, https://www.clingendael.nl/sites/default/files/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf.

and 3) more research is needed to understand how nation-states could best respond to cyber hostilities and the instruments that should be used.

As offensive cyber activity becomes more widespread, policymakers are challenged to develop proportionate responses to disruptive or destructive attacks. Several variables, however, should be considered before responding. At the end of this article, a rough framework is presented upon which policymakers can build, offering a kind of end-result analysis. Combining the impact of cyberattacks, policy options, risks, time, attribution, and proportionality, the framework outlines the different levers of cyberpolitics that can be applied in response to escalating levels of cyber incidents.

## The Importance of Politics in Cyber Affairs

### *Testing the Limits*

During the past decade, governmental and non-state hackers have become increasingly sophisticated in their attacks on the digital systems upon which states depend for essential services, economic prosperity, and security. Such breaches have threatened critical infrastructure, intellectual property, privacy of users' data, important national security information, and government personnel data. Due to the advances in technology and the increasing dependency on cyberspace, cybersecurity, as well as its need for rules and common approaches, has become an increasingly important issue. At the same time, the concepts of attack, defense, deterrence, international cooperation, and espionage have assumed new meanings. The heightened reliance upon digital infrastructure and its vulnerability to multiple vectors of cyberattacks has led governments and non-state actors to utilize cyberspace for acting out their geopolitical differences and promoting their political objectives. This means also that the value of "non-kinetic warfare" is increasing. Both international and national discussions about cyberattacks and how to respond to them are long overdue, even if the strategic importance of the digital domain is widely acknowledged. The current "political cyber playbook" is still a slim volume, but it expands daily as parts of the world move towards greater strategic use of cyberweapons to persuade their adversaries to change their behavior.

Nation-states and non-state actors currently are testing the boundaries of the "cyber battlefield," and the number of the visible and invisible cyber activities and the level of their sophistication have been increasing. Innovative ways to utilize cyberspace are being developed and employed. In December 2015, we witnessed the first confirmed cyberattack to take down a power grid, which affected approximately 225,000 civilians in Ukraine.[14] Cyber capabilities (and the will to use them) are reaching a more advanced level, and it seems that we are not sure how to live in this new reality.

### *The Rise of Cyberpolitics*

In recent years, issues related to cyberspace and its uses have catapulted into the highest realm of politics. Previously, cyberspace had been considered largely a matter of low politics, background conditions, and processes. Today, cybersecurity has become a focal point for conflicting domestic and international interests and—increasingly—for the projection of state power.[15]

It is increasingly important to understand cyberspace as a political domain; this is often forgotten or neglected. When considering cyberspace from the perspective of the nation-state, today's topical cyber questions are very political. Like other domains, the cyber domain should be treated primarily as political. When politics is involved, questions of power are always present. For example, in the context of war, the cyber instrument is like land, sea, and air power—a means to achieve a political aim or increase power. Thus, the strategic use of cyberspace for pursuing political goals and seeking a geostrategic advantage has increased.

With the creation of cyberspace and our deepening dependence on it, a new arena for the conduct of politics is taking shape; moreover, we may be witnessing a new form of politics. This process is described as "cyberization,"[16] which refers to the ongoing penetration of all political fields by different mediums of the cyber domain. Therefore, the concept of cyberpolitics[17] is useful. Cyberpolitics refers to the conjunction of two processes: (1) those

[14] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[15] Jelle Van Haaster, "Assessing Cyber Power," in the *Eighth International Conference on Cyber Conflict: Cyber Power*, eds. N. Pissanidis, H. Rõigas, and M. Veenendaal (Tallinn: NATO CCD COE, 2016), pp. 7–22.

[16] Jan-Frederik Kremer and Benedikt Müller, eds., *Cyberspace and International Relations, Theory, Prospects and Challenges* (London: Springer, 2014) pp. xi–xvii.

[17] Nazli Choucri, "Cyberpolitics in International Relations," in *Oxford Companion to Comparative Politics*, ed. Joel Krieger (New York: Oxford University Press, 2012), pp. 267–271.

processes pertaining to politics regarding the determination of who gets what, when, and how; and (2) those processes using cyberspace; that is, an arena of digital interactions. In the cyber and physical arenas, politics involves conflict, negotiation, and bargaining over the mechanisms, institutional or otherwise, to resolve contentions over the nature of core values in an authoritative manner. Thus, cyberpolitics is tangible when nation-states consider proportional responses to cyberattacks.

Cyberpolitics is employed across the world largely by academics who are interested in analyzing the use of cyberspace for political activity as well as its breadth and scope. Although cyberpolitics is present at both national and international levels, both cyberpolitics and the cyber domain have created new conditions that do not have clear precedents, even if cyber issues are at the core of the foreign and security policies of nation-states. In the coming years, we will have actual cases that will reveal the true content of cyberpolitics. At that point, we may then return to using the concept of politics—of which cyber affairs are integral—without the need to emphasize the concept of cyberpolitics. Indeed, the cyber domain is no different from the conventional frames of politics.

### *Global Cyber Norms Are Still at an Early Stage*

In 2015, a group of governmental experts at the United Nations tried to develop some rules in the field of information and telecommunications in the context of international security.[18] The report significantly expanded the discussion of cyber norms, rules, and confidence-building measures. The group recommended that states cooperate to prevent harmful cyber practices and should not knowingly allow their territory to be used for damaging international acts using information and communications technologies (ICT). One important recommendation was that a state should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. Even if the report emphasized that "making cyberspace stable and secure can be achieved only through international cooperation" and necessitates that states take appropriate measures to protect their critical infrastructure, it did not give any guidance

[18] United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," July 19, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172.

how to respond especially to state-sponsored cyberattacks. Furthermore, the report stated that it may be insufficient to attribute an attack to a specific state based on the fact that the cyberattack originated in that state's territory or was launched from its ICT infrastructure.[19]

States retain the inherent right to self-defense under Article 51 of the UN Charter when faced with an imminent threat. State behavior in cyberspace should therefore be in line with the UN Charter; however, the challenge of attribution and the understanding of the extent of damage by a cyberattack may complicate the situation. The right to self-defense, including the use of force, would apply if a cyberattack reaches the level of an "armed attack"; yet, the legal debate on what constitutes an armed attack in cyberspace has only just begun. It is conceivable that harmful cyber hostility attributable to a state amounts to a violation of the Article 2 (4) of the UN Charter, given its character and effects.[20] This leads to the question of how to evaluate the impact of cyberattacks, especially if they do not cause physical damage.

A cyberattack does not necessarily have to cause physical damage for it to be considered serious. Possibly due to the long tradition of physical security, physical destruction is strongly emphasized, and it is also easier to observe any physical consequences. The old way of thinking is that a "severe cyberattack" should involve physical destruction, including death and damage to critical infrastructure. However, as we become increasingly dependent on data and non-kinetic assets, could the manipulation of health or financial records, for example, be treated with the same level of severity as physical consequences?[21] Moreover, is there a difference between the manipulation of banking data or health-care data, as the former potentially could result in severe economic disruptions and the latter in death at its extreme? The answer is ambiguous. Moreover, it is unclear what a "major" cyberattack means in practice. It needs to be understood that the answer to the question, whether or not a cyberattack is an act of war, is a political decision and not a conclusion.

[19] Ibid.

[20] "All members shall 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 other manner inconsistent with the purposes of the United Nations."

[21] Jarno Limnéll and Charly Salonius-Pasternak, "Challenge for NATO—Cyber Article 5," Briefing Paper, Center for Asymmetric Threat Studies, Swedish Defense University, June 2016.

## Five Variables

In determining appropriate responses to a cyberattack, policymakers need to consider the following five variables—questions that must be answered before responding.

*Who Did It?* Attributing a cyberattack to its sponsor—the state or non-state actor behind the attack—remains a significant challenge as it requires effective measures and the ability to identify the perpetrators behind the attack. The problem of attribution is exceedingly complex and not always solvable. Cyberspace allows for a great deal of anonymity, and attacks can be routed through servers all over the world to mask their origin. Misattributing a cyberattack could lead to a response directed at a wrong target. When considering proportionate response, policymakers should understand the level of confidence they have in attributing the attack.[22] For instance, if the level of attribution is low, decision makers will be limited in their choice of response, even if the severity of the attack is high. Governments need to calculate the costs that would incur if they wrongly attributed an attack and consider the potential costs of escalation. Thus, the degree of attribution influences the action taken.

The ability to attribute an attack to a specific source is important for maintaining credibility and ensuring legitimacy at home and abroad. The challenge is that sufficient proof of attribution may be gathered via "secret intelligence data sources" or obtained from "friendly nations," yet the state does not want to publicly reveal these intelligence sources. Releasing at least some proof of attribution is necessary, if the state wants to build international legitimacy for the retaliatory actions it takes.

Attribution involves many aspects, including technical, legal, and political. It is a multi-dimensional issue that requires an analysis of multiple sources of information, including forensics, human intelligence reports, signals intelligence, history, and geopolitics. As Rid and Buchanan argue, attribution is an exercise of minimizing uncertainty on three levels: tactically, attribution is an art as well as a science; operationally, attribution is a nuanced process instead of a black-and-white problem; and strategically, attribution

[22] Tobias Feakin, "Developing a Proportionate Response to a Cyber Incident," Council on Foreign Relations, August 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

is a function of what is at stake politically.[23] Successful attribution requires a range of skills at all levels, careful management, time, leadership, stress testing, prudent communication, and recognizing limitations and challenges. Even if attribution capabilities have increased due to the great interest of security experts on all three levels, the conclusion of the attribution in order to respond is always a political decision.

*What is the Impact?* Policymakers need to understand the extent of the impact of a cyberattack, as it determines the type and level of response. How harmful the attack has been to national security and society, what kind of services are affected, and whether the attack has caused a significant loss of confidence in the country's reputation are just a few of the questions concerning the effects of cyberattacks. It can take weeks, if not months or years, for computer forensic experts to ascertain accurately and conclusively the extent of the damage done to the target organization's computer networks. For example, it took roughly two weeks for the Saudi authorities to understand the scope of the damage of the Shamoon incident, which erased data from thirty thousand Saudi Aramco's computers. Companies or governmental organizations also sometimes only realize that they have been hacked months or years after the attack. Clearly, it is easier to assess the physical impact of an attack.

When the effects of a cyberattack are not always clear, it is hard for decision makers to determine if the cyber hostility is at the level of an attack and if it requires a response. Many examples of cyber infiltration fall short of their purpose, qualifying rather as nuisance activities or even garden-variety espionage.[24] The challenge with calculating proportionality in the cyber context resides in the speed and covert nature of the cyberattack: it is difficult to establish the magnitude and consequences of a cyberattack. Information to understand the effects can also be difficult to acquire; for example, financial institutions and private companies may be reluctant to provide information about the damage suffered because of business confidentiality.[25]

[23] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2014): 4–37.

[24] James Stavridis, "How to Win the Cyberwar against Russia," *Foreign Policy*, December 12, 2016, http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

[25] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (New York: Oxford University Press, 2014).

*Which Instruments Can be Used for Response?* When considering a proportional response to cyberattacks, the decision is always about the options available to the state. It is said that every nation-state can respond using at least four instruments: diplomatic (i.e., foreign policy instruments such as diplomatic communication, warnings, and sanctions), informational, military, and economic.[26] Policymakers need to consider the full range of responses at their disposal, from a quiet, diplomatic rebuke to a military strike. There is no reason to believe that cyber hostility of any form directly requires a proportionate cyber response. The response does not need to be limited to cyberspace, since nothing bars the state from using other means, although each carries its own political risks. The US Defense Service Board has even suggested that in case of the largest possible cyberattacks, the United States should not rule out a nuclear response.[27] It is usually argued that kinetic responses should be only permissible if the attack has intended lethal effects, causes human suffering or loss of life, or if human rights are directly violated.[28] In increasingly digitizing societies, this is too narrow of an approach, as argued earlier in this article. Currently, however, it becomes difficult to justify kinetic military response to a cyberattack that does not cause physical harm in the conventional sense.[29]

The key issue is to consider which cyber or physical (or other) countermeasures can be used as part of the nation-state's "response arsenal" and which measures should be used in each case. This is a question of the lever of national power at a state's disposal and willingness to use it. Response to cyberattacks may be delivered overtly or covertly. If cyber methods are used, a covert response can be difficult to develop quickly unless the government has already prepared its capability against a specific target, which likely involves prior cyber espionage in order to understand

[26] Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic," *Defence Studies* 14, no. 4 (2014): 370–393.

[27] Department of Defense, Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA569975.

[28] See for example, Thomas Wester, "Just Cyberwar," Cyber Security Policy and Research Institute, November 24, 2014.

[29] Patrick Lin, Neil Rowe, and Fritz Allhoff, "Is it Possible to Wage a Just Cyberwar?," *Atlantic*, June 5, 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-justcyberwar/258106/.

the target's vulnerabilities. A covert response also does little to warn other countries. An overt cyber response also can be unappealing as states may lose the ability to launch similar cyber responses against other targets and will more likely generate a counter-response. If the response is visible to the public, it should also be accompanied by a narrative of justice, and not of revenge. States may also choose to outsource their responses to proxy hacker groups; in doing so their control over the response may be limited, which could lead to escalating actions.

*What Are the Policy Guidelines?* Policymakers need to consider the current national security and cybersecurity strategies, which describe the general policy guidelines of the state regarding the political willingness to act and to leverage power. If the state is a member of international alliances and organizations, their policy guidelines must also be considered when formulating the proportionate response. Otherwise, the state can be accused of not following the agreed-upon and shared policies. As mentioned before, cyberspace is not immune to the legal norms that require nations to respond proportionally to an attack.

When a cyberattack occurs, it is possible for policymakers to overreact. Several cyber experts have estimated that overreaction is very real, and decision makers should weigh the possible escalation carefully before responding. As Libicki argues, decision makers should understand what is at stake; that is, what it is that they hope to gain by responding with a given method.[30] Cybersecurity professionals also may have an incentive to trumpet the threat of cyberattacks, which, at times, may heighten the risk of overreacting. Even if political pressure is great following a cyberattack, political prudence is needed. At the very least, a certain level of restraint should be encouraged. Self-restraint is a concept that is relevant for de-escalating the situation, especially if kinetic response is considered. In general, in order to deter the situation from escalating, the adversary needs to believe that the outcome of escalation will be much worse than that of restraint, which occasionally can be a stronger means of manifesting national power.

[30] Martin C. Libicki, "Cyberwar Fears Pose Dangers of Unnecessary Escalation," *RAND Review*, Summer 2013, http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyberwar-fears-pose-dangers-of-unnecessary-escalation.html.

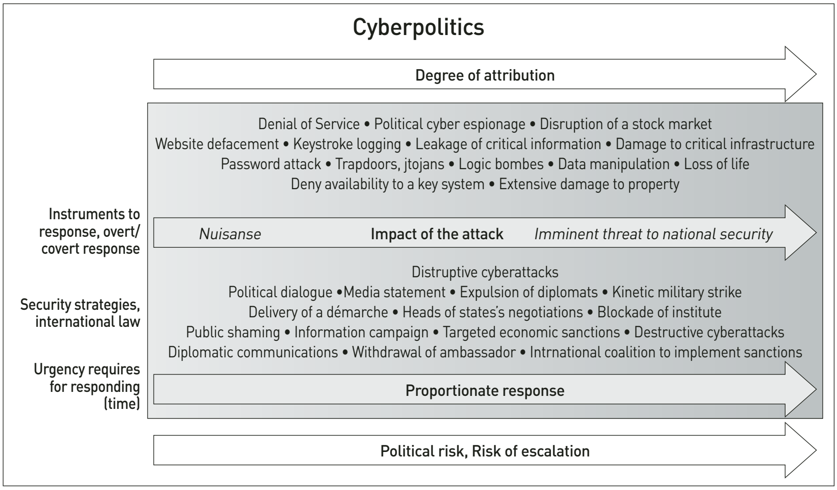
*How Urgent is a Response?* Time is a relevant issue in politics. The political pressure to respond increases especially when the impact of the cyberattack is acknowledged publicly, and the official accusation of the attacker is announced. Not responding fast enough could mean the loss of face and political credibility. Political rivals would likely also exert more pressure towards "doing something." Therefore, the low level of certainty in attribution may be used as an excuse to do nothing.

## Response Framework

Cyber hostilities provide governments with a complex set of decisions to make, from understanding the level of attribution and the severity of the attack to evaluating proportional response and assessing the risks involved in taking certain courses of action. Decision makers also must assess their kinetic and non-kinetic instruments that can be used in response while time passes and political pressure increases. Passivity in the face of cyberattacks likely will encourage opponents to be more aggressive. Policymakers need to be proactive in determining appropriate response options. Developing a framework for responding to cyberattacks allows policymakers to quickly consider solutions and counter with options that have already been analyzed for merit and possible consequences. Identifying appropriate response in advance could prevent the state from making mistakes that could unintentionally jeopardize its political, economic, intelligence, and military interests. Although each response will be case-specific (situation-dependent), a framework will enable policymakers to quickly consider their options.

Figure 1 below represents a rough example of the framework upon which policymakers should build to determine the potential responses to a cyber hostility before it even occurs. This gives decision makers a starting point for making their own assessments about the course of action to be taken at the time of crisis. Combining the degree of attribution, incident impact, policy options, risks, security strategies, international law, urgency, and proportionality, it outlines the different levers of cyberpolitics that should be applied in response to the levels of escalation and the severity of the cyberattack. The purpose of the framework—while deliberately simplified—is to illustrate the different aspects that policymakers need to carefully analyze when a state considers a range of options and responses to a cyberattack, including the decision to do nothing. According to the framework, the more severe the cyberattack, the more strongly the response should be. The framework illustrates the impact and severity of a cyberattack, with website defacement at one end of the scale and loss of life at the other. This is analyzed against the level of response, ranging from media statements to military responses. The options of response can be complemented covertly and/or overtly with different instruments. Across the response spectrum are inherent political and legal risks associated with each decision, and risks increase as the level of the response does.

**Figure 1:** Political Response Framework


Cyberpolitics
Degree of attribution
Denial of Service • Political cyber espionage • Disruption of a stock market
Website defacement • Keystroke logging • Leakage of critical information • Damage to critical infrastructure
Password attack • Trapdoors, jtojans • Logic bombes • Data manipulation • Loss of life
Deny availability to a key system • Extensive damage to property
Instruments to response, overt/ covert response
Nuisanse
Impact of the attack
Imminent threat to national security
Distruptive cyberattacks
Political dialogue •Media statement • Expulsion of diplomats • Kinetic military strike
Delivery of a démarche • Heads of states's negotiations • Blockade of institute
Public shaming • Information campaign • Targeted economic sanctions • Destructive cyberattacks
Diplomatic communications • Withdrawal of ambassador • Intrnational coalition to implement sanctions
Security strategies, international law
Urgency requires for responding (time)
Proportionate response
Political risk, Risk of escalation

As Feakin argues, policymakers should clearly understand the costs associated with each response.[31] Each response will have an impact on the state's diplomatic relations, reputation, power, and military and intelligence operations. Implications need to be understood before a response is chosen. Assessing options will require input from relevant government agencies, as well as private-sector companies, whose operations and businesses could be affected by the response.

The framework should not be interpreted as strict political "redlines" for certain responses. Two sides should be considered when possibly setting

[31] Tobias Feakin, "Developing a Proportionate Response to a Cyber Incident," Council on Foreign Relations, August 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

redlines concerning cyber hostilities. On the one hand, redlines invites adversaries to act below the line, thinking that they have immunity or low political risk in carrying out their cyber operations. Redlines can also push states into the corner so that they are compelled to respond when the line is crossed in order to preserve their credibility. Presumably, states do not want to be too precise about sharing potential responses with the public. On the other hand, setting redlines is a strong message of deterrence to a state's adversaries and lets them know that the state will respond if they cross the line. A certain degree of imprecision may be politically the best solution: the state announces that there will be a response, but it does not reveal the details beforehand.

## Conclusion

The role of the cyber domain is increasingly shaping the global security environment and power dynamics between states and other actors. At the same time, cyber capabilities are reaching a more advanced level. We have entered an unstable and suspicious era, and we have done so without a clear roadmap of tested political fundamentals. States are trying to navigate the bounds of acceptable and proportionate responses when faced with confrontational cyber hostilities. Political understanding and commitment is needed more when states are trying to determine the proportionate way to respond to different cyber hostilities. In cybersecurity, the focus is too often on technical details without understanding the political context. Ultimately, the decision as to whether a cyberattack is an act of war or something else is a political one, particularly in cases that fall into the gray area between annoyance and actions that attempt to end the existence of the state. Operating in today's "unpredictable hybrid security environment" requires more political expertise and preparation in cyber issues. Undoubtedly, the significance of cyberpolitics will increase in the coming years. Moreover, policymakers will be forced to re-conceptualize "cyberwar" or "cyber conflict" as a form of "hybrid war" that is contested even during peacetime.

Protocols for responding to cyber hostilities are unclear and should be understood as a lack of power in cyberspace. This article introduced a political response framework that provides a starting point for governments and decision makers to build their country-specific frameworks. Given the likely pressure that will be exerted upon governments to respond to cyberattacks, policymakers need to develop a response framework of their own before disruptive or destructive cyber hostilities occur. The framework presents the main variables that should be taken into consideration when formulating a response to a cyberattack. The framework also encourages governments to develop their readiness and capabilities in order to obtain answers to the questions presented in the framework—before deciding how to respond.

Even if a political response framework is created, it does not mean that it will be used accurately. One reason is that new methods to utilize cyberspace are being developed all the time. In politics—and in cyberpolitics—there will always be flexibility depending on both the current decision makers and ambiguity of the situation. As each state has its own cultural, political, and military characteristics, all states should develop their own policy-response frameworks. What is recommendable in one national framework may not be so in another.

# Human Terrain and Cultural Intelligence in the Test of American and Israeli Theaters of Confrontation

Kobi Michael and Omer Dostri

This article describes and defines the concept of "human terrain" that developed in the American military following its experiences in Afghanistan and Iraq and elaborates on the reasons that led to its development. It focuses on the theoretical foundations and on the correlations between human terrain, cultural intelligence, and intercultural competence, all against the backdrop of the American and Israeli experiences in different theaters of confrontation.

Acquiring an in-depth understanding of the local culture is an essential condition for ensuring the relevance of a military mission. Cultural intelligence as a means of correlating the cultural knowledge obtained by the Human Terrain System with the intelligence necessary for carrying out the military mission is also crucial. Recognizing the importance of cultural intelligence led the American military to develop its Human Terrain System, which is composed of professional teams of social scientists who are embedded in forces at various levels and whose role is to help the forces in the combat theaters gain an understanding of the culture and the society.

Commanders and team members who took part in the program widely agreed that the Human Terrain System contributes to the relevance and success of the military mission; alongside the importance attributed to the system, however, its operation also sparked criticism, both in military and academic circles. Despite

Dr. Kobi Michael is a senior researcher at the Institute for National Security Studies. Omer Dostri holds an MA in Diplomacy from Tel-Aviv University and is an intern at the Institute for National Security Studies.

the methodological, operational, and organizational developments of the Human Terrain System in the American context, gaps still exist, and in many cases, the deliverables are inadequate. Gaps in knowledge of human terrain and its assimilation in the combat doctrine and in the intelligence methodology also exist among the security and intelligence agencies in Israel.

**Keywords**: intelligence, cultural intelligence, human terrain, military, the IDF, the US military, culture, methodology, intercultural competence

## Introduction

The concept and the term “human terrain” developed in the American military back in 2006, as a result of difficulties with which the military forces contended in the Iraqi and Afghani theaters.[1] Human terrain relates to the social, ethnographic, cultural, economic, and political elements in a densely-populated arena in which a military force operates and is premised on the belief that the key to a mission’s success is to focus on understanding the people.[2]

Military and intelligence doctrines, which place emphasis on the operation of the military force, its firing capabilities, and precise technologies for hitting the targets and achieving military victory are not enough to efficiently quell an uprising or engage in peace-keeping operations. In such operations, the fighting force is dealing with a civilian population, whose cultural and political characteristics are usually strange and different from those of the fighting force.[3] Therefore, the task force and its commanders need a different

[1] Within the Israeli context, this term was referred to for the first time in an article by Ohad Laslevi, “The Human Terrain as a Basis for Operating Forces: Contending with the Bedouin during the Campaign in the Negev Desert during the War of Independence,” in “*Bein haqtavim”* vol. 1: *Frontier – Study of the Challenge Emerging on the Borders* (Dado Center for Interdisciplinary Military Studies and Maarachot Publishing, February 2014): 7–27 (in Hebrew), https://www.idf.il/media/6790/בין-הקטבים-1-התכסית-האנושית-אהד-לסלוי.pdf.

[2] Roberto González, “Human Terrain: Past, Present and Future Applications,” *Anthropology Today* 24, no. 1 (2008): 21–26.

[3] Kobi Michael and David Kellen, “Cultural Intelligence for Peace Support Operations in the New Era of Warfare,” in *The Transformation of the World of War and Peace Support Operations*, ed. Kobi Michael, David Kellen, and Eyal Ben-Ari (Westport: Greenwood, 2009).

kind of intelligence that can widen its understanding and narrow the cultural differences between them and the local population—gaps that detract from the mission's relevance.[4]

General Rupert Smith discussed the importance of the cultural issue and defined contemporary war as "war amongst the people."[5] This type of war is characterized by a blurred distinction between the civilian and the military fronts during intensive military activity in densely populated urban areas, and with increasingly significant involvement of non-state actors in the form of terrorist and guerilla organizations operating from within the population and under its protection. These characteristics affect the type of intelligence necessary to understand the importance of the civilian population and environment as the battlefield, the target during the fighting, as well as the pawns during the fighting. At the same time, emphasis should be placed on weakening the patronage of the rebel forces—whether terrorist or guerilla—while increasing support for the fighting militaries and leveraging the influence of local leaders and forces to help promote the objectives of the fighting. These, coupled with the moral necessity and the international legal imperative of protecting the civilian population, led the US military to internalize the understanding that it needed to deepen its knowledge about civilian populations in those theaters.

This article describes and defines the concept of "human terrain" that developed in the American military and elaborates on the reasons that led to developing this concept. Focusing on the theoretical foundations, its definitions, and characteristics, the article analyzes the correlation between human terrain, cultural intelligence, and intercultural competence. It discusses the characteristics of implementing the Human Terrain System in the confrontation theaters of the United States and Israel and presents the key lessons learned, which could also be relevant to the combat challenges facing the Israel Defense Forces (IDF).

[4] Ibid.

[5] Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Knopf, 2007).

## Human Terrain—Background, Characteristics, and Theoretical Definitions

Human terrain is defined as "characterizing cultural, anthropological, and ethnographic information about the human population and the interactions within the joint operations area." Human terrain analysis is "the process through which understanding the human terrain is developed. It integrates human geography and cultural information."[6]

The Human Terrain System project is a US military program that recruits, trains, and deploys human terrain teams, comprised of military and civilian experts, who are embedded in military units in the combat theater.[7] The project began in 2006, given the difficulties encountered with the new combat theaters in Iraq and Afghanistan. As a result, in 2007, the US Department of Defense approved and funded professional support for providing American military forces with a needed understanding of the local sociocultural issues in Iraq and Afghanistan.[8]

The US Army Training and Doctrine Command manages the Human Terrain System. Teams of five to nine civilian and military personnel are deployed to support brigade, division, and theater-level staffs and commanders and prepare them for contending with a civilian population. They do this by providing meticulous instruction before deploying them, and they continue to provide professional support after their deployment, using a support and analysis center and providing software tools to enable sociocultural analysis.[9] The teams are comprised of experts in both the social sciences and

[6] Ministry of Defense, "Joint Doctrine Note 4/13-Culture and Human Terrain," (Swindon, Wiltshire: Ministry of Defense, 2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/256043/20131008-_JDN_4_13_Culture-U.pdf.

[7] Montgomery McFate and Steve Fondacaro, "Reflections on the Human Terrain System during the First 4 Years," *Prism* 2, no. 4 (2011): 63–82, https://www.ciaonet.org/attachments/19701/uploads.

[8] Christopher A. King, Robert Bienvenu, and T. Howard Stone, "HTS Training and Regulatory Compliance for Conducting Ethically-Based Social Science Research," *Military Intelligence Professional Bulletin* 37, no. 4 (2011): 16–20, https://fas.org/irp/agency/army/mipb/2011_04.pdf.

[9] Yvette Clinton, Virginia Foran-Cain, Julia Voelker McQuaid, Catherine E. Norman, and William H. Sims, "Congressionally Directed Assessment of the Human Terrain System" (Alexandria, VA: Center for Naval Analysis, 2010), p. 15, https://info.publicintelligence.net/CNA-HTS.pdf.

military operations, who collect knowledge and gain understanding about the populations residing in the regions of the fighting, aided by interviews and interactions with individuals from those populations.[10] The teams conduct socioscientific analyses of the local population to help the deployed military forces increase their situational awareness, improve culturally-informed decisionmaking, enhance operational effectiveness, and preserve and share sociocultural knowledge.[11]

## Between Human Terrain, Intercultural Competence, and Cultural Intelligence

### *What is culture?*

"Culture" is defined as the customs, concepts, ideas, and social norms that are shared by a group of people and guide their beliefs and behavior. Characterization of a culture requires answers to questions such as: How are the people organized? What are the people's beliefs and values? What are the ways in which the people interact with each other and with outsiders? As a rule, people do not behave randomly, but rather, they behave in a way that appears logical to other people in their group. Their behavior is accepted and understood within the group due to their shared ideas, which define normative behavior.[12] Culture is layered with multiple meanings, based on language, society, economics, religion, history, and other fields. These layers are expressed by tangible characteristics that form one's cultural identity, such as physical appearance, attire, architecture, gestures, social laws, style of communication, and beliefs.[13]

### *Between intercultural competence and cultural intelligence*

The word "intelligence" has two different meanings: intelligence in the sense of an individual's aptitude or competence and in the sense of military information-gathering. Consequently, the term "cultural intelligence" refers to two related but different concepts: intercultural competence and cultural intelligence. Intercultural competence relates to "a cognitive

[10] King et al., "HTS Training and Regulatory Compliance," p. 16.

[11] McFate and Fondacaro, "Reflections on the Human Terrain System," p. 63.

[12] Ministry of Defense, "Joint Doctrine Note 4/13 – Culture and Human Terrain."

[13] CADS Staff, "Cultural Intelligence and the United States Military," (Washington, DC: Center for Advanced Defense Studies, 2006), https://www.files.ethz.ch/isn/26999/14_cult_int_us.pdf.

and psychological capability of individual or group's ability to adapt to, select, and shape a culturally-different environment."[14] Inkson and Thomas defined intercultural competence as "being skilled and flexible about understanding a culture, learning increasingly more about it and gradually shaping one's thinking to be more sympathetic to a [different] culture and one's behavior to be more fine-tuned and appropriate when interacting with other cultures."[15] Intercultural competence is one of the most important tools for developing cultural awareness. Cultural intelligence also relates to the military operational functions of collecting and analyzing information about an arena and an opponent, the interpretation of which is influenced by cultural aspects. Intercultural competence is an essential precondition for cultural intelligence, due to the need to understand the context and the differences between adversaries, and it is even more critical in the context of a "war amongst the people."[16]

Intercultural competence facilitates engaging in a set of behaviors that includes language, interpersonal skills, and more. The acquisition of intercultural competence is not a prescribed or defined process; rather, it is a perpetual learning process through education and experience, combined with the individual's aptitude for comprehending the needs of different environments. These enable individuals not only to learn about other cultures but also to develop the capacity to understand these cultures. Understanding other cultures allows individuals to anticipate needs and take necessary actions, recognize minute cultural cues, facilitate communication, conduct negotiations, and arrive at solutions.[17]

## Cultural intelligence

Cultural intelligence engages in a rational organization of local politics, as well as in understanding cultural codes, needs, and the internal order of social networks. This intelligence is used to not only identify threats but also opportunities to promote political change. Therefore, cultural intelligence needs

[14] Michael and Kellen, "Cultural Intelligence for Peace Support Operations," p. 170.

[15] David C. Thomas and Kerr Inkson, "Cultural Intelligence: People Skills for a Global Workplace," *Consulting to Management* 16, no.1 (2005): 5–9.

[16] Michael and Kellen, "Cultural Intelligence for Peace Support Operations," p. 170.

[17] Todd J. Clark, "Developing a Cultural Intelligence Capability" (master's thesis, Fort Leavenworth, Kansas, US Army Command and General Staff College, 2008).

to be based on a broad understanding of the political and social dimensions of the confrontation theater.[18] In the context of international relations, cultural intelligence is defined as "an analysis of social, political, economic, and other demographic information that provides understanding of a people or a nation's history, institutions, psychology, beliefs and behaviors." Today's conflicts in locations such as Iraq and Afghanistan require the military to place an emphasis on the local populations, which constitute the key terrain in the war against terrorism and in global wars.[19] In order to produce high-quality cultural intelligence, the information-collection and research professionals must free themselves of ethnocentric attitudes that attribute universal value or meaning to the values of their home countries, and instead, they must practice openness and sensitivity to other cultures.

In a critique written by Dina Rezk about deconstructing the ethnocentric mindset of Western intelligence agencies over the past decades, she explained that, to this day, Western intelligence researchers still have a hard time relating to particular cultural behaviors in Arab-Muslim societies, such as the role of Islam in society, the dominant use of rhetoric, political motivation, and the primacy of the sense of honor.[20] According to Rezk, the alternative to cultural knowledge is a state of Western-influenced universalism of values, doctrines and beliefs—one-dimensional notions such as "democracy," "freedom," and "rationality"—to which all are expected to conform on an ideological and perceptual level. Rezk argues that the dangers of such universalism reinforce how necessary and important it is for intelligence communities to devote further efforts to making progress in cultural studies.[21]

The urgency for intelligence agencies to gain an understanding of the opponent's culture receives more meaningful expression in the contemporary theater of "war amongst the people." In this conflict theater, there are restrictions on the use of force, and the quality of the cooperation between the military actors and the civilian ones (the civilian population, non-government organizations, and international organizations) is both reciprocally affected and mutually exclusive. Since all actors in the theater are considered producers

[18] Michael and Kellen, "Cultural Intelligence for Peace Support Operations," p. 162.

[19] Clark, "Developing a Cultural Intelligence Capability."

[20] Dina Rezk, "Orientalism and Intelligence Analysis: Deconstructing Anglo-American Notions of the 'Arab'," *Intelligence and National Security* 31, no. 2 (2016): 226.

[21] Ibid., pp. 244–245.

of intelligence, there must be a shared language among everyone to achieve fruitful cooperation. At issue, inter alia, are non-state organizations, the police, and the private sector, which collect and produce information that is needed for intelligence purposes, but they are still not full partners in today's arenas.[22]

Military forces that are working to achieve their goals are compelled to understand the political and cultural context and to adapt the military doctrine and means to this context and to the conflict theater in question. One of the most important operational tools for this purpose is intelligence. Therefore, intelligence means and methods must be adapted to conflict theater's political context and its dynamic nature. Factors that military commanders anticipate in a traditional military theater are unlike those that the military must consider when operating within a civilian population.[23]

Intelligence professionals must understand the culture, language, and environment in the conflict theater and that information-gathering in this type of theater requires intensive engagement with the local population. The local population is a group of people who are simultaneously the arena (the military operating theater), the target (for the goals of subverting their support of terrorist and guerilla groups that are operating under their shelter and support and for establishing legitimacy and the conditions for their cooperation with the military forces against these insurgents), as well as a key source of intelligence.[24]

Insurgents, including terrorist and guerilla organizations, understand the local culture better than any foreign military force. Therefore, they have an enormous advantage over the foreign military force in assimilating into the population and carrying out their activities with the population's assistance and protection. To ensure that the military force successfully gains the support of the local population, the military must understand the local people and its culture so that it can operate the mechanisms for intervention and cooperation with the population in order to weaken the guerilla and terrorist groups. It must minimize the insurgents' support base among the local population

[22] Michael and Kellen, "Cultural Intelligence for Peace Support Operations," p. 162.

[23] Kobi Michael, "Doing the Right Thing the Right Way: The Challenge of Military Mission Effectiveness in Peace Support Operations in a 'War Amongst the People' Theater" in *Cultural Challenges in Military Operations*, ed. Cees M. Coops and Tibor Szvircsev Tresch (Rome: NATO Defense College, October 2007), pp. 254–263, https://www.ciaonet.org/attachments/381/uploads.

[24] Ibid.

by undermining their propaganda that justifies the insurgents' actions as solutions to the population's grievances;[25] and design a sociopolitical structure (a collaborative effort with the military and the local population) that will change the local population's perspective and enable them to independently cope with these forces over time.

Eran Zohar, who analyzed the functioning of the Israeli military intelligence prior to and during the "Arab Spring," argued that any attempt by intelligence agencies—such as the IDF Intelligence Corps—to understand the enemy cannot succeed as long as the intelligence investigators do not understand Arab culture and language: "The difficult and exhausting work of learning about the enemy and the attempt to comprehend its intentions should not be pushed aside because it is easier to define the enemy's rationale."[26] Zohar states that "an intelligence agency profits from intelligence researchers who amass a thorough and intimate understanding of the target country and are familiar with its history, culture and traditions. These qualifications may be helpful in predicting revolutions."[27]

American experiences in Iraq and in Afghanistan exposed the problematic nature of the cultural encounters between the task forces and local populations, as the locals perceived the American task forces as foreigners and as invaders.[28] Robert Mihara also maintained that the American invasions into Afghanistan and Iraq exposed the Bush administration's lack of understanding of the political developments in the world and of the prerequisites for state-building in those two countries. As far as Mihara is concerned, the American policy and strategy embraced a belief that democratic and liberal ideologies are compatible for remaking societies in various countries, including Iraq and Afghanistan. However, large segments of the local society were not interested in partaking in the Bush administration's state-building dreams and objected to the democratic and liberal values that the Americans were

[25] US Department of the Army, "Insurgencies and Countering Insurgencies," FM 3-24/MCWP 3-33.5 (May 2014), http://www.marines.mil/Portals/59/MCWP%20 3-33.5_Part1.pdf.

[26] Eran Zohar, "Israeli Military Intelligence's Understanding of the Security Environment in Light of the Arab Awakening," *Defense Studies* 15, no. 3 (2015): 20.

[27] Ibid., p. 26.

[28] Richard Burchill, "Jihadist Insurgency and the Prospects for Peace and Security," *Small Wars and Insurgencies* 27, no. 5 (2016): 958–967.

trying to promote.[29] The United States' limited success in recent years battling uprisings and terrorist attacks by radical Islamic groups in Afghanistan and in Iraq, and also the recent fighting against the Islamic State in Iraq and Syria derives from inadequate knowledge and a lack of understanding of the belief systems (mainly religious beliefs) that motivate Islamic terrorist attacks (Salafi-jihadism) and of the reasons for their success in recruiting activists, local support, and resources.[30]

The absence of a religious foundation in the modern Western political ideology does not negate the importance of religion in other cultures. A religious ideology is, apparently, the most important factor that the West needs to focus on —or at least, to try to understand better—when jihadist insurgency movements are the issue. Fighting against an insurgency does not always end with a clear military defeat of the insurgents and their supporters; nevertheless, it is necessary to ensure significant achievements during this fighting, which would enable the restoration of order and prevent additional future attacks by the insurgents.[31]

An efficient battle against a jihadist insurgency indeed requires the West to formulate a military strategy and to use military force; at the same time, it must also direct its efforts against the ideology that is driving terrorist groups. In addition to focusing on the strategic issue, it is important to understand the people who are engaging in Islamic terrorism, and what attracts them to join the battle. The challenge that the West faces during confrontations of this kind is developing its ability to "conquer" the hearts and minds of the population.[32] This competition to capture the hearts and minds of the population—particularly the young—was met by a major rival in the form of terrorist organizations, such as the Islamic State, which are exploiting the internet age and social networks for cultural intelligence activities. The

[29] Robert Mihara, "The Inutility of Force," *Infinity Journal* 5, no. 3 (Fall 2016): 25–28.

[30] Burchill, "Jihadist Insurgency and the Prospects for Peace and Security."

[31] Ibid.

[32] Rupert Smith, *The Utility of Force.*

objectives of this activity are not only to recruit activists through public opinion but also to make terror a popular, desirable, and imitable way of life.[33]

Moreover, a significant share of the images and video clips used by the Islamic State to entice the young population in the Arab and Muslim world to support the organization or join it and take part in its activities is directly inspired by contemporary Western culture, which is well known by young audiences from the cinema, video games, and popular music video clips. Paradoxically, the terrorist organizations use modern Western culture and brands for promoting anti-Western values and culture.[34]

Understanding the culture of the local population is critical, and it contributes significantly to contending with attacks by "lone wolves"; that is, terrorist attacks by individuals who are not officially affiliated or associated with a specific terrorist organization, or who sometimes claim to belong to such an organization before, during, or after a terrorist attack, as they identify with the ideology espoused and with the aim of increasing the resonance of their act of sacrifice and its impact on public opinion.[35]

A lone terrorist, who has been influenced by radical ideas and messages, decides to commit a terrorist attack independently and usually quite spontaneously, which makes it extremely difficult to thwart. Nevertheless, it is still possible to identify clues that individuals or small groups might commit a terrorist attack, such as visits to countries where terrorist organizations are active, involvement in criminal activities, previous arrests, or high-profile suspicious activity in social networks. "In order to attempt and enter the minds of potential terrorists, technological resources are not enough and the intelligence service must understand moods, 'habitats,' socio-economic backgrounds and environmental factors. This requires cultural, linguistic and mental understanding."[36]

[33] Javier Lesaca, "On Social Media, ISIS Uses Modern Cultural Images to Spread Anti-Modern Values," *TechTank* (blog), Brookings Institution, September 24, 2015, https://www.brookings.edu/blog/techtank/2015/09/24/on-social-media-isis-uses-modern-cultural-images-to-spread-anti-modern-values/.

[34] Ibid.

[35] Col. (res.) Shlomo Mofaz, "Intelligence Challenges in an Era of Terrorism," *Israel Defense*, July 28, 2016, http://www.israeldefense.co.il/en/content/intelligence-challenges-era-terrorism.

[36] Ibid.

A military organization—being a disciplined, hierarchic organization—operates according to principles that differentiate it from other organizations, mainly civilian organizations. The military's aloofness from the civilian society in a foreign and hostile environment becomes a significant obstacle in their ability to develop and augment their cultural intelligence. As stated, overcoming this obstacle requires the military to mingle and closely interact with the local population so that it can acquire a deep familiarity and understanding. Achieving these targets is necessary to reach optimal efficiency in completing the military missions, particularly in a complex arena like that of a "war amongst the people." This type of combat requires openness to diverse strategic military means, including a variety of sources and types of intelligence—like cultural intelligence— some of which is found outside the military milieu.[37]

## The Natural Links between Intercultural Competence and Cultural Intelligence

Military forces operating in the contemporary conflict theater contend with terrorist or guerilla organizations that operate within the civilian environment and use civilians as human shields. The emergence of this complex type of warfare compels Western military forces to adapt their doctrines and modes of action to the new challenges so that they can cope effectively.[38]

The changes in the battlefield and in military activities have highlighted how essential it is that the various military forces familiarize themselves with the local population and with their needs as a means of achieving a successful military mission. Intelligence gathering is supposed to supply this need. An essential precondition to obtaining reliable and high-quality intelligence is the improvement, development, and assimilation of intercultural competence within the military—primarily among the forces in the conflict theater—in order to generate cultural intelligence.

In the tense and complicated situations that characterize contemporary combat, intercultural competence becomes an essential skill among commanders and senior officers operating in the conflict theater. Intercultural competence, which enables effective interactions with people from another

[37] Michael and Kellen, "Cultural Intelligence for Peace Support Operations," pp. 262–263.

[38] Ibid, p.168.

culture, becomes the cognitive platform for understanding and internalizing information and for communicating with the local population and institutions, as well as with civilian organizations operating in the area.[39]

One of the major cultural challenges that Western military forces have contended with has been their encounters with societies and populations (mostly Muslim) in Arab-Muslim countries and in non-Arab Muslim countries (such as Afghanistan). Religion and ethnicity play a far more important role in Muslim societies than in the Western world. The fact that, unlike the Western world, the Arab and Muslim world has not undergone a secularization process, and that the importance of religion has even intensified in most Middle Eastern countries over the last generation, makes it extremely difficult to assess the behavior of Arab and Muslim society and culture in terms of realpolitik and according to Western logic.[40] A foundation of knowledge derived from cultural intelligence will enable higher competence in assessing "religious edicts, the motivation that they generate, and the tension between religious dictates and the constraints of reality." In the absence of a developed methodology of cultural intelligence and an adequate relevant foundation of knowledge, the West "lacks sufficient comprehension of the political and social functions of religious, ethnic and tribal affiliations which affect the political order and sometimes undermine it."[41] The West is having a hard time contending with Arab and Muslim populations, as evidenced by the American imbroglio in Iraq as the United States failed to grasp the role of ethnicity in the vanquished country as well as the state's instability since its establishment.[42]

## Development of Human Terrain System: The American Experience

### *The Need for the Human Terrain System*

The Human Terrain System in the US military broadly refers to the organizational structure and work processes needed for conducting ethnographic field research and for developing the knowledge base that helps the military forces during security operations and in managing or resolving disputes. The ethnographic research is based on data collected in the field by small

[39] Kobi Michael, "Doing the Right Thing the Right Way," pp. 259–260.

[40] Ephraim Kam, "The Middle East as an Intelligence Challenge," *Strategic Assessment* 16, no. 4 (January 2014): 89-101.

[41] Ibid., p. 94.

[42] Ibid., p. 98.

teams of social scientists who intermingle with the local population and investigate its characteristics. They do this by conducting interviews and by various types of interactions with the local population.[43] More than 1,000 personnel were deployed during the years that the Human Terrain System was in operation. The overall cost of operating the system from 2007 to 2014 reached nearly USD 750 million, making the Human Terrain System the largest investment in a single social science project in the history of the US federal government.[44]

The American forces that contended with the local population in Iraq and Afghanistan needed to understand the force structure within the population and to map the potential influential leaders in the community. They also had to gain the trust of the local population as a means of reducing its support for the rebel organizations, while responding to the population's needs and improving its safety and welfare.[45] Debriefings at the Pentagon by commanders who returned from a tour of duty recounted the difficulties and limitations the forces encountered in navigating the conflict theater and contending with the rebel forces, which were caused, inter alia, due to the lack of requisite sociocultural knowledge.[46] The need for the Human Terrain System increased especially after the United States' major combat operations in Iraq ended in May 2003, when the main challenge became achieving postwar stability in the civilian arena, which required revising military operations and its preparedness.[47]

### *Characteristics and Organizational Structure*

The Human Terrain System in the American military is organized into two main categories: the deployed teams and the professional teams. The professional teams, comprising eight divisions, are headquartered in the

[43] Richard M. Medina, "From Anthropology to Human Geography: Human Terrain and the Evolution of Operational Sociocultural Understanding," *Intelligence and National Security* 31, no. 2 (2014): 137–153.

[44] Christopher Sims, "The Life and Death of the Human Terrain System," *Foreign Affairs*, February 4, 2016, https://www.foreignaffairs.com/articles/afghanistan/2016-02-04/academics-foxholes.

[45] McFate and Fondacaro, "Reflections on the Human Terrain System," p. 65.

[46] King, et al., "HTS Training and Regulatory Compliance," p. 16.

[47] McFate and Fondacaro, "Reflections on the Human Terrain System," p. 65.

United States and provide logistic, operational, training and research support to the various deployed command levels.[48]

The human terrain teams in the field perform their roles at four levels:

- Providing support to brigade-level commands;
- Providing support to division and higher-level commands;
- Coordinating the social science research and analysis between in-theater personnel and human terrain teams stationed at the theater headquarters and providing social science support to the theater headquarters;
- Professional accompaniment of operations.

### *Development of the Human Terrain System*

After an initial test of the concept in 2006, five human terrain teams were formed and deployed to support American military brigades in Afghanistan and Iraq. In the first evaluation report of the first team deployed to the Salerno forward operating base in Afghanistan in early 2007, the brigade commander and his staff credited the human terrain team with significantly improving the deployed forces' capacity to understand the local population, which enabled them to interact more successfully with it. The outcome was that, even before all five pilot teams had been deployed, the American military already requested the deployment of additional teams.[49]

Following the success of the initial teams, the Human Terrain System progressed from the "proof-of-concept" stage, which was carried out by external contractors, to the stage of "enduring capability" operated by civilian government employees and experts employed by the military and financed by a federal budget (from the Department of Defense).[50] The American General Staff recognized the significance of the requirements expressed in both the Operational Needs Statements and the Joint Urgent Operational Needs Statements[51] and responded by establishing a Human Terrain System at all command levels in the theater, from the brigade to the division levels.[52]

[48] Clinton et al., "Congressionally Directed Assessment of the Human Terrain System," pp. 15-17.

[49] Clinton et al., "Congressionally Directed Assessment of the Human Terrain System," p. 15.

[50] King et al., "HTS Training and Regulatory Compliance," p. 16.

[51] Ibid, p. 67.

[52] Steve Chill, "One of the Eggs in the Joint Force Basket: HTS in Iraq/Afghanistan and Beyond," *Military Intelligence Professional Bulletin* 37, no. 4 (2011): 11–15.

Within four years of its establishment, the experimental Human Terrain System evolved from an abstract concept to an institutionalized military program. It expanded from five teams to thirty; its annual budget was increased to USD 150 million; and it became an organization comprised of 530 professionals. Concurrently, the Human Terrain System's mapping software, the MAP-HT Toolkit, was developed and implemented in Iraq and Afghanistan, and an instruction and training program was developed and implemented to prepare the human terrain teams for deployment.[53]

The Human Terrain System was operated in forward and tactical "Village Stability Operations," alongside Special Operations Forces, all the way up to the strategic level. "Military and civilian personnel, regardless of rank or position, benefitted from the higher degrees of understanding, awareness and interpretation that social sciences frameworks offer." However, the efforts of the human terrain teams exacted a price when four of its members were killed while deployed in the field.[54]

### *The Tension between Military Intelligence and the Human Terrain System*

Following the development of the Human Terrain System, a debate ensued within the US military about the question of the placement and integration of the human terrain teams in the military's organizational structure. The debate focused on the uncertainty about stationing the teams together with the intelligence cells or the nonlethal cells (which are comprised of psychological operations and civil affairs units). Towards the end of 2008, it was decided to station the teams in the nonlethal cells.[55] The decision to not include them in the intelligence cells did not blur the intelligence purpose of the Human Terrain System. Cultural information, which is collected, input, processed, and analyzed by the human terrain teams and can contribute to the safety of the units and the local population, is considered military intelligence for all intents and purposes.[56]

[53] McFate and Fondacaro, "Reflections on the Human Terrain System," p. 64.

[54] Myron Varouhakis, "Challenges and Implications of Human Terrain Analysis for Strategic Intelligence Thinking" (Paper presented at the annual meeting of the Political Studies Association, Sheffield, 2015).

[55] Cristopher Sims, *The Human Terrain System: Operationally Relevant Social Science Research in Iraq and Afghanistan* (Carlise, PA: US Army College – Strategic Studies Institute, 2015), pp. 239–240.

[56] Ibid.

Counterinsurgency tactics in a densely populated theater amplified the tensions between intelligence and human terrain research. These tactics, which rely on cooperation with the local population in the confrontation theater and recruiting its support in the task force and for its objectives, have been described as "at least as important to our success as combat operations." Counterinsurgency operations, which require an in-depth understanding of the population and its culture, caused the conventional intelligence pyramid (strategic, systemic, and tactical) to become inverted. Information collected at the tactical level for the sake of carrying out the military mission among the civilian population became more important than intelligence at higher levels.[57] This inversion reflects the importance of developing human terrain intelligence at the tactical level for the purposes of generating high-quality intelligence at the systemic level and of formulating a relevant overarching strategy.

The clear link between intelligence and cultural research turned the work of the human terrain teams into a gray area, between the intelligence channel and the sociocultural information channel. The operational planning and the need to protect the safety of both the coalition forces and the civilians in the theaters of confrontation necessitated high-quality intelligence cultivated by a deep understanding of the human terrain.[58] In essence, the correlation between professional expertise, military intelligence, and sociocultural research may be defined as "cultural intelligence."

### *Test Cases in Iraq and Afghanistan*

In Iraq, the conflicts between the Yezidis, the Iraqi government, and the Kurdish forces exacerbated regional tensions in 2008. The Yezidis lived in an area of conflict between the Kurds and the Iraqi government. Topographically, this area extended over a region rich in oil; oil resources and their allocation were the subject of disputes and economic-political battles between the Iraqi central government and the Kurds.[59] Furthermore, English-language literature on the Yezidi culture was limited and rare, due to reluctance of social scientists to engage in this topic during the Ba'athist regime in Iraq,

[57] Ibid, pp. 240–241.

[58] Ibid.

[59] Ibid.

which intensified after the regime's downfall.[60] The social scientist Jennifer Clark identified and understood the characteristics of the dispute—which was being waged in an area without any military presence—and its complexity. Her sociocultural research led to a decision to separate the hawkish sides by deploying US Marines; this force sought to reduce the level of friction between the populations and curtail the violence.[61]

In Afghanistan, a social scientist from the Paktika district, who was researching the agricultural system in the region and understood the complexity of the region's water issue, recommended that the American military take part in supervising the irrigation system, which constituted a critical component of the local agricultural system.[62] As a result of this research, the State Department began implementing water management projects in Afghanistan. The projects aimed to improve the agriculture, raise the standard of living, and increase the employment of the male population, which was liable to join the rebels if the crisis in the agricultural system persisted.[63]

### *Conclusions from Implementing the Human Terrain System*

A decade of fighting in Iraq and Afghanistan led American military commanders and the human terrain teams to reach a broad consensus about the advantages of having access to sociocultural experts, sociocultural information, and the analysis thereof. These experts and information help the military to plan how to deal with the civilian population, carry out military operations, and evaluate their repercussions.[64] For example, the brigade commander of the 56th Stryker who served in Iraq in 2008, said the following about his human terrain team (HTT): "If someone told me they were taking my HTT, I'd have a platoon of infantry to stop him . . . The HTT has absolutely contributed to our operational missions. We succeeded in changing some situations that we would have resolved using lethal means, to situations where we use nonlethal means, on the basis of the HTT information."[65]

[60] Sims, *The Human Terrain System*, pp. 278–280.

[61] Ibid.

[62] Ibid, p. 282.

[63] Ibid.

[64] Mark Bartholf, "The Requirement for Sociocultural Understanding in Full Spectrum Operations," *Military Intelligence Professional Bulletin* 37, no. 4 (2011): 4.

[65] McFate and Fondacaro, "Reflections on the Human Terrain System," p. 64

Despite the appreciated contribution of the human terrain teams, it was still insufficient. The Afghanistan and Iraq Joint Urgent Operational Needs Statement reported gaps in operational capabilities: "US Forces continue to operate in Afghanistan lacking the required resident and reach-back sociocultural expertise, understanding, and advanced automated tools to conduct in-depth collection/consolidation, visualization, and analysis of the operationally-relevant sociocultural factors of the battle space."[66] The command in Iraq stated that "detailed knowledge of host populations is critical in areas where US forces are being increased to conduct counterinsurgency and stability operations in Iraq. US forces continue to operate in Iraq without real-time knowledge of the drivers of the behavior within the host population. This greatly limits Commanders' situational awareness and creates greater risks for forces."[67]

In response to the critique by Cristopher Sims on the Human Terrain System in the US military,[68] Thomas Mahnken proposed a number of recommendations to the decision makers in the US government and military, based on the experience amassed through the use of the Human Terrain System: first, recruit more immigrants and foreign-language speakers; second, strengthen the cultural and social expertise by increasing the number of officers who specialize in the social sciences, as opposed to the current emphasis placed on technology, engineering, and other math-based disciplines; third, obligate cadets to learn foreign languages during their military studies; fourth, offer military inductees additional opportunities to learn and work throughout the world with the aim of engaging with different cultures and acquiring important information and knowledge about them.[69]

## Criticism of the Human Terrain System

The Human Terrain System was the subject of controversy between some members of the military and the intelligence community in the United States and among some academics. The debate inside the military and within academic

[66] Ibid.

[67] Ibid.

[68] Sims, "The Life and Death of the Human Terrain System."

[69] Thomas G. Mahnken, "The Military and the Academy," *Foreign Affairs*, May 6, 2016.

and public circles generated substantial media coverage and prompted a discussion about the use of social sciences for national security purposes.[70]

*Criticism in the Military Establishment*

The criticism of the human terrain project within the military came mainly from the lower echelons in the American military[71] and from some social science researchers who had participated in the system's activities. They argued that the military had failed in implementing the project due to a "lack of professionalism, organization and general competence on the part of the staff, contractors and administrators [of the project]."[72] In response to the professional criticism, Pikulsky, Orton, Lamb, and Davis offered some observations and conclusions about the design, development, and implementation of the Human Terrain System:

a. The Pentagon was slow to set up a program for providing ground force commanders with sociocultural knowledge. The first human terrain team was deployed more than five years after the start of Operation Enduring Freedom, which began in October 2001, against the al-Qaeda organization in Afghanistan.

b. The Human Terrain System survived only because a new organization, the Joint Improvised-Threat-Defeat Agency,[73] had the flexibility to allocate resources to promising, new ideas and defined its mission broadly for launching a personnel-intensive program in a system focusing primarily on new technology.

c. The US Army Training and Doctrine Command had trouble meeting the high demands for human terrain teams from commanders in the field.

d. The Human Terrain System lacked a theoretical foundation, which was validated by field experience, and that could have been used to update

[70] McFate and Fondacaro, "Reflections on the Human Terrain System," p. 64.

[71] Ben Connable, "How the Human Terrain System is Undermining Sustainable Military Cultural Competence," *Military Review* 89, no. 2 (2009): 57–64, https://www.wired.com/images_blogs/dangerroom/files/MilitaryReviewConnableApr09.pdf.

[72] Zenia Helbig, "Personal Perspective on the Human Terrain Systems Program," (Paper presented at the annual meeting of the American Anthropological Association, Washington, DC, November 2007), https://www.wired.com/images_blogs/dangerroom/files/aaa_helbig_hts.pdf.

[73] The threats referred to here are improvised explosive devices, roadside bombs, and so forth.

its training program and instruct commanders how to utilize the full potential of the human terrain teams.

e. The Human Terrain System survived because commanders valued the contributions of the teams who operated it. The commanders' evaluations attested to the sparsity of the sociocultural knowledge amongst the American military forces, so that even the limited contribution of the Human Terrain System was considered vital.[74]

Sims added that the Human Terrain System was "a victim of its own success." Instead of forming five teams over two years, as originally planned, the American military formed more than twenty teams. As a result, many teams were deployed with inadequate equipment, and only a small number of them succeeded in completing their tasks reasonably. For example, in many instances, academics failed to conduct methodical research and were forced to make do with superficial PowerPoint presentations. According to Sims, the methodological and cultural gaps between academia and the military caused disruptions in the communications between them.[75] Furthermore, some social science researchers complained about the lack of adequate access to the local populations, as the military did not share its transport schedules to keep them safe from exposure. Some academics succeeded in acquiring information before the start of the mission, but the fast pace of the military operations constrained their ability to plan.[76]

### *Criticism in the Academic World*

Many in academic circles considered the Human Terrain System as problematic and nebulous, in ethical and academic terms, and some described it as neither research nor intelligence.[77] The majority who argued against the use of sociocultural information during a war focused on its potential use for controlling populations, for psychological warfare, or for targeting people

[74] Christopher Lamb, James Douglas Orton, Michael Davis, and Theodore Pikulsky, "The Way Ahead for Human Terrain Teams," *Joint Force Quarterly* 70, no. 3 (2013): 25–26, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_21-29_Lamb-et-al.pdf.

[75] Sims, "The Life and Death of the Human Terrain System."

[76] Ibid.

[77] AAA Commission on the Engagement of Anthropology with the US Security and Intelligence Communities, "Final Report on The Army's Human Terrain System Proof of Concept Program," 2009.

for incarceration, assassination, or other forms of violence, while being aided by academic methodologies and researchers. Some of its opponents drew comparisons between the Human Terrain System and controversial projects and operations previously carried out by the Central Intelligence Agency (CIA) in eastern Asia and Latin America. Furthermore, those opponents claimed that the Human Terrain System caused disastrous results among the local population, which included acts of violence, redistribution of populations, and agricultural poisoning, even though no evidence corroborated that the system was operated or was configured to operate in this manner.[78]

The American Anthropological Association (AAA) had reservations about the use of anthropologists in the Human Terrain System because of what it perceived as militarization of an academic/scientific discipline and as "unacceptable application of anthropological expertise."[79] In March 2010, the AAA sent a protest petition to the US Congress and Senate, which included four key arguments against the Human Terrain System. First, there is no proof that the Human Terrain System is effective. Second, it is a dangerous system—three social scientists were killed in the field (correct to 2009)—while others complained about deficient training, and the military personnel complained that protecting the human terrain teams jeopardized soldiers' lives. Third, it is a waste of public funds; and lastly, anthropologists and other social scientists believe it is unethical, because it contravenes scientific research standards and federal standards that prescribe the obligation to obtain the consent of the research subjects.[80]

### *The Human Terrain System in the American Military—Looking Ahead*

In 2015, reports were published about the supposed termination of the Human Terrain System project.[81] Despite this, the American government approved an allocation in its 2015 budget for an experimental human terrain program for the US Pacific Command, which was scheduled to end on September 30,

[78] Medina, "From Anthropology to Human Geography," pp. 142–143.

[79] AAA Executive Board, "American Anthropological Association's Executive Board Statement on the Human Terrain System Project," 2007.

[80] Ibid.

[81] Tom Vanden Brook, "Army Kills Controversial Social Science Program," *USA Today*, June 29, 2015, http://www.usatoday.com/story/news/nation/2015/06/29/human-terrain-system-afghanistan/29476409.

2016.[82] Moreover, in March 2016, a senior official in the US Department of Defense announced that it is unclear why the American military claimed that the human terrain project had ended; not only is the project still underway, but the military will be able to expand it if an additional budget becomes available.[83]

## The Perception of Human Terrain and Cultural Intelligence in the Israeli Context

Israel makes use of the Human Terrain System similarly to the way the American military uses it, when contending with similar actors and arenas in the Middle East—radical Islamic groups and terrorist organizations. Besides the similarities, however, there are significant differences between the two countries. First, the United States is fighting on distant continents, and the daily lives of its citizens are almost never affected by these wars. In contrast, Israel's battle is intensive and more tangible as it is waged in arenas either inside the State of Israel itself or along its borders, and, by its very existential nature, involves the nation's survival. The Israeli civilian society is involved in these wars and is affected by them—together with the IDF—far more than their counterparts in the United States.

Secondly, the American agencies' and institutions' handling of the subject of the culture of the enemy is a relatively new field. In contrast, the institutions and bodies in Israel that engage in the various aspects of the daily lives of the Arab population in the State, in the territories of Judea and Samaria, and in the Gaza Strip are very experienced, maintain intensive contact with this population, and have been familiar with its culture and characteristics for decades. The nature of the challenges that Israel faces, with its western lifestyle, obligates the country—as an existential compulsion relating to its very survival—to deeply familiarize itself with the various cultures in the region and their mindsets. The objective is for Israel to better understand who it is dealing with, militarily and politically, and to efficiently prepare itself to provide a suitable response.

[82] Roberto Gonzalez, "The Rise and Fall of the Human Terrain System," *Counterpunch*, June 29, 2015, http://www.counterpunch.org/2015/06/29/the-rise-and-fall-of-the-human-terrain-system.

[83] Tom Vanden Brook, "$725M Program Army 'Killed' Found Alive, Growing," *USA Today*, March 9, 2016.

### *The Importance of Understanding the Culture and Characteristics of the Local Population by the IDF and the Security Forces in Israel*

The document "the IDF Strategy," which was published in August 2015, states that, among the challenges facing the IDF are "a diminishing threat from state-standing armies and a rise in the threat from quasi-state, irregular, or semiregular organizations that are striving to become government entities," and the "deployment and assimilation of the enemy in settled civilian regions."[84] These challenges have compelled the IDF to contend with combat situations in densely-populated areas and to be familiar with the culture of that population, which spawn the terrorist organizations that it is fighting; superficial and inadequate familiarity with the enemy's culture is liable to cause strategic and operational errors.

The Coordinator of Government Activities in the Territories, Major-General Yoav Mordechai, referred to the change in nature of the battlefield, stating that

> Today, according to the IDF's approach, the population is a key component of any field analysis. In the past, it would analyze the enemy and the topography. Today, understanding the population, familiarization, understanding the infrastructure and the possibilities of evacuating it, are key factors in any operation. Before any operation, we map the sensitive sites . . . this does not mean that it cannot strike any location if it feels threatened. The component of civilian assistance is, first and foremost, a moral consideration, because we have no intention of hurting innocent civilians, but another task is to allow sufficient time for the military to complete its operational objectives.[85]

The chief of staff, Lieutenant-General Gadi Eizenkot, spoke about the importance and criticality that the military learn about the local population's culture and their environment, stating that "the initial tendency is to deal with the new acts of violence by pouring them into molds from the past. But we must realize that this is a new situation, and in order to deal with it, we need to understand the currents at work within the Palestinian society." He

[84] Chief of Staff's Office, "IDF Strategy" August 2015, http://www.idf.il/sip_storage/files/9/16919.pdf.

[85] Yiftach Carmeli, "The Coordinator of Government Activities in the Territories Unit: 'The Civilian Population is a Key Component of the Pre-combat Field Analysis,'" *IDF website*, December 2, 2014.

added that "militaries and intelligence organizations usually focus on two axis poles: one pole includes the opponent's decision-makers and command systems, and the other pole—its capabilities. The undercurrents at work on the opponent's side are a subject that is difficult to understand, and they are actually the most disturbing."[86]

Changes in the Palestinian arena in recent years have underlined even more the importance of acquiring cultural knowledge, especially about the structure of the sociopolitical power and the affiliations between the various population groups and their characteristics. Underlying the changes is the political and institutional weakness of the Palestinian Authority, which has failed to successfully manage the territories under its authority.[87] This weakness is expressed by internal power struggles—including violent ones—and by the development of alternative power structures, which have different and distinct characteristics in each geographic and/or demographic segment of the territories under the Palestinian Authority.[88]

In addition to changes in Palestinian society and politics, the events of the "Arab Spring" also led to geopolitical transformations in various Middle Eastern countries. These changes led to a new situation for Israel, in which it was forced to adapt to a reality in which most of the threats against it are not from countries but rather from ultra-national and sub-national systems and camps. These threats derive from the fragmentation, diversity, complexity, and multiplicity of interests of the various actors in the region. This situation requires Israeli intelligence to study the map of the Middle East differently than it had before. Moreover, Israeli intelligence must prepare itself for

[86] Gadi Eizenkot, "IDF Challenges 2015–2016," *Military and Strategic Affairs* 8, no. 1 (July 2016): 5–16, http://www.inss.org.il/uploadImages/systemFiles/ArmyStrategics8-1.01LtGenEizenkot.pdf.

[87] About the patterns of the Palestinian Authority's state failure, see Kobi Michael and Yoel Guzansky, *The Arab World on the Path to State Failure* (Tel-Aviv: Institute of National Security Studies, 2016), pp. 111–122.

[88] Pinhas Inbari, "The Palestinian Authority Continues to Crumble," *Jerusalem Center for Public Affairs* (blog), June 26, 2016, http://jcpa.org.il/2016/06/הרשות-הפלסטינית-ממשיכה-להתפורר/; Pinhas Inbari, "Is a Pro-Jordanian Political Power being Formed in Mount Hebron?" *Jerusalem Center for Public Affairs* (blog), June 1, 2016, http://jcpa.org.il/2016/06/האם-מתגבש-כוח-פוליטי-פרו-ירדני-בהר-/חברו; Pinhas Inbari, "The Refugee Camps—Growing Threat to the Stability of the Palestinian Authority," *Jerusalem Center for Public Affairs* (blog), August 9, 2015, http://jcpa.org.il/2015/08/מחנות-הפליטים-איום-גובר-על-יציבות-הרשו.

additional changes that are liable to occur, since the arena is dynamic and unstable.[89]

Yaakov Amidror emphasizes that the transformations in our region require "weighing the possibilities, thinking, and attempting to understand what needs to change in order to better cope with the new situation that has emerged." According to Amidror, the old frameworks, countries, ideologies, alliances, and rules have disappeared, and the new reality is being shaped largely by sociological processes that derive from the behavior of the masses and not from decisions by any leadership in a hierarchic entity; that is, a significant share of Israel's enemies are not countries. Added to this are the difficulties posed by the development of new technology: the new world is built on internet and cyberspace, creating a new intelligence universe with many opportunities and challenges.[90] According to Amidror, "The outcome, in terms of intelligence, is that a significant portion of the vast experience amassed in the system is irrelevant. For example, it is important to really understand the battle between the Shia and Sunna when Islam was first created, more than the battle between Egypt and Syria thirty-four years ago. New phenomena require a different perspective."[91] These developments reflect the complex reality in arenas of confrontation in proximity to Israel and the importance of creating a broad knowledge base about Arab societies, their power structure, political culture, and the prevailing attitudes so that Israeli forces can ensure operational relevance.

### *COGAT and GSS*

Two main bodies in Israel are in contact with the Palestinian population and with institutions of the Palestinian Authority and constitute centers of knowledge about pertinent issues: The Office of the Coordinator of Government Activities in the Territories (COGAT) and the General Security Service (GSS).

[89] Yossi Kuperwasser, "Outline of the Current Threats," in "IDF Challenges," *National Security Discussions,* no. 30 (August 2016): 9–15 (in Hebrew), http://besacenter.org/wp-content/uploads/2016/09/CSD30web.pdf.

[90] Yaakov Amidror, "The Intelligence Challenges," in "IDF Challenges," *National Security Discussions*, no. 30 (August 2016): 23–28 (in Hebrew), http://besacenter.org/wp-content/uploads/2016/09/CSD30web.pdf.

[91] Ibid., p. 23.

COGAT is responsible for coordinating activities of government ministries, the IDF, and the security agencies vis-à-vis the Palestinians, while ensuring that the relevant government civilian affairs policy is being implemented. COGAT also engages in promoting humanitarian issues, as well as infrastructural and economic projects in the West Bank and Gaza Strip.[92] In addition, COGAT focuses on foreign relations, including with international organizations, and has a public inquiries department, a spokesperson's office, and the Office of the Advisor on Palestinian Affairs. COGAT trains the next generation of coordination and liaison officers and provides courses in Arabic to various units in the security establishment.

The Civil Administration operates in Judea and Samaria under COGAT's authority and coordinates the activities vis-à-vis Palestinians and the Jewish settlements there. A Coordination and Liaison Administration office also operates in the Gaza Strip and is responsible for civilian, economic, and security coordination with the Palestinian side.[93]

The officers' training program in the Civil Administration includes many lectures on Islam, Palestinian society, the fundamentals of the dispute, the roles of the international organizations operating in the region, and an Arab language course. The training program also imparts an in-depth understanding of the rules of war and international law, which often constitute a basis for the IDF's activities in the territories.[94] Civil Administration officers in the various arenas maintain ongoing contacts and dialogues with Palestinian Authority officials as well as with unofficial sources from within Palestinian society. These channels of communication help Israel to develop its knowledge base about the local population, and these communications help both sides to maintain and deepen the coordination between them and adapt to changes and developments.[95]

The former director of the Civil Administration in Judea and Samaria, Brigadier-General David Menachem, spoke about the importance of cultural

[92] Coordinator of Government Activities in the Territories website, http://www.cogat.mod.gov.il/en/Pages/default.aspx.

[93] Ibid.

[94] Anshel Pfeffer, "The IDF is Trying to Improve the Handling of Palestinians," *Haaretz,* November 5, 2010, http://www.haaretz.co.il/news/politics/1.1228496.

[95] Liran Ofek, "Security Coordination is (Still) Here," *Shorty, Security at Eye Level* (blog), Institute for National Security Studies, October 12, 2015 (in Hebrew), http://heb.inss.org.il/index.aspx?id=5193&Blogid=10749.

knowledge and its contribution to the IDF's operational effectiveness in the context of Operation Brother's Keeper, during which the military was deployed throughout Judea and Samaria with the mission of locating three kidnapped Jewish teens who later were found to have been murdered by Palestinian terrorists. The realization that Hebron is considered one of the most important strongholds of the Hamas movement in Judea and Samaria derived, according to Menachem, from the understanding that "the Arab population in Hebron is more traditional, religious and less liberal than what you will find in Ramallah, for example, and the connection to the Islamic movement and to Hamas is natural . . .This does not mean that Hebron's residents are terrorists, but rather, that the cultural-religious-ideological platform in Hebron is closer to what Hamas is offering."[96]

This cultural knowledge assisted the IDF in deciding not to disrupt the daily lives of the Palestinian population in other areas in Judea and Samaria during Operation Brother's Keeper, and it continued to issue work permits there. The deputy director of the Coordination and Liaison Administration in Hebron, Major Moshe Tatro, explained that if an incident of the scale of Operation Brother's Keeper had occurred a few years earlier, the IDF's mode of operation would have been different.[97] This change may be attributed to the contribution of the cultural knowledge amassed over the years.

Another source of cultural knowledge in Israel is the General Security Service (GSS). A key portion of the training of field officers in the GSS begins in *ulpan*, the GSS's language school, which has been operating for forty-five years. During their training, the field officers acquire high proficiency in Arabic and are exposed to different dimensions of the cultural context, including the religious dimension of the Palestinian society.[98] The field officers' cultural knowledge is developed and enhanced due to the operational experience that they acquire in the field, although in recent years, it has been "remote learning," due to the limited access to Palestinian population centers, mainly in the Gaza Strip. During Operation Protective Edge, GSS field officers were deployed alongside the Nachal Brigade officers during the take-over of territory in northern Gaza. The Nachal Brigade officers were

[96] Yiftach Carmeli, "One Year After Operation Brother's Keeper: How the Operation Affected the Palestinian Population in Hebron," *IDF website*, December 6, 2015.

[97] Ibid.

[98] Amir Bohbot, "Exposé: The Secret World of the Shadow Forces Fighting Terrorism," *Walla*, April 24, 2015, http://news.walla.co.il/item/2843137.

impressed by the level of expertise that the field officers demonstrated and commended them for their scope of knowledge and command in the field, despite having never set foot in Beit Hanoun.[99]

A similar contribution may be attributed to the interrogators of captives, who are deployed with the combat forces and are responsible for obtaining intelligence by questioning captives in the theater and by interrogating captives who are transferred to prisoner camps in the rear. The professional training processes of interrogators of captives impart them with a relatively deep understanding of cultural aspects, which is important for engaging interrogees. The former head of the GSS, Yaakov Peri, explained that

> You must have an in-depth understanding of the territory under your purview. You need to be a professor of your particular territory and you must be well versed in the socioeconomic, economic, political, and social aspects of the diverse populations that live in it—you must be familiar with the influential clans and organizations, you must know the streets and every detail that will help you control your territory.[100]

Notwithstanding the growing awareness of the importance of the cultural dimension within the organizations described above, this dimension is still not enough developed and does not yet have a sufficient impact on their intelligence work processes (collection, processing, and dissemination), mainly in relation to macrosocial aspects. The materiality of cultural intelligence has not yet been assimilated in the processes of training, force-building, or in the operating doctrines of COGAT, the Civil Administration in the territories, or the GSS, and it has also not yet been translated into routine, orderly and methodical cooperation with academic researchers and their integration into the various levels of the intelligence research network.

## Conclusions

The Human Terrain System in the American military was created and developed due to the challenges posed by fighting in densely populated theaters. The evolution from classic warfare to war against jihadist terrorists, to counterinsurgent operations and peace-keeping operations in other countries and on other continents compelled the combat forces to change their patterns

[99] Ibid.

[100] Ibid.

of activity. This change led to a need for high-quality intelligence about the non-state opponent operating from inside the civilian population and under its protection.

Acquiring a deep understanding of the local culture is a vital condition for ensuring the relevance of the military mission. It became evident that cultural intelligence, as a means of correlating the cultural knowledge created by the Human Terrain System and the intelligence needed for carrying out the military mission, is essential. In order to guarantee high quality cultural intelligence, both cultural awareness and sensitivity are needed, which together are an expression of intercultural competence.

The recognition of the importance of cultural intelligence led the American military, which has been operating in geographically and culturally remote and complex arenas in recent decades—such as Iraq, Afghanistan, and Syria—to develop the Human Terrain System. This system is based on professional teams of social scientists, who are embedded in forces at various levels and whose role is to help the forces in the combat theaters gain an understanding of the culture and the society. Commanders and team members who took part in the human terrain program widely agreed that the Human Terrain System contributes to the relevance and success of the military mission. However, alongside the importance attributed to the system, its operation also sparked criticism, both in military and in academic circles. Despite the criticism, and contrary to reports of termination of the program, the US Department of Defense announced that the program will continue and that additional resources might also be allocated to it.

Since it is reasonable to assume that the United States will continue to be involved in operations against insurgents and terrorists in the Middle East, the need to understand the society and culture in the operating theaters will be critical, particularly given the emergence and strengthening of the Islamic State, in addition to the commitment of the US-led coalition to destroy it. Such an understanding can also be important to the United States in sustaining existing alliances and developing new political relations in Asia, Europe, Africa, and South America. Cultural intelligence has become essential input in the era of "wars amongst people." Despite this, and despite the methodological, operational, and organizational developments of the Human Terrain System in the American context, gaps still exist and, in many cases, the deliverables are inadequate.

Gaps in knowledge of cultural matters also exist among the security and intelligence agencies in Israel; their assimilation in the combat doctrine and the intelligence methodology is not optimal. Given the characteristics of combat in densely populated theaters with which the IDF contends, it is recommended to develop information collection and research capabilities, alongside training methodologies and processes in the field of cultural knowledge in the various arenas, and to receive assistance from social scientists and integrate them both in the processes and in the organizational frameworks. This will facilitate the development and improvement of Israel's knowledge base about neighboring cultures.

# A Cooperative Approach between Intelligence and Policymakers at the National Level: Does it Have a Chance?

David Siman-Tov and Shay Hershkovitz

The proximity of relations between intelligence officers and policymakers and the balance between the aspirations of the intelligence officers to influence the decision-making process and their primary professional duty to gather accurate intelligence is an ongoing argument within the intelligence discourse. Other discussions focus on whether the primary professional duty of the intelligence officer is merely to create intelligence or also to actively shape policy, and whether strategic intelligence is a product of research groups in the intelligence community or of a dialogue between intelligence and the policymaker, ultimately leading to new strategic knowledge that facilitates the formation of a national policy.

We argue that the development of knowledge for shaping policy on the strategic level should be done in a cooperative manner—in a meeting between intelligence officers and decision makers. The lack of suitable conditions in the space between intelligence and policymakers, however, prevents this in many cases. The limited ability of the intelligence community and the political echelon to act cooperatively and develop a facilitating framework of mechanisms and learning processes should therefore be recognized, in addition to the intelligence community's limitations and the characteristics of the strategic environs.

David Siman-Tov is a senior researcher at the Institute for National Security Studies.
Dr. Shay Hershkovitz is a lecturer in political science at Tel Aviv University.

This article reviews the main approaches concerning the interface between policymakers and intelligence—the traditional approaches versus what we call the "cooperative approach." It proposes an approach that regards intelligence on a national level as a joint project of intelligence officers and policymakers. At the same time, the article analyzes the tension and obstacles in implementing this approach and proposes possible ways of overcoming them.

**Keywords**: Strategic intelligence, national intelligence, intelligence community, policymakers, intelligence circle

## Introduction

Much has been written about the complex relations between the civilian and military establishments and specifically policymakers and intelligence officers. Already in the 1940s, with the establishment of national intelligence institutions, pioneering attempts began in the United States to devise and shape the theory of intelligence in the context of the space between the policymaker and intelligence. Then, as now, the main argument focused on the question of how closely intelligence officers should work with policymakers, and what the balance should be between intelligence officers' aspirations to influence the decision-making process and their primary professional duty to gather intelligence reflecting the most accurate situation. Other arguments have focused on whether the intelligence officer's primary professional duty is merely to create intelligence, or also to be an active partner in shaping policy, and whether strategic intelligence is a product of research groups in the intelligence community, or a product of a dialogue between intelligence and the policymaker—the latter who both influences and is influenced—ultimately leading to new strategic knowledge that facilitates the formation of a national policy.[1]

Already at the dawn of intelligence, which was designed as a state institution to provide strategic information, questions were asked about its role on the strategic level: What should be its place in determining and implementing policy? Should intelligence exist in its own right? Does intelligence generate

[1] This discussion echoes a broader debate in social studies—whether knowledge can be separated from the person who knows it, and whether objectivity with respect to human behavior is possible. For an interesting discussion on this point, see Richard Bernstein, *Beyond Objectivism and Relativism* (Philadelphia: University of Pennsylvania Press, 1983), pp. 1–50.

output allegedly unconnected to the shaping of national strategy, or does it constitute, in the words of former head of Israeli Military Intelligence Directorate Yehoshafat Harkabi, "a policy tool?"[2] These questions concern two facets. The first is the way parties outside the intelligence system perceive the function and role of intelligence. The second is how the intelligence system perceives itself.

## Strategic Intelligence

Before delving into the complicated relations between the heads of the intelligence community and policymakers, strategic intelligence should be specified as a research output of the intelligence agencies and a result of the discourse between intelligence and the decision makers. The function of strategic intelligence is to aid policymakers in formulating a general outlook, shaping policy, and making decisions in national security. It must provide assessments for aiding and enabling policymakers to understand the situation, manage risks, and take advantage of opportunities. Intelligence should also challenge current policy by describing gaps in the understanding of the strategic environment, outlining strategic trends, and assessing the observer's future place in the strategic environment.

A key question here concerns the perspective that an intelligence agency chief should have in providing strategic intelligence: Can intelligence, in talking about the "other," remain indifferent and closed off in an "intelligence ivory tower" when addressing the policy of the policymaker to whom it is reporting? Furthermore, does the involvement of intelligence in policy matters blind the intelligence officers and make them biased in their provision of relevant strategic intelligence, or would separation of intelligence from the policymakers make the assessments of intelligence officers irrelevant, because they will not be used? Should strategic intelligence focus only on intelligence tasks, or is its role to facilitate discussion and inspire discourse in which policy is eventually devised and decisions taken at a national level?

[2] David Siman-Tov and Shay Hershkovitz, *Israel Military Intelligence* (Tel Aviv: Directorate Press, IDF Publishing House, 2013), pp. 52–53.

## The Traditional Approaches to Policymaker-Intelligence Relations

The traditional approach holds that intelligence should be as distant as possible from the decision makers and independent of their interests; otherwise, it runs the risk of becoming another player—one of many—in a discussion about policy, thereby committing a double error: intelligence is liable to present a "non-objective" picture and mislead the policymaker, and it will lose its authority as the main party representing the "real situation" in the strategic discussion led by the decision maker. The main advocates of this approach were William Donovan, Allen Dulles, and Roscoe Hillenkoetter—three of the forefathers of American intelligence.[3] They believed that intelligence officers should maintain a certain distance, albeit not totally cut off, from the decision-making process; intelligence officers should conduct research and make independent assessments, and refrain from judgments tailored to the decision maker's ideological and political considerations.[4]

This approach also was supported by Sherman Kent,[5] at least at the beginning of his academic career, when he wrote in 1949 that the intelligence at the national level was a "service function," and should refrain from contaminating the intelligence output with subjective judgments resulting from direct contact between the information consumer and the information. Kent thereby shaped the concept of the intelligence officer as a producer and the policymaker as a consumer; in other words, two substantially and operationally separate functions. According to Kent, intelligence is

[3] Donovan headed the Office of Strategic Services (OSS) in World War II, and is regarded as the founder of the CIA. Hillenkoetter was the first director of the CIA in 1947–1951, and Dulles was director of the CIA in 1953–1961.

[4] They presumably were influenced by the positivistic discourse prevailing at the time among American academics, who enshrined "scientific" (i.e., objective) investigation in social studies fields. For a review on this subject, see Peter Halfpenny, *Positivism and Sociology: Explaining Social Life* (London: Allen and Unwin, 1982).

[5] Sherman Kent was a professor of history at Yale University, before beginning a seventeen-year career in the OSS and CIA during World War II. He headed the CIA research institute and is considered the most prominent theoretician in national intelligence and influential in shaping the American intelligence community. His influence continues until today in writing about intelligence and the practice of intelligence.

obligated to respond to requests by the decision maker, but must maintain the independence and objectivity of the intelligence process.[6]

In his description of the relations between the producer and the consumer, Kent cited several problematic aspects. First, the decision makers are inherently skeptical towards the intelligence product. This is because intelligence officers tend to accept only limited responsibility for the intelligence product (particularly when forecasts are involved), which does not contribute to the decision makers' confidence in the intelligence they receive. Kent therefore believed that intelligence should make clear its function as an outside observer of the phenomenon being investigated, and do this objectively, which would enable the policymaker to make the right decisions concerning the necessary policy. Second, Kent argued that excessive closeness between the producer and the consumer impairs the objectiveness of the intelligence, has a detrimental effect on the confidence of the intelligence "consumer" in the "producer" (which is, in any case, limited), and counteracts the basic purpose of the intelligence. In order to remain relevant, intelligence nevertheless must have some degree of proximity to the decision makers, but must not get too close so that it does not lose its objectivity and professional integrity.[7] Donovan best expressed this approach when he said, "Intelligence must be separate from the people it serves, so that the materials it obtains will not be distorted by the outlook of the people directing the intelligence activity."[8]

Kent therefore proposed to subject the contact between intelligence officers and the policymaker to a rigorous regime, because a gap in expectations is liable to emerge between the two sides in the absence of institutionalized channels of communication. In addition, Kent was concerned that the decision maker would impose impossible tasks on intelligence, causing the intelligence officers to adopt an apologetic attitude. He therefore advocated creating mechanisms and institutionalizing work processes that would enable a policymaker to provide orderly direction for intelligence work. Such direction would build confidence between the two sides and allow intelligence to succeed in its task.

[6] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1949), p. 200.

[7] Ibid, p. 180.

[8] William J. Donovan, "Central Intelligence Agency," *Vital Speeches* 12, no. 14 (May 1946), p. 428.

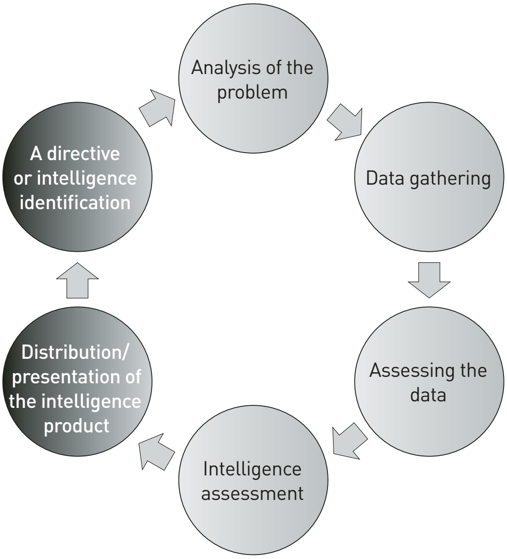
Kent developed the concept of the "intelligence circle," in which he described a "minimal interface between intelligence officers and the political echelon,"[9] with most of the knowledge-development process and thinking to occur within the intelligence system. Kent described a linear process with six stages. The first stage is when a strategic problem appears or is detected due to a directive issued by a policymaker, or when intelligence discovers something out of the ordinary through intelligence gathering. The second stage is the analysis of the problem, which takes place among the intelligence groups themselves. The third stage focuses on gathering information about the problem, which takes place among the intelligence research groups. In the fourth stage, the intelligence research groups assess the data, while comparing the new to the familiar. The fifth stage is formulating a hypothesis, i.e., making an assessment based on the information gathered. In the sixth stage, the intelligence output is presented and disseminated to the policymaker. In the first and last stages, a meeting takes place between the intelligence groups and the policymaker.

Researchers have made efforts over the years to perfect the intelligence circle concept. They have assumed that the basis of producing the knowledge is virtually an exclusive product of intelligence, and accordingly have adjusted and revised the concept. For example, Amos Jordan and William Taylor added elements of management and coordination to Kent's basic concept of the circle. These are part of the basis of the "intelligence circle," which can be perceived as a kind of gear surrounded by six other smaller elements.[10]

[9] Kent, *Strategic Intelligence for American World Policy*, pp. 159–164.

[10] Amos Jordan and William Taylor, *American National Security: Policy and Process* (Baltimore and London: Johns Hopkins University Press, 1981).

Figure 1: The Intelligence Circle According to Sherman Kent


Analysis of the problem
Data gathering
Assessing the data
Intelligence assessment
Distribution/ presentation of the intelligence product
A directive or intelligence identification

In the blue circles, an interface exists between intelligence and the decision makers. In the green circles, internal processes take place within the intelligence community. A directive is an instruction by the political echelon that identifies a problem. Alternatively, it is possible for intelligence to detect a problem and bring it to the policymaker's attention.

A post-traditional approach developed later, based on the traditional approach. This approach does not regard intelligence as the only element nor necessarily as the most significant one in the decision-making process. Jack Zlotnik argued in favor of a closer connection between the intelligence officer and the decision maker, given the fact that the intelligence officer must contend with other parties for the decision maker's attention. In his opinion, reducing the distance between the intelligence officer and the decision maker renders the intelligence officer more prominent and enables him to better understand the effect of intelligence on the decision-making process, which in turn improves the intelligence work.[11]

[11] Jack Zlotnick, *National Intelligence* (Washington, DC: Industrial College of the Armed Forces, 1964); Jack Zlotnick, "Bayes, the Forum for Intelligence Analysis," *Studies in Intelligence* 16, no. 2 (Spring 1972): 43–52.

In addition to describing the real situation, the post-traditional approach holds that intelligence should also present the decision maker with the possible consequences of implementing policy. At the same time, it stresses the need for a clear distinction between the creator of intelligence and its consumers, particularly in all matters pertaining to the structural aspects. For example, John Huizenga asserted that although an ongoing dialogue between the two was needed, since intelligence was an inherent part of the decision-making process, intelligence should strive to provide as objective a picture as possible and should not be subjected to the policymaker's considerations.[12]

Since the beginning of national intelligence in Israel, the traditional approach has been dominant. Academics and intelligence officers repeatedly have emphasized the need for intelligence to remain "pure" and faithfully reflect the existing situation, without being distracted by the policymaker's political considerations.[13] According to them, reality, with all its complexity, could be revealed by perfecting intelligence gathering, and the job of the intelligence officer at the national level was therefore to understand and interpret reality and make this interpretation accessible to the decision maker.[14]

As noted, intelligence officers are not the only ones who advocate this approach. It can also be found among some policymakers. The Israeli situation is unique in this context, because Israeli policymakers, such as Moshe Dayan, Yitzhak Rabin, Ezer Weizman, Ariel Sharon, and Ehud Barak, frequently have had military and defense experience. At times, some of them preferred that intelligence provide them with raw data, interpret only infrequently, and not intervene in decision making. Others believed that since they bore the responsibility, it was better for them to assess the intelligence by themselves without any filtering by intelligence officers. Furthermore, a series of painful intelligence failures engraved in Israeli history and the investigative

[12] Huizenga was a member of the US State Department Policy Planning Council in 1964–1966, and later deputy director of the CIA Office of National Estimates. The above remarks appear in his testimony before the Murphy Commission, which dealt with the US administration's organization for handling foreign affairs. For the full report, see research.policyarchive.org/20213.pdf.

[13] Uri Bar-Yosef, *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain* (Pennsylvania State University Press, 2004).

[14] Colonel Y., "The Other Within Us—the Intelligence Officer between Objectivity and Relevance," *Maarachot* no. 434 (2010): 52-59, (in Hebrew), http://maarachot.idf.il/PDF/FILES/5/112575.pdf.

commissions that followed made the decision makers realize that they could not always avoid bearing responsibility for the decisions they made, even if these decisions had been recommended by the intelligence officers. For this reason, also, decision makers have tended to regard intelligence assessments with caution, not to mention with suspicion.

Another phenomenon discernable in Israel is the tendency of some policymakers to refrain from involving the intelligence community in political initiatives. Examples of this include the peace initiative with Egypt, the Oslo process, the withdrawal from Lebanon, and the disengagement from the Gaza Strip. The reason for this is strict compartmentalization and the desire to keep the circle of those involved as small as possible in order to prevent leaks in the early stages; moreover, it may also reflect the policymakers' disinclination to regard the intelligence community as a partner in making decisions and formulating strategy.

## Problems with the Traditional Approach

The traditional approach regards knowledge in general and intelligence knowledge in particular as something "real" if it constitutes an accurate portrayal of reality and "correct" if it faithfully describes the state of affairs as it "really" is. This is applied to both limited and broad portrayals, as well as concrete, physical, and abstract ones and extends the concept of a "factual report" to more consciousness-related and abstract realms. A key contention in the criticism of the traditional approach is that in contrast to the tactical environment, in which knowledge is universal, knowledge in the strategic environment cannot be detached from the ones who know, including their perspective and interests.

In order to illustrate this, we will consider an intelligence problem from the realm of tactics, in contrast to that of strategy. A tactical question is likely to be the location of tanks at a certain point. The answer to this question is exact, absolute, and rests on a factual basis: whether the platoon is at a specific point. The answer is not subject to the observer's interpretation, because any observer, regardless of identity, can see the platoon of tanks in satellite photographs. What is involved, therefore, is universal knowledge.

A question on the strategic level is likely to be whether the enemy regime is stable. The answer to this is interpretive and depends, among other things, on the intention, interests, perspective, and policy of the person who asks the question. For example, is the reference to political, economic, or social stability, or stability and instability in the sense of replacing the policymaker or the entire governmental system? What aspect of stability of the enemy regime is relevant to the questioning party who is able to change the state of strategic affairs? Is the person who asks the question a head of state, such as Syria's President Assad or Egypt's President el-Sisi, for whom stability is a matter of survival? Is it an external party—such as Israel or the United States—for which stability may relate to the existence of a peace agreement or the permanency of an entire region, such as the Middle East?

In contrast to the presence or absence of tanks in a specific location, stability as a strategic question depends on the observer's perspective and the interpretation given. If we take the Israeli governmental system as an example, many Israelis perceive it as stable, even if the average lifespan of Israeli governments is a little more than two years. On the other hand, a foreign observer is likely to regard the Israeli system as suffering from chronic instability, making investment in the country risky.

Another problem arising from the traditional approach involves the above-mentioned "intelligence circle" concept. The concept of "gathering" (of intelligence reports) constitutes a metaphor for the compiling of facts collected, which is the task of the intelligence officer. From that perspective, the concept of "processing" reflects the idea that the intelligence officer connects the pieces of information to form a broad and complete picture of the "real" situation. According to the traditional approach, the intelligence task is equivalent to a jigsaw puzzle, with no room for subjective interpretation, other than formulating an assessment, which supplements the missing parts of the puzzle. The practice of national intelligence work, which characterizes the relationship between the intelligence officer and the political echelon, is therefore one of separation and unilateralism. The intelligence officer is usually required to give an assessment at the beginning of a discussion, or to communicate the conclusions and assessments in a written review. In other words, assessing the enemy precedes discussing the formulation of a policy towards the adversary. Thus, in the strategic intelligence environment, the intelligence assessment precedes the political action, as in the battlefield, in which the intelligence information precedes the operation.

## The Cooperative Approach

The close contact between the American intelligence officers and decision makers during the 1960s and the series of intelligence failures during the 1970s led to a change in the approaches and for advocating a clear and inflexible separation between intelligence and decision makers. The intelligence failures in the Vietnam War, press leaks about the CIA's sensitive intelligence operations, and revelations that the CIA was conducting operations without the approval and knowledge of the political echelon led to the establishment of investigative commissions. These commissions reconsidered the work of the American intelligence services and fostered the formation of a new approach in intelligence work, which, for the purposes of this article, will be called the "cooperative approach."[15] The existence of clandestine activity by the American intelligence services, without the knowledge of the political echelon, caused members of these committees to recommend not only institutionalized oversight but also the establishment of mechanisms for improving the connection between intelligence and policymakers. The committees recommended that a channel for direct personal dialogue, sometimes informal, should be developed between intelligence officers and intelligence consumers, because the relationship between the two parties are essentially symbiotic, and close work relations between them should be regulated through organizational mechanisms and verification of two-directional communication of information and feedback.

Notably, one of the main supporters of the cooperative approach, Professor Willmoore Kendall of Yale University had published as early as 1949—many years before this approach became popular—an article entitled "The Function of Intelligence," in which he took issue with the arguments raised in Sherman Kent's book.[16] Kendall believed that the role of intelligence was to help decision makers influence and shape reality. He therefore saw nothing

[15] Prominent commissions include the Schlesinger Committee in 1971; the Rockefeller Commission, which published its findings in June 1975; and the Church Committee, which was appointed by the US Senate and published its reports in April 1976. It is interesting to note that another investigative commission formed three decades later (the 1996 Aspin-Brown Commission) reached the same conclusions as the Church Committee about needing closer relations between the decision maker and the intelligence officer.

[16] Wilmoore Kendall, "The Function of Intelligence," *World Politics* 1, no. 6 (1949): 452–453.

wrong with close relations between the two, and he even argued that such relations were necessary and desirable. Like Kent, Kendall also believed that the decision maker should be the one guiding the intelligence officer. In contrast to Kent, however, he went on to assert that intelligence helps decision makers influence reality by clarifying the ways in which events around the world influence—and are likely to influence—national security. Intelligence officers therefore cannot separate themselves from their own perspective, because it constitutes an integral part of their work.

Roger Hilsman,[17] one of the authors of American intelligence theory, favored the approach expressed by Kendall, holding that intelligence should be encouraged to consider how its assessments affect the range of possibilities placed before the decision maker. Hilsman argued that intelligence officers should not be isolated from the party for whom they create their product. According to Hilsman, intelligence officers work for the decision makers and serve their goals by providing them with the background necessary for assessing situations and making decisions,[18] in contrast to the opposite situation, described well by Robert Jervis, of "keep[ing] intelligence pure when it is irrelevant."[19]

William Brands also believed that the intelligence product should be useful to the decision makers, and the intelligence community should therefore have a good understanding of their needs. Thus, the intelligence officer should be in the proximity of the decision maker. According to Brands, the needs of the decision maker are like a beam of light that directs the intelligence gathering and the research efforts, while at the same time the decision maker gives feedback about the intelligence information received.[20]

Adoption of this approach by the policymakers within the American intelligence community can be seen in Robert Gates' speech in 1992, shortly

[17] Hilsman was a professor of political science recruited to the American army in World War II and then continued to national intelligence. In his last position, he served as director of research in the US State Department.

[18] Roger Hilsman, *Strategic Intelligence and National Decisions* (Glencoe: Free Press, 1966); Roger Hilsman, "On Intelligence," *Armed Forces and Society* 8 (Fall 1981:129–143; Roger Hilsman, *The Cuban Missile Crisis: The Struggle Over Policy* (Westport: Praeger, 1996).

[19] Robert Jervis, "What's Wrong with the Intelligence Process?" *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986): 39.

[20] William J. Brands, "Intelligence and Foreign Policy: Dilemmas of a Democracy," *Foreign Affairs* 47 (1969): 288.

following his appointment as director of the US Central Intelligence. Gates emphasized that the open dialogue had to exist between intelligence and the policymaker, particularly given that none of the parties involved in the strategic discussion was immune to errors: "No one has a monopoly on the truth; we are all learning new things every day . . . Dialogue must take place, each participant must be open to new ideas, and well-grounded alternative views must be represented."[21]

Gates claimed that the interaction between intelligence officers and decision makers is a meeting in which the two sides conduct a dialogue and jointly create knowledge, and not a one-sided, linear event in which only the intelligence officer gives information to the policymaker:

> Getting the policymaker to read our product should not jeopardize our objectivity; it does not mean sugarcoating our analysis. On the contrary, it means providing a frank, evenhanded discussion of the issues. If we know that a policymaker holds a certain viewpoint on an issue that is different from our analysis, we ought not lightly dismiss that view but rather address its strengths and weaknesses and then provide the evidence and reasoning behind our own judgment.[22]

In contrast to the popularity of the traditional approach in Israel, the cooperative approach is regarded less highly, and most who support it are intelligence officers. They are inclined to blur the procedural aspect formalizing such cooperation. They stress the trust of the two sides as the key to partnership, as well as the idea of shared responsibility.[23] Senior commanders in the Israeli intelligence community, such as Itai Brun, former head of the Research Department of the Military Intelligence Directorate, have also emphasized recently that the job of intelligence officers should not be confined to clarifying the situation and presenting it to the policymaker. In Brun's opinion, they should also be involved in shaping policy on the various levels.[24]

[21] Robert Gates, "Guarding Against Politicization," *Studies in Intelligence* 36, no. 5 (1992): 8.

[22] Ibid.

[23] Gershon Hacohen, *What is National in National Security* (Ben Shemen: Ministry of Defense Publishing House, Modan Publishing House, 2014) (in Hebrew).

[24] Itai Brun, *Intelligence Analysis: Understanding Reality in an Era of Dramatic Changes* (Tel Aviv: Israel Intelligence Heritage and Commemoration Center – IICC, 2015), p. 42.

In his testimony before the State Comptroller, who investigated Operation Protective Edge in Gaza in 2014, former head of the Military Intelligence Directorate, Major General Aviv Kochavi emphasized that the military commanders and the political cabinet did not need to be passive listeners to the intelligence evaluations. In his view, they should have taken part in the process of scratching at the intelligence and should have cooperated in analyzing and interpreting the information. From his perspective as the head of the Military Intelligence Directorate, Kochavi notes that the dialogue with the cabinet enriches the intelligence analysis, and he emphasizes that assessment bodies, even if they have reliable sources, need to be exposed to criticism.[25]

Among the prominent advocates of the cooperative approach is former head of the Military Intelligence Directorate of the Israel Defense Forces (IDF) Moshe Ya'alon, who also served in key IDF command positions (head of the Central Command and chief of staff) and in the government. In a recent interview, Ya'alon noted that the processes of joint learning and thinking between the political and intelligence echelons are essential for developing an appropriate strategy, and he also had practiced cooperation, in which the discourse had taken place in a non-hierarchal fashion and without "ceremony," both in the framework of his positions in the army and when he was minister of defense. At the same time, Ya'alon stated that the political echelon is not always able to reveal its intentions to the military-strategic echelon, particularly the intelligence echelon, and is entitled to preserve strategic ambiguity. In such cases, the intelligence community must develop the ability to analyze the intentions of the political echelon and its directive, so that it can direct intelligence efforts in a way that will assist in the designing of an appropriate strategy.[26]

The point of departure in our theoretical approach to the desirable pattern of relations between the intelligence officer and the decision maker is what we call the "cooperative approach." This approach rests on a fundamental assumption that does not regard intelligence knowledge as referring to an independent objective reality by the observer. Thus, we do not regard

[25] State Comptroller, "Operation Protective Edge," (February 28, 2017), p. 75 (in Hebrew).

[26] Interview with Moshe Ya'alon, conducted by David Siman-Tov, Institute for National Security Studies, October 6, 2016.

intelligence as an “institution for discerning reality”[27] in isolation from the observer. As we see it, the objectives, values, and strategic interests of the observer of intelligence, and even the fact that the observer has been selected to watch the subject of a given study—rather than someone else—all constitute an essential framework for the way in which reality is interpreted. We therefore oppose the concept that regards the development of knowledge about an environment or enemy as an exclusive project of intelligence, and we do not regard the intelligence output as the final step in the intelligence process—that is, as a “product” placed on the table of the “consumer”—but rather as the opening point of a discourse and the development of shared knowledge.

Our approach emphasizes three dimensions in the role of intelligence on the national level. The first is the change in the perception of intelligence as clarifying reality by “discovering” the truth, simply because it does not exist on the strategic level. The second is that the quality of the intelligence assessment is based on its relevance to the decision maker, and not on its ability to reflect the “objective” reality. The third dimension emphasizes the need for policymakers and intelligence officers to cooperate in creating conditions for an open dialogue and to develop knowledge at the national level with the aim of designing and implementing policy.

## From Facts to Interpretation

As noted, the knowledge necessary for designing a successful strategy is abstract knowledge, which is conceptualized in a concrete context and reflects an idea and interpretation, rather than real information. In contrast to the intelligence information in a tactical environment, intelligence at the strategic, national level is developed by the intelligence officer and is not received as intelligence information. The challenges here that face the intelligence community are materially different than in the earlier approach: the intelligence officer does not collect factual information, but rather interprets and conceptualizes the enemy’s situation as a basis for a fruitful discourse with the policymaker, so that it can serve as a platform for devising policy. In most cases, this conceptualization cannot be judged as “correct”

[27] Yitzhak Ben-Israel, *The Philosophy of Intelligence* (Tel Aviv: Ministry of Defense Publishing House, 1999) (in Hebrew).

or "incorrect," because it reflects only a possible concept used in forming a concrete policy, and not a universal one.[28]

It should be emphasized that the switching of the intelligence community from facts to interpretations does not mean that it has abandoned the factual sphere. Interpretation in a strategic environment rests on facts obtained at the tactical level. In the switch from objectivity to relevance, the intelligence community must carefully avoid compromising the professional integrity of the person who observes the facts, thereby enjoying an advantage over other partners in the strategic discussion. In this context, intelligence enjoys a double advantage: it has a unique access—and sometimes an exclusive one—to the factual level and is among the few parties around the discussion table accustomed to the knowledge-development processes that are essential to decision making.

## From Objectivity to Relevance

Although approaches that emphasize relevance at the expense of objectivity and even deny the possibility of being objective are sometimes heard, leaders of the Israel intelligence research community—like the American community—favor efforts at achieving objectivity, or at least maneuvering between objectivity and relevance. The CIA website, for example, emphasizes the need for objective research:

> Members of the DA (CIA Directorate of Analysis) help provide timely, accurate, and objective all-source intelligence analysis on the full range of national security and foreign policy issues to the president, Cabinet, and senior policymakers in the US government.[29]

As noted, aiming for objectivity in intelligence information is futile, because information and knowledge will always be relative and dependent on the observer. We therefore wish to abandon the principle of evaluating the quality and role of intelligence in the context of objectivity and replace it with the principle of its relevance to decision making. Josh Kerbel and Anthony Olcott

[28] Thomas L. Hughes, "The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making," *Headline Seri*es 233, (December 1976): 5; Richard Betts, "Policy-Makers and Intelligence Analysis: Love, Hate or Indifference?" *Intelligence and National Security* 3, no. 1 (1988):184–185.

[29] See the CIA website, https://www.cia.gov/offices-of-cia/intelligence-analysis/index.html.

have expressed well this principle as a criterion for evaluating intelligence in dealing with decision makers at the national level.[30] They argue that a synthesis between intelligence and decision makers is needed, in which intelligence would no longer be merely a provider of information, but also would provide knowledge and ideas. This requires a two-fold change: first, decision makers must expose their policy to intelligence and ask questions about more than just data.[31] Second, intelligence officers must be involved in formulating recommendations and must overcome their reluctance to do so, which has prevented them from including the consequences of their forces' activity in their assessment. According to Kerbel and Olcott, dialogue and cooperation will render it impossible to speak about policy successes or intelligence failures, because they will be intertwined. Another change results from the shift from the need to study policy and adapt intelligence assessments to the needs resulting from this policy. Kerbel and Olcott argue that with the new synthesis, intelligence will provide what is needed, not what it has. The new intelligence officer will learn to accept political and strategic goals as legitimate and proper.[32]

Developing such a pattern of intelligence, which includes shaping policy, is liable to cause tension between the intelligence officer and the decision maker. According to Kerbel and Olcott, an intelligence officer who does not identify with the proposed policy should resign, although the risk exists that in the absence of tension between the two sides, intelligence would become a tool for the policymaker[33] (as was alleged concerning Western intelligence assessments on Iraq in 2003).[34] In Kerbel and Olcott's opinion, the main achievement of this approach, beyond making intelligence relevant, was that

[30] Josh Kerbel and Anthony Olcott, "Synthesizing with Clients, not Analyzing for Customers," *Studies in Intelligence* 54, no. 4 (2010): 11–27.

[31] Ibid.

[32] Ibid.

[33] Yehoshafat Harkabi, *Intelligence as a State Institution* (Tel Aviv: IDF Publishing House, 2015), p. 71. Harkabi, who was chief of the IDF Military Intelligence Directorate and later served as a strategic advisor to the Ministry of Defense and as a strategic consultant for the prime minister, called this approach "intelligence tailoring."

[34] Paul R. Pillar, "Intelligence, Policy and the War in Iraq," *Foreign Affairs* (March–April 2006).

decision makers had a partner with whom they could consider, ask questions, and formulate an appropriate policy, if they wanted to.[35]

## From a Producer/Consumer Dichotomy to a Partnership

Policymakers need a partner so that they can, together with intelligence and other parties, understand the limitations and weak points of the players in the strategic environment and consider them when shaping a successful strategic policy. The task of formulating a strategy is therefore a joint task led by the policymakers in which intelligence plays a special—albeit not exclusive—role, because it is supposed to bring insights and interpretations about the strategic environment into the discourse. At the same time, the knowledge brought by intelligence does not stand on its own (as described in Kent's "The Intelligence Circle"); joint processes of developing knowledge and formulating insights also are involved. Presenting intelligence insights about the environment as a topic itself, without reflecting upon the observer's insights, is meaningless.

In view of the above, formulating a system of strategic insights concerning a strategic environment or enemy must include intelligence officers and policymakers. We therefore seek to eradicate the traditional dichotomy that distinguishes between producers and consumers of intelligence and to regard them as partners—at least on the theoretical level—even if unequal ones. We do not propose completely doing away with Kent's "intelligence circle" concept. As we see it, however, its first and final stage should take place in a close and interactive interface between intelligence and the policymaker, which makes the pattern of their relations a two-sided one.

The following table summarizes the distinction between the traditional approach and the active cooperative one that we are advocating.

[35] Kerbel and Olcott, "Synthesizing with Clients."

Figure 2: A Comparison between the Traditional Approach and the Cooperative Approach[36]

| Traditional Approach | Cooperative Approach |
|---|---|
| What do you want to know? | What do you want to achieve? |
| Focused on threats | Focused on opportunities |
| Refers to the past | Refers to the future |
| Inclined to be tactical | Must be strategic |
| Output | Process, dialogue |
| Searches for comparisons and analogies | Tries to detect what is unique |
| Interested in objects | Interested in context and affinities |
| Introverted | Extroverted |
| Tends to focus on what went wrong | Makes it possible to also evaluate what succeeded |
| Rewards sharpness with large systems, more personnel, specialties, and broad plans | Rewards imagination, flexibility, accommodation, and is less hierarchal, and more networked. |
| Gathering | Cognition—insight |

## Problems in Implementing the Cooperative Approach

The cooperative approach appears to be an accepted practice in the interface between the intelligence community and military policymakers, such as the command intelligence officer, who is an integral part of the study group led by the commander. At the same time, over the years, real difficulties have emerged in implementing the cooperative approach on the national level, i.e., in the interface between the intelligence community and the political echelon. We believe that the reason for this lies in the behavioral and structural characteristics of both the policymaker and the intelligence officer, as well as in the tensions that are typical of the national environment.

A fundamental tension exists in the strategic environment between the perspective of the intelligence community, some who want to describe the future, and the perspective of the policymaker, who aims to shape the future.[37] Policymakers frequently believe that intelligence officers tend to expand uncertainties in the world in which the policymakers act, instead

[36] This table is based on a table in Kerbel and Olcott, "Synthesizing with Clients," p. 22.

[37] Hans Heymann, "Intelligence and Policy Relationships," in *Intelligence Policy and Processes*, ed. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle (Boulder: Westview Press, 1985), pp. 57–66.

of reducing them. The policymakers need solutions, while the intelligence assessments mainly pose challenges and rarely provide the policymakers with solutions. Furthermore, the intelligence community is inclined to qualify its assessments and to outline a range of scenarios that are frequently described in a vague fashion. Policymakers often want intelligence to provide them with forecasts, but intelligence officers who adhere to the status of prophet cannot be loyal partners for policymakers in the complete sense of the word.

Another important obstacle in implementing the cooperative approach is that policymakers usually do not want to share their covert considerations and intentions with the intelligence community. Policymakers are anxious about leaks and sometimes do not wish to be challenged, preferring instead to promote a specific outlook, without having a professional party cast doubt on it. An additional problem is the absence of a common language between the policymaker and the intelligence officer. For policymakers, the intelligence community's language is unclear, or at least it does not reflect the levels of certainty they need for managing risks.

Furthermore, there is not always a direct connection between intelligence assessments and decision making. Sometimes policymakers make decisions in isolation from the intelligence assessment and do not involve the intelligence community's insights about the environment and its players; rather, these decisions reflect other considerations stemming from the policymaker's perspective. Furthermore, decisions are sometimes made contrary to the intelligence assessment, because the difference in an intelligent officer's perspective and that of a policymaker is likely to result in varying—not to mention contradictory—interpretations of reality.

Another problem is that the decision maker receives information about the strategic environment from a wide range of information sources, most of which are not intelligence sources. This is especially true now, in which everyone has access to a huge mass of information, interpretations, and various insights; policymaker even have their own sources. Policymakers can ask themselves, sometimes with justification, whether the intelligence community can add any value to alternative interpretations, which are directly available to them and may reflect a policymaker's own outlook.

In addition, policymakers have an advantage over the intelligence community in understanding the strategic system, particularly when they have experience and personal ties with other policymakers around the world.

The policymakers usually show a profound understanding of the way the international system works, which is liable to keep them from regarding the intelligence community as a partner, especially if the intelligence community stresses military threats at the expense of diplomatic opportunities. The nature of the policymakers' political agenda is liable to hinder any partnership between policymakers and intelligence—policymakers are interested in knowledge about civilian companies, economics, and culture in contrast to the intelligence community, which emphasizes military threats. This gap could make it difficult for the policymakers to regard the intelligence community as a partner, even if they want to do so.

We have so far described mainly the difficulties and obstacles that prevent the policymakers from regarding the intelligence community as a partner. At the same time, intelligence officers also face obstacles that may prevent them from regarding themselves as partners. These obstacles can result, for example, from the intelligence community's profound adherence to the traditional approach and from the nature of the intelligence output. In many cases, this output does not encourage dialogue; rather, it seeks to describe end results, which even then are often not clearly formulated.

The combination of these two-directional obstacles and especially the lack of mutual recognition by the two sides that the cooperative approach constitutes a genuine opportunity for an open strategic dialogue between the intelligence community and the policymakers make implementing this approach a very difficult task.

## Conclusion

Limitations and obstacles stand in the way of achieving a synthesis between the intelligence community and decision makers, including the decision makers' wish to avoid exposure and/or to be committed to a policy, their concern about leaks, and a bureaucratic and conceptual tradition. Other significant barriers include principles of producer-consumer relations, which are still quite dominant in the national intelligence discourse, as well as the striving for (imaginary) objectivity.

A changing pattern of relations between the intelligence community and policymakers is only now beginning. The idea of cooperative relations between the two sides appears to be the correct direction and should therefore be shaped accordingly in order to provide an optimal response to the current challenges facing both policymakers and intelligence officers. The preliminary condition for creating such a transformation is a desire to change, as defined by Kerbel and Olcott.[38] Furthermore, the cooperative concept needs to be recognized—along with the new potential it entails—so that the policymakers and the intelligence community can apply it. Although this concept may not be suitable for all policymakers, a substantial effort is required by those for whom it is appropriate. If intelligence officers are interested in encouraging an open dialogue with the policymakers, they should present policymakers with output that does not purport to "predict the future" at the strategic levels, because these forecasts will only create distance between them and the policymakers. Policymakers are more likely to regard the intelligence offers as partners if they are given output that presents a range of possibilities and enables the policymakers to manage risks.

If the policymakers are interested in changing the pattern of relations with the intelligence officers, the policymakers must create conditions for an open dialogue with the intelligence community, and allow it to voice different and challenging opinions. The policymakers must build relations of trust with the intelligence officers and inform them of their plans and doubts to the greatest possible extent. For their part, the intelligence officers must respond to this trust by discretely maintaining the policymakers' confidence and preventing leaks.

The partnership between the intelligence community and the policymakers at the strategic level cannot be taken for granted; both sides must make a major effort at implementing a partnership. At the same time, such a partnership has the potential for a new type of dialogue that will contribute to both utilizing intelligence and devising a better strategy.

[38] Kerbel and Olcott, "Synthesizing with Client."

# Comparative Assessment of Indian and Israeli Military Strategy in Countering Terrorism

Vinay Kaura

Prime Minister Narendra Modi of India recently compared his country's cross-border response against terrorists in Pakistan—following the attack in Uri in Indian-administered Kashmir—to Israel's pre-emptive and retaliatory raids across its borders. This has given rise to serious debate about whether it is desirable for India to adopt Israeli military strategy. A country's history, political culture, and dominant discourse of national security greatly influence policymakers and their communities. With that in mind, in this article, it is argued that the fundamental differences in strategic orientation, diplomatic posture, and military tactics in India and Israel explain their different approaches and priorities in responding to terrorism. Due to the different circumstances in which the Israeli and Indian militaries operate, co-opting Israeli counterterrorism strategies would be very challenging for India.

**Keywords:** India, Israel, Arab, terrorism, insurgency, civil-military, Israeli military, Indian military, Kashmir, Palestinian, cybersecurity, border

## Introduction

Israel as an example to emulate has become an important topic in strategic circles and academia in India since Narendra Modi, India's prime minister, compared the two country's armed forces. Speaking at a public function in

Vinay Kaura, PhD, is an assistant professor in the Department of International Affairs and Security Studies, and coordinator, Center for Peace & Conflict Studies Jaipur, Sardar Patel University of Police, Security and Criminal Justice, Rajasthan, India.

the Indian state of Himachal Pradesh in October 2016, Prime Minister Modi likened the Indian army's targeted action a month earlier against terrorist launching pads across the Line of Control (LoC) in Pakistan-administered Kashmir to Israel's policy of targeted military actions and assassinations. He said that "our army's valour is being discussed across the country these days. We used to hear earlier that Israel has done this. The nation has seen that the Indian Army is no less than anybody."[1]

Whether Modi's observation in Himachal Pradesh was tailored for his political supporters or indicated a decisive transformation in India's strategic culture remains to be seen. But benchmarking Israel as the ideal of military action would certainly situate it within the broader narrative of Indian military strategy. The prime minister's comments and the subsequent widespread resonance in all quarters raise several questions. Does India have institutionalized structure and mechanisms in place that can be compared to Israeli standards? If not, should India aspire to match Israeli standards?

Central to the inherent volatility and instability in the Middle East is the United Nations (UN) decision in 1947 to partition the former British mandate of Palestine into two states: one Jewish and one Arab. In fact, Palestine was the first issue that the UN General Assembly was called upon to adjudicate. Rejecting the partition plan, the Arab states immediately declared war on Israel. Failing to resolve the issue with the 1948 war, the Arab states then maintained a war of attrition against Israel that was punctuated by two wars, the 1956 Sinai War and the 1967 Six-Day War. President Nasser of Egypt nationalized the Suez Canal in 1956 and set in motion the events that would lead to war in October 1956, in which Israel attempted to capitalize on British and French anger over Nasser's abrupt and unexpected nationalization move.

In 1967, many Arab states made a concerted effort to eliminate the Jewish state, but were pre-empted by a successful Israeli attack. The Six-Day War fundamentally altered the territorial, strategic, and psychological landscape of the Middle East, with Israel capturing territory from Syria, Jordan, and Egypt. After that, the Arab aim changed from eliminating the Jewish state to recapturing these territories. In the 1973 War, known as the Yom Kippur War, Egypt and Syria launched a surprise attack to regain the lost territories. Initially the Israeli military suffered heavy losses, but soon the tide turned and the Israeli military pushed the Egyptians and Syrians back to their original

[1] PTI, "PM lauds Indian army," *Hindu,* October 19, 2016.

lines. In 1981, Israel invaded Lebanon, with the aim of silencing the artillery attacks by the Palestinian Liberation Organization (PLO).

Although Israel has signed peace treaties with Egypt (1979) and Jordan (1994) and has begun a peace process with the PLO, the conflict has remained intractable. Israel has faced two major Palestinian intifadas in the West Bank and Gaza since the late 1980s. It must not only prepare its armed forces for a major interstate war, potentially against Syria or Iran, but also for counterterrorist and counterinsurgency operations. In addition, the Iranian-backed radical Shia militia, Hezbollah, has maintained guerrilla operations against Israeli soldiers and civilians along the Israeli border, which sparked an interstate war in 2006. Israel's cross-border attack on Hezbollah in Lebanon in 2006 can be defined as a case of extraterritorial law enforcement.

## Strategic Orientation

Security, survival, and sovereignty are the root of Israel's strategic orientation. Israeli strategists feel a sense of geostrategic vulnerability. Israel's lack of territorial depth has exerted a strong influence on its strategic doctrine. One cannot forget that in 1948, Israel's territory was quite small and narrow, and Jerusalem was not included within its borders, until the city was divided between Israel and Jordan by the 1949 cease fire. The victory in the 1967 War was a watershed event as the occupation of the West Bank, East Jerusalem, the Golan Heights, the Gaza Strip, and the Sinai Peninsula gave Israel much greater strategic depth than it had at its inception.[2] It can well be argued that this initial lack of territorial depth made it imperative that Israel fights battles beyond its own borders.

Existential fears also drive Israel's nuclear program, as does the assessment that in the event of military defeat in a conventional war, the nuclear option would come to Israel's rescue. Nuclear weapons are considered an insurance policy in case Israel is faced with extreme military and political exigencies, such as loss of its conventional military edge or acquisition of nuclear weapons by an Arab state. Israel's nuclear program embodies the country's preference to maximize power and freedom of action.[3] The Israeli

[2] Greg Cashman and Leonard C. Robinson, *An Introduction to the Causes of War: Patterns of Interstate Conflict from World War I to Iraq* (Plymouth: Rowman and Littlefield, 2007).

[3] Efraim Inbar, *Israel's National Security Issues and Challenges since the Yom Kippur War* (New York: Routledge, 2008).

perception of the Iranian nuclear program as an existential threat should be seen in this context.

The impact of the Holocaust gave new meaning to Zionism and left deep scars upon the State of Israel. The Holocaust is one of the largest mass annihilations of human beings in modern history; thus, the need for security has become a fundamental component of Israel's DNA. The emphasis placed on the exceptional price that the Jewish people paid for its national right is a reference to the Holocaust, which is used as both a source and justification for Israel's offensive security doctrine. It was by force of this doctrine that Israeli planes bombed the Osirak nuclear reactor in Iraq in June 1981 as well as a suspected Syrian nuclear site in September 2007. The justification for the 1982 Lebanon War was also based on the lessons of the Holocaust, as the Israeli leadership understood them.[4]

Analysis at this level implies that Israeli strategic planning has realized three important objectives: securing Israel's existence; defending Israel's territorial integrity; and gaining an upper hand in terms of power vis-à-vis Israel's enemies. Indeed, Israel has substantially advanced its relative position of power because it has managed to distance key Arab states from coalitions that seek to attack it. Moreover, Israel has several times withstood the test of war.

India's strategic perspective also has been shaped by historical and geographical factors as well as by the geopolitical realities it has faced at different periods. Beginning with independence in 1947 until the end of the twentieth century, India responded to the regional and global geopolitical situation based on its own security perceptions. During this phase, the India's security discourse was most influenced by the Cold War, when external threats in the dynamics of a bipolar world were the primary sources of insecurity; in contrast, nuclear weapons were perceived as providing a security guarantee. Strategic policy making was not institutionalized, and India's charismatic political leaders, notably Jawaharlal Nehru and his daughter, Indira Gandhi, determined India's strategic vision. The end of the Cold War and India's

[4] Guy Ben-Porat and others, *Israel Since 1980* (New York: Cambridge University Press, 2008).

nuclear tests in 1998, however, dramatically changed both its security perceptions and strategic perspective.[5]

India's contemporary strategic orientation is shaped by many aspirations and challenges that are quite unique. India is among the world's largest countries, both demographically and geographically, and its industrial and technological base is huge. A declared nuclear-weapon state with impressive space capabilities, India cannot but play an important role both regionally and globally. India is the natural leader in South Asia as it occupies almost three-fourths of the region's territory and population. India's borders, which are land- and sea-based, riverine and mountainous, are long and porous, making neighborly relations extremely difficult to manage. Most importantly, the borders have not been completely delineated and demarcated.

India is locked in an enduring conflict with its smaller neighbor, Pakistan.[6] The core dispute remains Kashmir, which Pakistan claims on religious grounds. Since 1947, India and Pakistan have fought three major and one minor war. India has also been fighting terrorism in several parts of the country and carrying out an asymmetric war in Kashmir. Pakistan increased its support for insurgency in Kashmir as it acquired nuclear capability. The introduction of nuclear weapons to the arsenals of both adversaries has since increased the potential costs of conflict. Nonetheless, both India and Pakistan have engaged in frustrating, intermittent, and ineffective peace talks aimed at settling their border disputes. The India-China dyad constitutes another rivalry in the region.

The challenges India faces from outside forces, such as Pakistan and China, may not be existential, but are still daunting. Until India reaches an understanding with Pakistan, peace and stability in South Asia is not possible. Growing instability and insecurity in Afghanistan has far-reaching implications for India. Effective international cooperation on terrorism is still a major challenge. The emergence of violent non-state actors confronting the Indian state has seriously affected national security. The internal threats to India in the shape of communal and social violence are also formidable.

[5] C. Raja Mohan, *Crossing the Rubicon: The Shaping of India's New Foreign Policy* (New Delhi: Viking, 2003).

[6] Sumit Ganguly, *Deadly Impasse: Indo-Pakistani Relations at the Dawn of a New Century* (Cambridge: Cambridge University Press, 2016).

## Military Tactics

Israel's security situation is precarious. Israel is surrounded by states and non-state entities that it has fought since its creation in 1948. Such conflicts include the War of Independence in 1948, the Sinai War in 1956, the Six-Day War in 1967, a war of attrition with Egypt in 1970–1971, the Yom Kippur War in 1973, the First Lebanon War in 1982, the First Intifada in 1987–1993, the Al-Aqsa Intifada in 2000–2005, the Second Lebanon War in 2006, and the Gaza War in 2014, also known as Operation Protective Edge. Iran, which does not share a border with Israel, has also expressed open aggression toward Israel. As far as non-state adversaries are concerned, Israel faces threats from Hamas and Fatah in the West Bank and Gaza; in Lebanon, Hezbollah continues to pose a danger to Israel.

The foremost priority of the Israeli military is to protect the state's sovereignty and territorial integrity. Israel has responded to its adversaries by building a military that relies on quality rather than quantity. It invests heavily in high-tech weaponry, recruits its armed forces through mandatory national service, and maintains a reserve force comprised of a significant portion of the country's population. The most salient trait of the Israeli military distinguishing it from most other national armies is the extraordinary impact it has had on the country's social structure.

There are two aspects of Israeli military operations. The first is covert operations that are designed to foil terrorist strikes and deter assaults on Israeli citizens. The second is a series of wars and military operations. Israel has been involved in direct military action for decades now. Israel's military's performance against its external adversaries like Egypt and Syria has been outstanding. The destruction of the Egyptian air force on the eve of the Six-Day War in 1967 was a coup that led to the imbalance of the Arab front. Israel's capacity to withstand the shock of the Yom Kippur War in 1973 and even turn the tables by launching a counterattack across the Suez Canal and over the Golan Heights was a stupendous military feat.

After years of adapting to the challenges of the intifadas, the Israeli Army also has become highly competent in addressing what it calls low-intensity conflict threats. Nonetheless, Israel found itself struggling to fight what its strategists refer to as high-intensity conflict (HIC) in Lebanon in 2006. The Israeli experience in Lebanon demonstrates that intense combat is not so much about scale as it is about the qualitative challenges posed by hybrid adversaries. Based on their experiences, the Israelis have reoriented the focus of much of their training in HIC with greater success.[7]

India has primarily geared its military strategy to wage interstate wars with both conventional and nuclear arsenals. Pakistan, India's arch rival, has focused its military strategy exclusively on waging a war against India. Nevertheless, Indian policy is far more complicated as it focuses on interstate wars with an emphasis on containing local insurgencies and small-scale border wars. However, recent experience does not provide any strong evidence that the Indian military has shifted away from interstate warfare.[8] This analysis finds credence in the argument of Rajesh Rajagopalan, who writes that "the Indian Army has been able to adapt to counterinsurgency to a limited extent, and that the primary limitation has been the strong conventional war bias in the doctrine."[9]

The ambiguity and controversy surrounding the Cold Start war doctrine is a stark reminder that India faces huge gaps between its doctrinal aspirations and its capabilities. At its core, the Cold Start doctrine, which emphasizes rapid mobilization and limited territorial objectives, is designed to attack and destroy Pakistan's military forces in "punishing blows" in retaliation for terrorist attacks against India, without triggering wider conventional or nuclear escalation. Although India's new army chief, General Bipin Rawat, has referred to the existence of this doctrine in a recent interview,[10] others have said that "there is still no evidence that India has the required capabilities to implement anything resembling Cold Start."[11]

## Comparative Assessment

Many Indians have mentioned on numerous occasions that India can use Israel as a model on issues involving military operations. It can be argued that both

[7] David E. Johnson and others, eds., *Preparing and Training for the Full Spectrum of Military Challenges: Insights from the Experiences of China, France, the United Kingdom, India, and Israel* (Santa Monica: RAND, 2009), pp. xx, xxvi.

[8] Norrin M. Ripsman and T.V. Paul, *Globalization and the National Security State* (New York: Oxford University Press, 2010), p. 126.

[9] Rajesh Rajagopalan, *Fighting Like a Guerrilla: The Indian Army and Counterinsurgency* (New Delhi: Routledge, 2008), p. 29.

[10] General Bipin Rawat, interview by Sandeep Unnithan, "We Will Go Across Again," *India Today*, January 16, 2017, pp. 13–14.

[11] Vipin Narang and Walter C. Ladwig III, "Taking 'Cold Start' Out of the Freezer?" *Hindu*, January 11, 2017.

India and Israel face strategic environments that require their armed forces to prepare for a mix of internal and external threats. These threats demand militaries that are trained, organized, and equipped for conventional and low-intensity operations. Adapting their militaries to low-intensity conflict or small wars has been a gradual process as organizational dynamics have led them to prefer preparing for conventional war; nonetheless, in several areas they have made efforts to adapt to the new situation, with varying degrees of results.

The fact that Israel must prepare its military for a variety of threats makes the country a good point of comparison with India. As the Indian military has learned in Kashmir and in Northeast India, violent, non-state actors—despite being labelled "low-intensity threats"—can be very difficult to handle. In addition to low-intensity threats, India's military must also prepare to deal with state adversaries who are armed with nuclear weapons. Thus, Israel's recent experience in dealing with both an insurgency in the Palestinian Territories and a well-equipped militia in Lebanon—while maintaining its readiness for operations against Iran and Syria—can be a useful model for the Indian military.

On the macro level, India's military certainly can learn from Israel's methods for homeland security. When it comes to specific issues, however, Israel's experience may not be relevant in terms of augmenting India's security environment. The following factors are worth noting for making any comparison between operations and campaigns undertaken by the militaries of India and Israel.

## Offensive vs. Defensive Strategies

Much of Israel's military behavior has been derived in part from long-term military conflicts and partly from Israel's geographic and demographic limitations. Consequently, the Israeli military has developed a military doctrine that involves fighting battles outside Israel's borders. In simple terms, Israel's national defense is offensive; it uses preemptive strikes as an important factor in its military strategy. On the other hand, India's military posture has been largely defensive. Although its military plans have catered to offensive actions against Pakistan, executing these plans has been difficult. Even when there was sufficient evidence that the terror attacks against the Indian parliament in 2001, in Mumbai in 2008, and the Pathankot airbase in

2016 were planned and masterminded by terrorists in Pakistan, the Indian government did not take punitive actions.

Israel's land mass and population is less than 1 percent of India's. Israel has fought wars with all its neighbors, and its relations with these neighbors have been tense due to territorial disputes. Israel lacks not only strategic depth, but also faces a real sense of geopolitical insecurity. This is an important reason for the country to push its defensive front beyond its borders, including offshore and into foreign territory. India, on the other hand, has sufficient strategic depth against its adversaries. After the Indian military's recent surgical strikes across the LoC, Prime Minister Narendra Modi said that "India has not attacked anyone. It is neither hungry for any territory."[12]

Israeli leaders tend to publicly threaten Israel's neighbors with military action, which are often reinforced by Israeli actions. The credibility of Israel's determination to use its military power increased significantly after Menachem Begin came to power in 1980. His hawkish image abroad obviously enhanced Israeli deterrence. Begin was more willing to use force than his predecessors to achieve political ends beyond Israel's borders.[13] Israel's Prime Minister Netanyahu, a vocal critic of his predecessors' so-called dovishness, also enjoys the reputation of being extremely tough on Hamas and Hezbollah. Despite his seemingly hardline orientation and aggressive public posturing, India's Prime Minister Modi has not yet acquired a hawkish image. He has yet to come up with an equivalent of the "Begin Doctrine," which holds that Israel would act pre-emptively to counter any perceived threat to its existence.

## Civil-Military Relations

A symbiotic relationship exists between Israel's citizens and its armed forces, with the latter acting as a unifying force for the whole of Israeli society. There is near unanimity among researchers that the military has had a central, if not dominant, role in shaping Israel's security policy. Although the military is subordinate to the political leadership in Israel, it is an equal partner in the security and foreign policy-making process. The uniqueness of Israeli civil-military relations is demonstrated by the fact that the military, which

[12] "India has never attacked or been hungry for territory, only fought for others: PM Modi," *Indian Express*, October 3, 2016.

[13] Inbar, *Israel's National Security Issues and Challenges since the Yom Kippur War*, p. 16.

is “deeply involved in the political process, influences both the political echelon and the public by its knowledge and persuasive argumentation, and still obeys the political echelon.”[14]

The very foundation of the concept of a “nation in arms” or a “citizens’ army” is rooted in Israel’s almost universal conscription policy, which was implemented due to Israel’s early numerical inferiority relative to its Arab neighbors. This policy fosters a strong bond between society and the military. While undergoing the compulsory military service, all Israelis learn to live together and share a common aim of defending their homeland. Even after becoming civilians, the Israelis continue to remain “soldiers on eleven months’ annual leave,” as Yigal Yadin, Israel’s second chief of staff had remarked.[15] An analyst has critically noted that “Israel is not so much a state that has a military; rather, it is a leading example of a militarily fueled society that codifies and mobilizes a state in its image.”[16] Because of the dominance of the military establishment in Israel, the distinction between civilian and military leaders is hard to determine. Military leaders, both retired and serving, continue to exert substantial influence on aspects of Israel’s politics, society, economy, and culture. Upon the conclusion of their military career, military leaders often seek second careers in the civilian sector. It is no accident that Ehud Barak, Ariel Sharon, and Yitzhak Rabin, all top military leaders, rose to the position of prime minister.

Paradoxically, the preponderance of Israel’s security establishment has often made it easier for top generals and spymasters to challenge the inflexible and tough policies of some prime ministers. Prime Minister Netanyahu has been gradually marginalizing the security establishment, which has been critical of some of his policies. The appointment of Avigdor Lieberman as defense minister in May 2016 has been perceived as an act of retaliation against the security establishment. Hardliner Lieberman is known for his harsh

[14] Kobi Michael, “The Dilemma behind the Classical Dilemma of Civil-Military Relations: The “Discourse Space” Model and the Israeli Case during the Oslo Process,” *Armed Forces and Society* 33, no. 4 (2007): 518–546.

[15] Ahron Bregman, *Israel’s Wars: A History Since 1947* (New York: Routledge, 1947), pp. 46–47.

[16] David Theo Goldberg, *The Threat of Race: Reflections on Racial Neoliberalism* (Victoria: Wiley-Blackwell, 2009), p. 137.

criticism of the Israeli military's conduct, and always demands aggressive measures against the Palestinians.[17]

Since Moshe Dayan's appointment as defense minister in 1967, the post of defense minister has been given to politicians with significant security background, apart from Menachem Begin (1980-1981), Amir Peretz (2006-2007), and now Avigdor Lieberman. However, Lieberman's appointment—likely to be a temporary phenomenon—should not be perceived as the end of the military establishment's dominant role in the Israeli political process.

On the other hand, India's civil-military framework is heavily tilted in favor of the civilian leadership. The military is discouraged from participating in the political process and is isolated from civil society. India's civilian bureaucracy almost completely dominates the security processes and top positions in the national security structures. The military leadership usually does not communicate its differences of opinion with the civil leadership to the media and the public.

The contours of the civil-military interface in independent India were formed during the tenure of Prime Minister Nehru when his controversial defense minister, V.K. Krishna Menon, set in motion several organizational changes, which the armed forces vehemently opposed. Given the way that India's political leadership handled the operational planning before and after the disastrous 1962 war with China, it became amply clear that purely operational matters must be left to the military's discretion. Since then, a tradition seems to have been established where broad operational directives are laid down by the political leadership, and the actual planning of operations is left to the military leadership.[18] Thus, for example, the military has continued to exercise its veto on operational issues such as withdrawing from Siachen Glacier and revoking the Armed Forces Special Powers Act (AFSPA) in some contentious areas.

Although retired Indian military leaders have been appointed as ambassadors and governors of states, unlike in Israel, they rarely become active in politics, and when they do, they do not play a significant role. General V.K. Singh, a former army chief, was elected to the parliament in 2014. This is only

[17] Isabel Kershner,"Naming of Israeli Defense Minister Augments Netanyahu's Alliance," *New York Times*, May 25, 2016.

[18] Harsh V. Pant, "Indian Strategic Culture: The Debate and its Consequences," in *Handbook of India's International Relations*, ed. David Scott (London: Routledge, 2011).

the second time when a former army chief has entered the parliament since the appointment of General Shankar Roychowdhary. Moreover, General Singh holds the position of a junior minister in the government and not in the Ministry of Defense.

Growing demands have been made to give the military a prominent role in the decision making of India’s national security. Those advocating for the enhanced role for the military strongly criticize India’s dysfunctional civil-military relations and lack of initiative in reforming the defense acquisition processes. It is argued that Indian democracy has been successful in maintaining a system of strong civilian control over the military, but has adversely affected the quality of strategic decision-making.[19]

## Diplomatic Environments

Israel and its opponents in the Middle East rarely interact as Israel only has diplomatic relations with two of its neighbors, Jordan and Egypt. Israel has not established diplomatic relations with Syria, Saudi Arabia, UAE, Qatar, Iraq, or the other major regional powers—much less Iran— as its relationship with these countries is marked by long-standing hostility. For example, Israel often threatens air strikes on Iran, which is an obvious expression of Israel’s perennial search for security. In contrast, India has always maintained formal diplomatic ties with both its rivals, Pakistan and China; even during military conflicts, India did not expel their ambassadors. Similarly, India reduced its diplomatic presence in Beijing following the Indo-China war in 1962, but did not terminate its relations. Indian leaders must consider this overall foreign policy situation before considering any punitive action against state and non-state entities across its borders.

Israel remains the most important and capable nuclear power in the volatile Middle Eastern region. Israeli military strategists are aware that Israel’s cross-border raids or pre-emptive strikes in Palestinian territory, Lebanon, or Syria would not invite superior military response or a nuclear attack. The maximum damage that can be inflicted on Israel could be guerrilla attacks and rocket launches by Hezbollah and Hamas. Such asymmetry gives Israeli military a stupendous safety valve. In contrast, India has two neighbors with nuclear power. It is neither possible nor desirable to replicate Israeli provocations.

[19] Stephen P. Cohen and Sunil Dasgupta, *Arming Without Aiming: India’s Military Modernization* (Washington, DC: Brookings Institution, 2010).

India's policy toward its immediate neighbors has a strong domestic impact, particularly in its border provinces. Sporadic tensions in Sri Lanka impinge on Tamil Nadu in southern India, which has close ethnic links with the Tamils of Sri Lanka. As shown by India's military intervention in Sri Lanka, political considerations in Tamil Nadu influenced New Delhi's policies toward the ethnic conflict in Sri Lanka. This holds true for India's policy on Bangladesh, where strong domestic input from the West Bengal is clearly visible. Even India's policy towards Pakistan is not insular, and is affected by political developments in Kashmir. In this way, India's policy toward its neighbors is shaped primarily by domestic political dynamics rather than by strict foreign policy calculations. In contrast, similar considerations do not constrain Israel's foreign policy.

## Relative Military Strength

In terms of the quality of its weapons and its manpower, Israel continues to hold a decisive advantage over its Arab neighbors. Besides sophisticated weaponry, Israel has distinct psychological and strategic advantages over its rivals. In contrast, although India enjoys a certain military lead over Pakistan, it does not have any overriding strategic and psychological advantages over Pakistan. Moreover, India does not have any advantage over China. Although India has buttressed its offensive capabilities and has been acquiring new power projection capabilities, it does not have credible indigenous defense-manufacturing facilities.

The Israeli military rectified most of the deficiencies revealed in the 1973 War and subsequently managed to attain several stunning achievements. The most famous special operation was executed in July 1976, when the elite special forces unit, *Sayeret Matkal*, rescued Israeli passengers who were held hostage at the Entebbe airport in Uganda after Palestinian terrorists hijacked their plane. Destruction of the Iraqi nuclear reactor in June 1981 was another successful special operation. Although condemned in international circles at the time, the preemptive strike almost neutralized Saddam Hussein's nuclear weapons program. These multiple triumphs have confirmed Israel's military superiority beyond its borders. On the other hand, the recently executed "surgical strikes" across the LoC in Kashmir is one of the few notable achievements of the Indian army beyond India's borders. The Indian army has continued to pursue defensive capabilities to enhance deterrence. Indian leadership has so far failed to display the political will to overcome policy paralysis in the defense sector. One swallow does not make a summer. It will take some time for India's military to develop capability to act beyond its borders.

No discussion of the Israeli military strength would be complete without commenting on the role played by the United States. Israel regards the United States as its principal supporter and ally, and the United States views Israel as a vital regional partner. The common interests of both countries are much greater than their so-called differences. As a result, the United States provides Israel with its latest weaponry, while Israel applies its capacity for innovation in science and technology to manufacture new weapons. Over the last few decades, Israel has become a leading exporter of defense equipment and has emerged among the top ten arms exporters in the global market. These trends provide explanations for the powerful Israeli military. On the other hand, India has neither access to first-rate military hardware nor critical diplomatic support from the world's leading superpower for any of its military actions.

## Legal Structures for Counterterrorism

Police, intelligence, and military organizations all contribute to counterterrorism efforts in India. India's closest structural equivalent to Israel's Ministry of Public Security is the Ministry of Home Affairs, which oversees national police, domestic intelligence, and paramilitaries. The major legislation that deals with terrorism in India is the Unlawful Activities (Prevention) Act (UAPA). Some Indian provinces such as Maharashtra and Karnataka have laws that are used to prosecute suspected terrorists. The Terrorist and Disruptive Activities (Prevention) Act (TADA), the first anti-terrorism law to define and counter terrorist activities, lapsed in 1995.[20] The subsequent Prevention of Terrorism Act (POTA) was repealed in 2004, after several allegations of misuse were made in applying the anti-terror law. An amendment to the already existing UAPA then followed. India's experiments with TADA, POTA, and UAPA have failed to deliver the desired results. There have been allegations of designing the anti-terror laws in order to shield or harass particular communities or

[20] "The Terrorist and Disruptive Activities (Prevention) Act, 1987," South Asia Terrorism Portal, http://www.satp.org/satporgtp/countries/india/document/actandordinances/TADA.HTM#7A.

religious denominations. The Second Administrative Reforms Commission (ARC) of India opined in its report in 2008 that "a comprehensive and effective legal framework to deal with all aspects of terrorism needs to be enacted. The law should have adequate safeguards to prevent its misuse."[21]

One of the major deficiencies in India's institutional approach to counterterrorism is the gross divide between how the central and state governments view counterterrorism. This is the reason that the proposal to create the National Counter-Terrorism Center (NCTC) has not been successful. Some state governments vetoed its formation on the basis that its functioning would undermine the federal structure of India's constitution.[22] The need to bifurcate the internal security function of the Ministry of Home Affairs into a separate ministry, just like Israel's Ministry of Public Security or the Department of Homeland Security in the United States, has been felt for a long time, but no action has been taken in this direction. The National Investigation Agency, which came into being after the Mumbai terror attacks in 2008, also lacks teeth in its present form.

Although both India and Israel are parliamentary democracies, the nature of their governing systems is different. Unlike India, Israel is a unitary state. This fact gives it certain advantages which are denied to India because of its federal character. Thus, the Israeli government does not feel constrained by the presence of another constitutionally-mandated executive authority that can confront its writ in creating legislative and institutional mechanisms for dealing with public safety and security, including counterterrorism. In June 2016, Israel enacted new legislation, expanding the state's counterterrorism powers and the definitions of terrorist organizations and terrorist acts.[23] The new anti-terror law is an amalgamation of most of the provisions of the existing counterterrorism law, while it replaces several defense regulations enacted

[21] Government of India, Second Administrative Reforms Commission, "Dealing with Terrorism: Legal Framework," ch. 4, in "Combatting Terrorism, Protecting by Righteousness," Report no. 8, http://arc.gov.in/8threport/ARC_8thReport_Ch4.pdf.

[22] Gurmeet Kanwal, "India's Counter Terrorism Policies are Mired in Systemic Weaknesses," Institute of Defence Studies and Analyses, May 14, 2012, http://www.idsa.in/idsacomments/IndiasCounterTerrorismPoliciesareMiredinSystemicWeaknesses_gkanwal_140512.

[23] Jonathan Lis, "Knesset Passes Sweeping Anti-Terrorism Law," *Haaretz*, June 15, 2016, http://www.haaretz.com/israel-news/1.725225.

by the British Mandate. Though intended to strengthen both the security and the legal establishments in their fight against terrorism, the new law's implementation, in practice, is going to be tough, particularly regarding the "checks and balances necessary to safeguard against unreasonable violations of individual human rights."[24]

## Cybersecurity

Israel has developed world-class expertise in cybersecurity to counter terrorism and other emerging threats. As the Israeli government institutions and military are under constant attack from cyberterrorists and jihadist hackers, Israel's law enforcement and the intelligence agencies have created a robust and secure communications architecture, with both defensive and offensive capacities in the domain of cybersecurity. It has been rightly observed that Israel's "cyber revolution is the third revolution after the agricultural and industrial one."[25] Other countries are adopting the Israeli approach in their national cybersecurity policy.

On the other hand, India has yet to develop appropriate mechanisms for ensuring that global best practices in cybersecurity are translated into a suitable doctrine. India's security agencies and armed forces lack a specialist culture; there are no cyber specialists or information warfare specialists who would continue working in their area of specialization after their limited tenures. The paramilitary and the military continue to be led by generalist officers, as they are often called. Even when these officers develop a degree of specialization in the cyber domain, their next appointment often takes precedence over retaining domain expertise.[26]

India's cyber capabilities lag significantly behind global players, and due to "little control over the hardware used by Indian internet users as well as the information that is carried through them, India's national security architecture

[24] The Legal Counseling and Legislation Department (International Law), "The Counter Terrorism Law 5775–2015," http://www.justice.gov.il/Units/InternationalAgreements/HumanRightsAndForeignRelations/Faq/CounterTerrorismLaw5775-2015_BackgroundDescriptionJune2016.pdf.

[25] John Reed, "Israel Cyber-Security Expertise Lures Growing Share of Investment," *Financial Times*, January 12, 2016, https://www.ft.com/content/dfa5c916-b90e-11e5-b151-8e15c9a029fb.

[26] Vivek Chadha, *Even If It Ain't Broke Yet, Do Fix It: Enhancing Effectiveness Through Military Change* (New Delhi: Pentagon Press, 2016), p. 129.

faces a difficult task in cyberspace."[27] The Information Technology (IT) Act, enacted in 2000, has long been considered outdated and in need of a complete overhaul. Several agencies have been entrusted with cybersecurity management at various levels, but overlapping organizational charters, the duplication of efforts, and obstacles in coordinating cyberoperations among various stakeholders are all challenges that have yet to be addressed.[28] Despite having a national cybersecurity policy in 2013 and a national cybersecurity coordinator in 2014, the overall cybersecurity ecosystem in India has not improved much.[29] India ranks 96 and 105 in terms of download speed and average bandwidth availability respectively.[30] India is still at least ten years behind Israel and other developed countries in the field of cybersecurity.

One recent example would suffice to explain India's serious shortcoming in the cyber front. In tune with global trends, cyberspace has provided Islamist extremist and jihadist organisations in Kashmir with a psychological platform through which they can transmit their message of propaganda, indoctrination, and recruitment to ever-expanding audiences. The rising use of internet and smartphones has added fuel to the fire.[31] The ways in which the security and intelligence agencies handled the recent turmoil and violence in Kashmir, in the wake of eliminating a terrorist on July 8, 2016, left much to be desired. Instead of effectively countering the cyber insurgency waged by local militants and Pakistan-based jihadist cyber networks, the Indian government responded by closing down mobile networks and internet connectivity in Kashmir, depriving its security agencies of vital clues, trends, and information in cyberspace. According to an analysis of social media platforms, such as Twitter, Facebook, and WhatsApp during the week of

[27] Arun Mohan Sukumar, "Upgrading India's Cyber Security Architecture," *Hindu*, March 9, 2016.

[28] Arun Mohan Sukumar and Col. R.K. Sharma, "The Cyber Command: Upgrading India's National Security Architecture," ORF Special Report 9 (New Delhi: Observer Research Foundation, March 2016).

[29] Subimal Bhattacharjee, "Too Casual an Approach to Cyber Security," *Business Line*, October 3, 2016.

[30] Chittaranjan Tembhekar, "Demon in the Details: India has Low Cyber Security, Bandwidth," *Times of India*, December 22, 2016, http://timesofindia.indiatimes.com/city/mumbai/demon-in-the-details-india-has-low-cyber-security-bandwidth/articleshow/56112036.cms.

[31] Justin Rowlatt, "How Smartphones are Shaping Kashmir's Insurgency," *BBC*, July 12, 2016, http://www.bbc.com/news/world-asia-india-36771838.

July 8–14, 2016, out of a sample of 126,000 responses, 45 percent was from "unknown" geographical locations; 40 percent was from Indian locations; and about 8 percent was from Pakistan.[32] This is hardly surprising. As long as the Indian government does not develop sophisticated cyberintelligence-gathering capabilities, militants will continue to exploit various social media platforms to incite terrorism.

## Conclusion

This article has looked at the Israeli strategic orientation, providing a brief history of the Israeli army's handling of the conflict, and has examined different circumstances in which the Israeli and Indian militaries operate. For Israelis, the asymmetric conflict with the Palestinians is about recognizing their right to live in a Jewish state, free from external threat. Those Palestinians who advocate and apply violent terrorist methods of resistance, including suicide bombings and rocket attacks, for overcoming this asymmetry further cement Israel's siege mentality.

This paper attempted to comparatively assess Indian and Israeli military strategies to show the differences in the way their militaries respond to terrorism and other forms of asymmetric warfare. It must be acknowledged that military responses to asymmetric warfare pose several moral, legal, and strategic difficulties. Israel has offensively and proactively responded to acts of terrorism, but India has preferred to remain defensive and reactive in its response. Terrorist attacks have occurred in India with alarming regularity. In the current geopolitical circumstances, there does not seem to be much hope of reducing the jihadist terror threat in the future. Every time an attack occurs in India, there is clamour for retributive action against the perpetrators; but India's approach to counterterrorism remains as defensive and unimaginative as ever. If India does not overcome the several strategic and geopolitical challenges outlined above, its military will not be able to counter terrorism in the ways that Israel does. There is an urgent need to devise new preventive measures against such attacks. Although the Indian army conducted retaliatory action after the Uri terror attack, it is difficult to predict with certainty that this offensive posture will continue.

[32] Himanshi Dhawan, "Pakistan May be Waging Proxy War in Cyberspace Too," *Times of India*, July 19, 2016, http://timesofindia.indiatimes.com/india/Pakistan-may-be-waging-proxy-war-in-cyberspace-too/articleshow/53273657.cms.

# Framing the Cyberthreat through the Terror-Ballistics Analogy

David Sternberg

Cyberthreats are a new and developing, complex phenomenon. A central way for decision makers to cope with this difficulty is through analogies as simplifying psychological constructs. One analogy that could be used is terrorism and specifically the terror-ballistics experience in Israel. Building on this analogy, three main takeaways are suggested. The first takeaway is that key assumptions on the cybersecurity future should be revisited. The second one is the possibility of adapting the "six Ds" counterterror framework—Defense, Detection, Deterrence, Defeat, Deny, and Diplomacy—to the cyberworld. The third takeaway from this analogy is on the organizational level, highlighting the need to create new flexible operational configurations as well as international collaborative structures.

**Keywords:** Cyberthreat, terror, ballistics, analogy, metaphor, Israel

> We do not understand nor internalize how much we are exposed [in the cyber domain] . . . in my eyes, it is similar to rockets . . . I was there when the rockets just began—in the 1980s. They were small, imprecise weapons. It didn't seem like a serious threat. But now, some thirty odd years later, soon rockets will have the capability of hitting a plate on the roof of the General Staff building. The same is true for the cyber field. While we try to defend our core

David Sternberg is a graduate of the Harvard Kennedy School. This article is a shortened version of an independent research course final paper at HKS. The opinions expressed are of the author's alone and do not represent any position of the Government of Israel.

> secrets, our defense systems, our national infrastructure, we can sustain a lot of damage to our civilian sector.
>
> Brig. Gen. Itai Brun[1]

## Understanding a New Phenomenon with Analogies and Metaphors[2]

Research in international politics extensively addresses the use of analogies as a tool for decision making (e.g., May, Jervis, Snyder and Diesing, Vertzberger).[3] At the core of this literature is the investigation of historical events as a basis for lessons to be implemented in current affairs. Yet analogies and metaphors could be adopted and applied not only to historical events but also to concepts, items, persons, mechanisms, and situations.

In doing so, the use of analogies and metaphors incorporates important psychological aspects in decision making. They serve as knowledge structures for information processing and comprehension, as well as for filling in missing data.[4] Linguistic and philosophical theories also highlight the use of analogies and metaphors as a central way for individuals and groups to construct and understand complex, intangible phenomena, and ultimately to drive actions.[5] There are dangers, however, in using analogies and metaphors for reasoning. The analogy as a psychological mechanism can lead the decision maker to accessible and relatively easy mental processing structures, which are not

[1] Yoav Limor, "'Attacks in the Golan Heights are a Matter of Time,'" *Israel Hayom*, January 16, 2015, http://www.israelhayom.com/site/newsletter_article.php?id=22837.

[2] For this work, analogies can be defined as the comparison of two different entities based on similar aspects, whereas metaphors are the projection of the characteristics of one entity onto another. To illustrate, an analogy would be "he is slow as a turtle" while a metaphor would be "the man's roar."

[3] Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992); Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7 (2012), http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270#p2.

[4] Khong, *Analogies at War.*

[5] George Lakoff and Mark Johnson, *Metaphors We Live By* (Chicago: University of Chicago, 1980).

necessarily the correct ones; it also creates a framing bias that affects the attitude and scale of the way that decision makers perceive the problem.[6]

## Why is it Important for Cyber?

The cyber arena is a fast developing and complex world. The cyber arena is hard to comprehend and conceptualize because of its heavily technological substance, its influence on daily lives, the interconnected multiple components, the different disciplines involved, and its rapid evolution. A generation gap between decision makers who are often "technologically illiterate" and advanced practitioners exacerbates these tensions. Analogies and metaphors can simplify this inherent obstacle and can guide generalists.

In reviewing the current cyber discourse in the United States, it is hard not to be impressed by the presence of more than a handful of analogies in the field, which likely represent both the challenge encompassed in the subject, as well as the thirst for anchors in the difficult intellectual comprehension of the issue. These comparisons differ in their type and scope but are used only with partial classification. Some are events, while others are categories of warfare, weapon types or historical processes.[7] A short list would refer to Pearl Harbor, September 11, Hurricane Katrina, the Cold War, the Monroe Doctrine, the Manhattan Project, the law of the seas, blitzkrieg, the strategic defense initiative, the outbreak of World War I, balkanization, airpower, economic warfare, biological warfare, immune systems, nuclear deterrence through mutually assured destruction (MAD), submarines, piracy, innovation wars, insurgency, and so on.[8]

In this regard, some assert that applying a martial conceptualization of cyberspace is counterproductive because it strengthens the framework of "threat," induces groupthink, and reduces the scope for collective problem-solving. Prominent metaphors in the cyber field, such as "cyberspace" and "biology," also fall short. Narrow definitions overlooking the interwoven nature of the cyber realm with real space and its non-linear dynamics are misleading. Biological metaphors, referring to methodologies in public health,

[6] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, 47, no. 2 (1979): 263–291.

[7] Emily O. Goldman and John Arquilla, ed. *Cyber Analogies* (Monterey: Naval Postgraduate School, 2014).

[8] Robert Axelrod, "A Repertory of Cyber Analogies," in *Cyber Analogies*, ed. Emily O. Goldman and John Arquilla.

epidemiology, and immunology, and concepts of "adaptation" or "holism," ignore the origin of the problem itself—that cyberspace is a human creation, which serves socio-political rationale and lives in the semantic level.[9]

The writing on this subject in Israel is less developed than in the United States. However, when looking at the public discourse, the use of analogies is evident. For example, some scholars use metaphors from the biological world ("mutated code") or analogies from the history of warfare, such as referring to cyberattacks as analogous to drones being introduced into the modern battlefield.[10] Some refer to the emergence of the aerial domain to describe the new cyber domain,[11] while others prefer the analogy of vandalism instead of warfare.[12] When explaining the matter to the public, the leading officials in the Israeli administration resort to analogies too, for example from public health or road safety.[13]

## The Terror-Ballistics Analogy

The term "terror ballistics" would be used in the context of this work to describe the tactics of attacks conducted by terror organizations, including the firing of artillery, mortar shells, short-medium-, and long-range rockets, guided rockets, missiles (including, for example, surface-to-surface; shore-to-sea; anti-tank; cruise missiles, MANPADS), and UAVs. As described above, a spectrum of analogies is used to describe the challenge of understanding the cyber world. This paper explores whether the analogy of applying terror to cyberattacks is suitable. To refrain from general comparisons, however, this paper focuses specifically on the narrower case of the terror-ballistics

[9] David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue* 44, no. 2 (2013): 147–164. For an in-depth analysis of the public health analogy, see, for example, Brent Rowe, Michael Halpern, and Tony Lentz, "Is a Public Health Framework the Cure for Cyber Security?" *Crosstalk* (Nov/Dec 2012): 30–38.

[10] Gabi Siboni, ed., *Cyberspace and National Security: Selected Articles* (Tel Aviv: Institute for National Security Studies, 2013).

[11] Shmuel Even and Daṿid Siman-Ṭov, *Cyber Warfare: Concepts and Strategic Trends* (Tel Aviv: Institute for National Security Studies, 2012).

[12] Jonathan Silber, "Cyber Vandalism—Not Warfare," *Ynet*, January 26, 2012, http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

[13] Hadas Geifman, "Dr. Eviatar Matania: 'Cyber Security is Likened to Hand Washing to Maintain Health—Important, But Not Enough,'" *People and Computers*, June 26, 2012 (in Hebrew), http://www.pc.co.il/it-news/89919/.

challenge that terror organizations have imposed upon Israel in the last two decades.

In their well-known work, *Thinking in Time*, Neustadt and May suggest applying analogies by distinguishing explicitly between their similarities and differences.[14] In this way, the decision makers will be aware of the analogy's strengths and weaknesses. This simple and intuitive practice applied to the example at hand—of rockets fired by terror organizations at Israel—reveals the following similarities and differences, both with caveats.

## The Similarities in Applying the Analogy of Terror Ballistics to Cyberthreats

a. *Some of the weapon's characteristics:* The characteristics of these weapons are a cornerstone in the terror organizations' adoption of terror ballistics as a leading tactic. These weapons are simple and inexpensive. They can be activated in salvo, operated in short time spans (taking minutes from decision to actual hit), and can deeply penetrate into the enemy's territory. These weapons are not defensible and are hard to locate because of minimal signature and large-scale deployment. In this sense, cyber weapons have similar features. They are operated en masse and their action is immediate. They are mostly easy to construct and use, and they are inexpensive (mainly requiring the acquisition of weaknesses and intelligence targeting). They also require a costly security solution and can easily infiltrate the "soft and blind spots" of the rival—mainly civilian and private—but also military targets. As for their signature and deployment, see the following paragraph.

b. *Some aspects of attribution*: The cyber realm introduces a central difficulty in terms of attribution (especially in real time), due to a mismatch

[14] Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Free Press, 1986).

between higher level identities and recognizable addresses (IP).[15] This issue weakens the base for retaliation and deterrence. Thus, a false response may be inaccurate and can lead to entanglement, embarrassment, and various damages. When applying the terror ballistics analogy, at the resolution level of a specific shooting event, two similar problems of attribution appear. First, there is the situation of a single firing incident, between rounds of wide-scale conflict. Here the dilemma of whether the main adversary is responsible for the shooting or if it is a third party frames the problem of attribution. This is a focal intelligence problem, for it is connected to the question of the strength of the current deterrence. The second problem is with a given firing event within an intensive conflict. Here, the question is whether a certain launching site is incriminated. This is important due to the nature of the civilian surroundings in which the terror organizations work. The high number of launchers, their storing and firing from civilian and humanitarian sites, the decentralized command and control operation, and their high mobility and camouflage attributes all create a problem in determining not who in general is responsible, but rather, who on the ground (persons and places) assumes the accountability, and should be acted upon. Thus, the need for a tailored response creates a need for a clear attribution.

c. *Non-state actors and sponsoring states roles:* In cyber warfare, a distinction exists between cyber operations conducted by states or governments and those exercised by non-state actors. Nevertheless, sometimes these non-state actors serve as proxies or as the façade of a national apparatus so that the state can maintain deniability or act under the threshold of war. The same

[15] This is a general proposition. As in all technological fields, this issue is rapidly changing. Some challenge this on not only a technological basis but also assert that the attribution problem changes in relation to the scale of the target (attribution on high value targets would rarely fall short), as well that attribution is an “art”: a multi-faceted process that combines technological evidence with operational and strategic thinking. As in real life, it is neither binary (“solved” or “not solved”) nor mere evidential in nature. In cyber, as well in other domains, attribution is based not only on digital forensic evidence but also on a wide range of intelligence sources; nevertheless, attribution in cyber could diverge from the terror ballistics analogy in terms of time, resources, and the adversary’s sophistication. About attribution, see Jon R. Lindsay, “Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack,” *Journal of Cybersecurity* 1, no. 1 (2015): 53–67; Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

phenomenon exists in the terror-ballistics field. Both states (e.g., Iran) and non-state actors (e.g., Hezbollah) have in the past used little organizations as an indirect means of operating against Israel.[16] Thus, in both cases, non-state actors can acquire the serious capabilities of real states or can disguise themselves as states. As mentioned above, this means a larger probability for incidents with the intent of provoking conflict and further complications for escalation control.

d. *Civilian and military infrastructures entanglement:* A wrong attribution may cause a mistake in identifying the attacker. In the cyber field, the classical example is a botnet attack that uses a pre-prepared captive infrastructure to launch an assault. The main implication is that by attacking a controlled "innocent" computer, collateral damage may occur. This problem is inherent when civic and military infrastructures are fused together. Unlike some other military domains, the shooting of rockets by terror organizations operating in civilian neighborhoods share the same story. The other but similar side of this entanglement is the shared purpose of cyberattacks and terror ballistics to damage critical civilian infrastructures and thus influence the civic routine. Guided rockets on a power station or its neutralization by a cyberattack is designed to terrify the population and to cause uncertainty, rather than hurt the general war effort.

e. *Some elements of escalation dynamics:* The danger of escalation is greater in cyberattacks because they do not require the movement of forces and weapons. Rather, they are cheap, easily launched, and instantaneous, and—in some cases—once launched, they can spread.[17] Several of these elements hold true for terror ballistics. There is little time for decision making when attack and counterattack take place. An error in counterattack or high collateral damage, which is also typical to a rocket war, could be experienced in a similar manner by the diffusion of a cyberattack aimed at civilian sensitive interests. These may trigger a fast escalation through retaliation and counter-retaliation. The low signature characteristic discussed above adds to the fog of battle and the difficulty in attributing it correctly.

[16] Eyal Zisser, "The Return of Hezbollah," *Middle East Quarterly* (Fall 2002): 3–11.

[17] Matthew Cohen, Chuck Freilich, and Gabi Siboni, "Four Big 'Ds' and a Little 'r': A New Model for Cyber Defense," *Cyber, Intelligence, and Security* 1, no. 2 (June 2017).

It could be argued that the variance in scale and pace between the two cases makes all the difference. Thus, in the cyber case, there are no obvious red lines and no clear common perceptions of whether one type of attack is "more important" or "more aggressive" than another, making escalation control extremely difficult. In contrast, in the ballistics context, relatively clear versions of proportionality can be applied. One could also suggest that Israel can choose to wait and respond in a day or two, and not necessarily be dragged through "active defense" dynamics to escalation. However, it seems that even if the pace is different, the principle still holds. Equations of retaliation are challenged constantly in the ballistics world in the same way that cyber incidents do not necessarily end with rapid escalation.

f. *Weapons' diversity:* The cyberweapons' arsenal extends along a continuum of sophistication. At one end is common malware that most security systems can neutralize due to a known signature. On the other end are advanced vehicles that utilize numerous zero-day weaknesses, skip between networks, camouflage themselves, and target specific high-quality infrastructure. In the rocket world, a different but similar scale exists. Short-range rockets or mortar shells, although risky and lethal as experience has shown, are at one end, while precise long-range items, attacking combat UAVs, cruise missiles, or shore-to-sea missiles, can maneuver differently and represent the advance in range, accuracy, and lethality, thus resulting in a different operational and strategic thinking.

g. *A multipolar problem:* Although external powers, such as Iran, Russia, and North Korea, have contributed to the proliferation of rocket technology, recent pressure by Israel on their supply routes seems to have transformed the process. This has quickened the development of workshops and plants relying on domestic capabilities to manufacture these weapons, as evident in the Gaza Strip in the last few years. This expanding decentralized industry—supported more by knowledge transfer rather than by material and machinery—is evolving into a diverse, multi-foci threat, mainly in terms of short-range systems in which no supply centers exist. The cyber world, in parallel, shares a similar structure of having many players that conduct their own R&D or, at least, the production and perfection of weapons.

h. *The learning process:* One of the main similarities in both cases is the learning dynamics. Unlike analogies from the biological world, here the situation is between intelligent adversaries. In both cases, "transformative technology" is the challenge,[18] given the difficulty of its strategic comprehension. In both cases, continued operational friction advances the understanding, vocabulary, and concepts in this field. In this context, even unique experiences like "Stuxnet" (an infrastructure attack), "Flame" or "Heartbleed," are considered transformative and as part of a continuum. The terror ballistics against Israel have also made advances in learning through crises (e.g., the Second Lebanon War). In practical terms, however, the learning process has been more continuous in nature. Accordingly, the term within the military jargon used to define developments in the field of terror is "a learning contest";[19] here too, it seems that a constructive tension between academia and practitioners' perspectives exists in conceptualizing the phenomenon[20]—exactly as in the cyber realm.[21]

## The Differences in Applying the Terror-Ballistics Analogy to Cyberthreats

On the other hand, being loyal to Neustadt and May's framework and being aware of previous faults, it is important to point out the main differences between terror ballistics and the threats of cyberattack:

a. *Laws of physics versus laws of cyber:* Looking at the shared characteristics of the weapons mentioned above, one should also remember the differences. On the one hand, rockets have characteristics that conform to very known and predictable laws of physics; on the other hand, cyberattacks are a weapon that can have infinite range and can linger unknowingly in a system for years, and can unexpectedly assume radically new characteristics (such as when adversaries suddenly find a major vulnerability that previously was unknown), and so forth.

The same could be argued not only about the type of weapon but also about the surrounding environment. The firing of rockets, as well as their

[18] Joseph S. Nye Jr., "Nuclear lessons for Cyber Security," *Strategic Studies Quarterly* (Winter 2011): 19–38.

[19] Brian A. Jackson, "Organizational Learning and Terrorist Groups," RAND Working Paper (2004): 27.

[20] Dima Adamsky and Yossi Baidatz, "The Development of Israel's Deterrence Concept—A Critical Discussion of its Theoretical and Practical Aspects," *Eshtonot* 8 (2014): 7–8 (in Hebrew).

[21] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 7–40.

supply chains and the deployment of launchers, is conducted within physical domains and under certain conditions. The warring sides use these conditions to acknowledge or deny achievements by their rivals. For example, a logical connection exists between the range of the rockets and the launching sites. In order to fire at more sensitive targets, terror organizations have to advance weapons to certain positions; only the increase in range changes this equation. That was the logic, for example, behind the UNSC Resolution 1701.[22]

In contrast, the cyber domain potentially could be reshaped. One example of this is the ongoing debate about the changing internet architecture and governance. Concretely, the basic argument around the concept of the "end-to-end" principle illustrates the potential ability to "redefine" the battlefield.

b. *The scope of the challenge:* Terror ballistics is a struggle limited by range and sovereignty. Israel confronts a given number of areas, namely Lebanon, Gaza, Sinai, Syria, and Iran. These areas have a set of characteristics, such as topography, borders, routes and ports, and ethno-demographic distributions. The enemies, or at least the main ones, are also known. Therefore, it is, in a sense, a system with boundaries, hierarchies, links, and tensions. Hence, it is possible to explore and learn it constantly. The terrain, the capabilities, and the intentions are learned through past conflicts and intelligence collection. In comparison, cyberattacks have a global reach. The attackers could be from distant locations, hold diverse affiliations, be of different sizes, hold new and old identities (including hybrid identities, in the case of cooperation), and be motivated by changing interests. This makes a difference in the starting point for attribution as discussed above, while in the case of terror ballistics, the number of possibilities is narrower and the question of attribution must be examined with a different resolution.[23]

c. *Context of the conflict:* The terror-ballistics phenomenon has been experienced mostly during major conflicts (e.g., with Lebanon) or in periodical rounds of fighting (as experienced vis-à-vis Gaza and Sinai). As a caveat to this, one could always argue that the ongoing rocket attacks

[22] The resolution (August 11, 2006) determined that no armed forces other than UNIFIL and the Lebanese armed force (implying, in other words, Hezbollah) could be present south of the Litani River. The idea was to prevent the deployment of short-range rockets.

[23] With the general analogy of terror in mind, the differences are more limited when considering the diverse affiliations, sizes, identities, and interests of terror organizations.

("dropping fire"), aimed at the southern towns of Israel (such as Sderot) from 2002 until nowadays, constitutes a continuum pattern rather than an event-based phenomenon. Nevertheless, although cyberthreats are also seen through prisms of crises or major events, cyberthreats are greater in number and frequency and do not inherently have a pattern of lows and highs. That makes the dynamics of terror ballistics very sensitive to the context of a given conflict, unlike in the case of cyberthreats. In other words, in the cyber case, there is no definition of "peacetime" versus "wartime," because there is constantly cyber activity with varying degrees of annoyance.

d. *"Weakest Link" defense, "Cascade Shape" attack:* Cyberspace is characterized by having a weakest link defense problem. Hence, even if the defense is strong and advanced on most levels, it takes only one undetected breach to enable a system meltdown. Of course, it is possible to advance architectures that weaken this fragility through implanting analogical or human factors in the transmission, by simplifying them or by disintegrating them;[24] however, these do not reflect the current trends, which are characterized by greater interdependency and integration. This unique feature leads also to different attack tactics, such as a cascade-based attack that utilizes a "learning by doing" process to discover weaknesses. Terror ballistics operate differently. The defense systems work on statistical parameters and risk-management, while the arsenal rockets build up on opportunities and long-term planning.

Rivals, however, may attempt to locate soft spots in the other's defense or offense during conflicts. Specifically, the discovery of a single weak point—although not inherent to the functioning of the entire system (as in cyber)—could trigger dramatic changes in the strategic situation. For example, the shooting of several rockets towards the national airport of Israel from Gaza during Operation Protective Edge caused US regulators to invoke a temporary directive barring landings at the airport. Foreign carriers were quick to follow, creating a surprising strategic impact—of an effective travel ban—for a short period.[25]

[24] Richard Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies,* (Washington DC: Center for a New American Security, 2014).

[25] The same could be argued of a single possible incident of a mass injury to a kindergarten or any other symbolic site that could completely change the dynamic of an armed conflict.

e. *Proliferation:* The comparison between the proliferation process in the terror ballistics case and the cyber one emphasizes two issues. The first one is physical versus electronic knowledge-based transfer. Cyberweapons are not characterized by special materials or loads; rather, they are constructed from bits and bytes and logic schemes. Their lethality or effectiveness is connected directly to other features that they carry, mainly the intelligence targeting (i.e., understanding the entry spots of networks and systems); the weaknesses they exploit; their ability to overcome security systems; and their low signature. They are thus capable of being manufactured in almost any circumstance. Although they also demand a certain know-how—such as how to make a workable rocket engine or guidance system for a given range—rockets still require the physical transfer of parts and materials, which must pass through borders and ports.

The second issue is the unique form of proliferation. Cyberweapons can be used only once, as they become useless the moment they are identified and signed.[26] The proliferation comes sometimes from a different mechanism of learning and adaptation of weapons once they are introduced to the world. For example, once a code of a cyberweapon such as "Stuxnet" or "Flame" is distributed globally, it automatically becomes a basis for constructing new versions of this technology. Thus, proliferation takes the form of reverse engineering. Unlike these unique features, terror ballistics, at least until more recently, relied heavily on an industry of rocket and missile proliferation mainly from Iran and other suppliers.

f. *The private-civilian sector role in the cyber problem:* Contrary to ballistic weapons, cyberweapons are completely "dual-use," both in nature (relevant technologies) and concepts. Thus, private companies and civilian actors assume large roles in all aspects of cyberattacks and cybersecurity, not only as targets, but also as contributors to defense, as threat assessors, and as offenders. In addition, a potentially large economic impact is tangible with the effect of not only physical destruction, as in the case of rocket attacks, but also with a variety of other effects such as the theft of technological advances.

To conclude, terror ballistics have many similarities to the cyber challenge, but at the same time, they have significant differences. The analysis of these similarities and differences portrays a mixed picture. It seems, however, that there is a good basis for comparison between the two. As a key distinction, it

[26] Siboni, ed., *Cyberspace and National Security: Selected Articles*.

is important not to refer to differences in pace, scale, change, and reach, for they are probably unparalleled in any other analogy. Rather, it is suggested to look at the terror-ballistics model through the lens of dynamics, learning processes, threat evolution, and relationships. Taking this into account, the similarities strengthen considerably.

## The Wider Terror Analogy

In generalizing the specific analogy between terror ballistics and cyberattacks, it could be argued that terrorism may be a useful analogy for cyberattacks. Although this paper cannot establish this claim, nevertheless, there seems to be a strong basis for this argument, when examining the shared dilemmas facing decision makers who encounter both terrorism and cyberattacks.[27]

Among these dilemmas are:

a. *A problem of definition:* There is no consensus on a universal definition of the phenomenon of both terrorism and cyberthreats.

b. *Intelligence challenges*: Intelligence is vital for detection, retribution, incrimination, and targeting functions, but struggles with inherent multi-dimensional, cross-national, and inter-agency tensions**.**

c. *The question of deterrence* when dealing with clandestine, decentralized, non-hierarchical, and groups with limited assets.

d. *The weight of offense tactics:* Counterterrorism has created a series of offensive tactics aimed both at capability and motivation of terror organizations. The cyber realm also raises questions about the need for, the timing of, and the criteria for initiating an attack.

e. *Legislative issues:* Questions of the existence of a unique primary legislation,[28] the coherence and coordination of international legislation,[29] the definition of the offense; and the implementation of laws to include

[27] Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for Decision Makers* (New Brunswick NJ: Transaction, 2007).

[28] This is a principle that reflects the American case, for example, in the "Patriot Act." Israeli anti-terror legislation is not structured on a primary source of legislation that deals directly with the subject; however, it does rely on emergency legislation. These regulations give the government a lot of flexibility and force to act decisively against terror, but they are also heavily criticized and debated.

[29] Jack Goldsmith. "Cybersecurity Treaties: A Skeptical View," In *Future Challenges in National Security and Law*, ed. Peter Berkowitz (Stanford: Hoover Institution, Stanford University, 2011).

assistance (support, training, and funding) are similar regarding both terrorism and cyberattacks.

f. *The public and media dimensions:* In both cases, mass media coverage amplifies actions or utilizes them to convey messages to targeted populations, revealing a set of dilemmas regarding information policy, educational policy, media censorship, and ethics.

g. *The essentiality of international cooperation:* The similar architecture of the problem, composed of an international network that involves state sponsors, as well as operating entities within the states' havens, proxies, or front entities, has created the need for both international common normative or legal platforms, as well as intelligence sharing and operational frameworks.

## Main Takeaways

Fostering the analogy of terror ballistics, three main takeaways can be suggested. The first one is about key assumptions on the future of cybersecurity. The second one relates to the ingredients of a counter-threat framework, and the last, on the organizational level, is for the need to create new flexible operational configurations as well as international collaborative structures.

Neustadt and May posit the question of "does a certain analogy fit when considering a new situation?" However, having revisited their *Thinking in Time*, it can be suggested that an analogy may not just "fit," but rather informs us also about the underlying assumptions and obscurities involved in describing a strategic issue.

Building on the research of Sulek and Moran,[30] five interesting assumptions or basic questions on cybersecurity can be explored through the terror ballistics analogy:

a. "States have the capability to retain leadership in governing the internet." Looking at the terror-ballistics analogy, it is evident that Israel has been superior in the aerial domain since the 1980s at least, although, unlike the cyber domain, it did not actually control the medium; in a sense, it was at bay. The terror-ballistics, perceived at first as unsophisticated,

[30] David Sulek and Ned Moran, "What analogies can tell us about the future of cybersecurity," *The Virtual Battlefield: Perspectives on Cyber Warfare* no. 3 (2009): 118–131.

quickly became a strategic equalizing force if not, at least, a challenging one to this supremacy.

b. "Nation states are a more serious threat than a non-state." In the ballistics world, it is, of course, dependable on the load (nonconventional or not). Currently, this issue mainly distinguishes between state capability and non-state capability. However, if, for the time being, we exclude non-conventional weapons from the picture, and we assume that both the magnitude of firing power and elements such as accuracy, lethality, and relative range (covering the entire surface of Israel) have become comparable within the radical camp (Iran, Syria, Hezbollah, and Hamas), then it seems that non-state actors can hold significant power. Thus, as in the first assumption, this assumption should be relaxed.

c. "How grave is the threat?" This issue has created a large debate in the public and academic domains. The skeptics (Rid, Mahnken, Gartzke, Libicki, Weimann, and others)[31] see cyberwar as an exaggerated threat, and they question its capability to cause serious, permanent, costly military and political damage to nations. The other faction (Kello, Clarke, Carr, and others), which reflects the practitioners' mindset, argues that the threat posed by cyberattacks is real, growing, and outpacing defense and existing doctrines.[32] Cyberattacks have proved significant in the military domain (e.g., in Estonia and Georgia's conflicts with Russia) and illustrated well the potential for a massive infrastructure meltdown (e.g., Stuxnet).

In the case of terror ballistics, although life and property have been lost and potentially could have been much more affected, one can wonder if this is much more limited, proportional to expectations and investments, and whether the "worst of all" assumption[33] has not been embedded in decision making. Accordingly, some have advocated for putting the emphasis on the offensive rather than defensive solutions.[34] However, in retrospective,

[31] See, for example, Martin C. Libicki, "Cyberattacks Are a Nuisance, Not Terrorism," *Rand Blog*, February 20, 2015, http://www.rand.org/blog/2015/02/cyberattacks-are-a-nuisance-not-terrorism.html.

[32] Cohen, Freilich, and Siboni, "Four Big 'Ds and a Little 'r."

[33] Yitzhak Ravid, "The Worst-Case Assumption," *Maarachot* no. 350 (1997): 2–12 (in Hebrew).

[34] Avi Kober, "Iron Dome: Has the Euphoria Been Justified?" *BESA Center Perspectives Paper* no. 199 (February 25, 2013), http://besacenter.org/perspectives-papers/iron-dome-has-the-euphoria-been-justified/.

most of the current discourse views the decision to invest heavily in the past years in a multi-layered defense system as a proven success. Thus, the Israeli analogy supports the assessment of the cyber realm as a substantive and evolving threat.

d. "Will next generation internet technologies and applications be more secure?" This is a question that deals with levels of vulnerabilities in developing infrastructures, unlike the ballistics' world. However, it could be argued that the combination of weapons and tactics and the evolving political-economic reality may present a whole new generation of threats. To illustrate that in the terror ballistics context, we could mention a few concerns such as (a) the risk to the gas platforms near Ashkelon (controlling 80 percent of Israel's energy supply) and to maritime transportation at the Port of Ashdod (overseeing 60 percent of imports to the country), both of which could be vulnerable to shore-to-sea missiles, UAVs, and cruise missiles; (b) the railroad to Sderot, which is exposed to anti-tank rockets; or (c) the danger to future airport operations (Ben Gurion Airport in Lod and the future airport at Timna).

e. "Is there sufficient political will for international diplomatic cooperation?" As discussed above, the capability to establish normative-legal frameworks seems weak. The terror-ballistics case demonstrates this through the failure of Resolution 1701. Adopting gradual and partial frameworks seems also to have failed. Dividing the threat into different segments, as in the diplomatic efforts in the man-portable air-defense systems (MANPADS) issue; the bilateral memorandum of understanding between Israel and the United States to prevent the smuggling of weapons to Hamas (January 2009); UNSC Resolution 1747 (March 2007), forbidding the export and transfer of arms from Iran; or the cease-fire agreements, all proved temporary, insufficient or unenforceable due to a combination of interests and priorities (China and Russia as impediments in the UNSC), ungoverned areas (Libya, Lebanon, Sinai), and rogue states. A possible lesson from the terror ballistics experience, although only partial due to the differences between the two cases, is that political capital should be invested primarily in "like-minded" cooperation and in unilateral prevention and deterring actions.

## From Four Ds to Six Ds

In the “National Strategy for Combating Terrorism,” declared in February 2003, the US government stipulated the strategy of **“Four Ds”** to confront the major security challenge of the new millennium. The four pillars were to **defeat** terrorist organizations; to **deny** terrorists the sponsorship, support, and sanctuary”; to **diminish** the underlying conditions for terror, which serve as the bedrock of ideas and visions and “lead people to embrace” terror; and to **defend** against terrorist attacks.

Cohen, Freilich, and Siboni suggest similar but different four Ds and explore their adaptability to the cyberthreat issue.[35] While they share the pillars of defeat and defense, they emphasize two other D principles: **detection** and **deterrence**. In a sense, these four Ds are the principles of Israel’s security paradigm. Similarly, the Israeli terror ballistics experience has been characterized by the following measures: **mitigation** (elimination of launchers and depots); **prevention** (cutting off arms supply); **defense** (multi-layered defense system); **deterrence** (deterring from future operations); and **diplomacy** (agreements and understandings).

In examining these three counterstrategies—the American “National Strategy for Combating Terrorism,” the four Ds by Cohen, Freilich, and Siboni, and the existing Israeli measures against terror ballistics—it is quite apparent that these strategies overlap and share the same principles. For example, the purpose of “defeat” in both frameworks of the four Ds is parallel to “mitigation” in the terror ballistics case in the sense of offensively confronting and degrading the enemy’s capabilities and morale as much as possible. The same applies to “prevention” in the terror ballistics context, which resembles the concept of “deny” in the four Ds—where armaments and logistical support are targeted; or the “detection” element, offered by Cohen, Freilich, and Siboni, which is embedded in the “defense,” “prevention,” and “mitigation” operations of the terror ballistics counterstrategy, for they cannot materialize without first detecting the threat.

As Cohen, Freilich, and Siboni demonstrate well and in detail, these elements also are reflected in the cyber realm. Their four D components apply to cyberattack issues and can be also applied to the terror ballistics analogy. From terror ballistics, the only two elements that are applicable to the analysis of the cyber realm are diplomacy and denial (or prevention), thus,

[35] Cohen, Freilich, and Siboni, “Four Big ‘Ds and a Little ‘r.”

creating a strategy of six Ds (Defeat, Deny, Diminish, Defend, Diplomacy, and Denial).

As for the element of **diplomacy**, I have referred above to the hardships of establishing normative legal solutions in the cyber realm. It is worthwhile, however, to explore some opportunities for creating general normative solutions within cyberspace among like-minded states, and then encouraging other states to follow those norms over time (like the model of the Nuclear Suppliers Group on export control). Furthermore, multilateral, like-minded collaboration seems to be a plausible and necessary tool for operating in a cross-jurisdictional reality. It may include not only the necessary operational (e.g., enforcement) and intelligence cooperation (information sharing) but also joint technological R&D between nations, which enhances detection and monitoring capabilities. The Israeli-American collaboration in developing air-defense systems, as well as proposing these solutions to like-minded partners, could serve as a model for the cyber industry as well.

Regarding the element of **denial** (prevention), it can be presumed that the elements of assistance, support, and finance of the adversary are weaker in the realm of cyberthreats than in the terror-ballistics theater and, therefore, less vulnerable. In other words, when the supply chain is shorter and narrower and the entire eco-system is less visible, the adversary is less exposed to any intervention. However, other elements, such as the adversary's know-how, intelligence, and coverage, are still valuable and at least could be identified and exposed, as in the terror ballistics case when arms shipments from Iran to Palestinian terror organizations were seized and disrupted in 2001, 2009, and 2014.

Finally, in addition to recognizing the different strategies, their prioritizing remains a key issue. In the example of terror ballistics, it is obvious that the combination of prevention and defense was the most dominant measures. Directly targeting the arsenals of launchers and rockets, influencing the battlefield through diplomacy, or deterring did not achieve the same results as the preventative measure of seizing and disrupting large transports of arms and the defensive measure of the Iron Dome.

Judging from Cohen, Freilich, and Siboni, it seems that this is not the case in the cyber realm as all strategies applied have substantial caveats. None alone seem more dominant. Although the strategies of defense and detection are much more developed, and Israel emphasizes its capabilities in these domains,[36] the sheer number of attacks (over a million in the Operation Cast Lead alone) is challenging.[37] In other words, in contrast to the experiences of terror ballistics, the main conclusion in the cyber domain is to find a **hybrid strategy** rather than a **leading strategy**.

## The Organizational Aspect

The issue of how to organize a counter cyber operation essentially is based on the complexity and dynamics of the threat. Drawing on the experience gained from counterterror campaigns, the significance of creating and positioning the right functions within a national effort is apparent.[38]

In this context, the need for a new strategic organization at the national level to face this novel challenge should be addressed first. When observing the terror analogy, it appears that previous case studies, such as the organizational learning in the aftermath of September 11, the formation of the National Counter Terrorism Center (NCTC), and military-cyber domain practices, are supportive in establishing new national organizations. The same principal, of creating new organizations to counter the cyber problem, can be found nowadays at the military and organizational level. For example, in 2009, the US military established a Cyber Sub-Command,[39] while the IDF recently has begun to examine the same course of action.[40] Accordingly, the Israeli government decided in February 2015 to move in the direction of consolidating forces and means by establishing the Cyber Authority. This entity is supposed to receive operational responsibilities and join the existing National Cyber Bureau (NCB).

[36] Yonah Jeremy Bob, “Rule of Law: Obama, Israel and Cyber Warfare,” *Jerusalem Post*, March 22, 2013, http://www.jpost.com/Features/Front-Lines/The-cyber-partys-over-307367.

[37] David Shamah, “Hackers Threaten ‘Israhell’ Cyber-Attack over Gaza,” *Times of Israel*, July 9, 2014, http://www.timesofisrael.com/hackers-threaten-israhell-cyber-attack-over-gaza.

[38] Bruce Hoffman and Jennifer Taw, *A Strategic Framework for Countering Terrorism and Insurgency* (Santa Monica: RAND Corporation, 1992).

[39] Some, including Admiral (Ret.) James Stavridis (former NATO commander in chief), have advocated for creating a whole new cyber branch of the armed services.

[40] Israel Defense, “Election Results and the Defense Establishment,” *Israel Defense*, March 19, 2015, http://www.israeldefense.co.il/en/content/election-results-and-defense-establishment.

In a closer look at the organizational level, however, some questions arise. In the terror realm, for example, it is unclear if the NCTC performs its expected duties while the relationship between the NCTC and the other national intelligence agencies, such as the CIA, is also not clarified.[41] In the cyber arena, the lack of clarity vis-à-vis the intelligence establishment extends beyond the terror example. Intelligence is not only the enabler of a strike; as in the terror ballistics case, intelligence is interwoven between the offense and defense because the borders between intelligence collection (cyber exploitation) and operations are blurry by definition.[42]

The Israeli experience sharpens the dilemma because the security system is smaller in scale than in the United States and dominated by three strong agencies. These agencies not only enjoy political strength[43] but also have created a symbiotic working relationship when needed and a division of labor with rotating leadership in accordance with the context.[44] Looking at the terror-ballistics realm, the same lesson can be observed by the IDF's

[41] Richard A. Best, *The National Counterterrorism Center (NCTC) Responsibilities and Potential Congressional Concerns* (Washington DC, Congressional Research Service, 2011).

[42] An example is in the United States, where the operational and intelligence establishments are largely dependent on one another, demonstrated by the fact that the Cyber Command and the NSA share the same leadership. The underlying reality for this symbiosis is the problem of defining the boundaries between intelligence and counter-intelligence collection operations and defense, active-defense, and offense initiatives and responses.

[43] Two of them are subordinate directly to the prime minister, thus deflating the authority of any other parallel body.

[44] Israel did establish a specialized entity for coordination in the field of terror. The National Bureau for Fighting Terror was created in 1996 during waves of suicide attacks; this body, however, does not undertake actual planning, operational, and intelligence capabilities, which have remained solely in the domain of the existing security branches, the most dominant being the Israel Security Agency (ISA). For more on the structure and significance of the Israeli intelligence community, see Yosef Kuperwasser, "Lessons from Israel's Intelligence Reforms," Analysis Paper, no. 14 (Washington DC: Brookings Institute, 2007) and Shmuel Even and Amos Granit, *The Israeli Intelligence Community: Where To?* (Tel Aviv: Institute for National Security Studies, 2009) (in Hebrew).

consolidation of responsibility.[45] Therefore, it is not surprising that tensions around the question of authority in the cyber realm have already emerged.[46]

Thus, ultimately, the question asked is "why not transform the current intelligence organizations to face the cyber adaptive challenge, rather than create new ones?"[47] One of the ways to do so is by introducing new structures at the operational level. In other words, the emphasis should be placed not on the issue of the "unity of command," but rather on platforms that enable flexible operations. By using this line of argument, what was defined as "special forces" in the context of the terror threat, could find new applications in the cyber world. One suggestion could come from the terror ballistics analogy, where the IDF created integrated "fire centers."[48] This organizational structure was developed in order to concentrate all tools necessary for detecting launchers and integrates different capabilities for achieving flexibility and agility at the tactical level.[49]

These collaborative platforms should not be limited to the local level only but could be enhanced also at the international level. As in the case of terror, this strategy of international cooperation does not lack problems of interests, laws, and politics; however, the Israeli government recognizes the importance of developing this area. Accordingly, for example, joint R&D

[45] The military developed a strong integrative arm vis-à-vis the civilian authorities in the form of the Home-Front Command to coordinate civil-defense issues. An attempt to operate a parallel body in the form of a special ministerial office, the Office for the Protection of the Home Front, has failed due to the inner political struggles in the government.

[46] For example, conflicts arose between the ISA and the NCB around the question of responsibility for defending critical civilian and public networks.

[47] Aviem Sella, "The Establishment of the National Cyber Authority—A Mistake," *Israel Defense*, April 6, 2015 (in Hebrew), http://www.israeldefense.co.il/he/content/הקמת-רשות-הסייבר-הלאומית-טעות .

[48] Israel Defense, "Employing any OrBat on the Ground or in the Air," *Israel Defense*, June 2, 2015, http://www.israeldefense.co.il/en/content/employing-any-orbat-ground-or-air.

[49] This should be distinguished from the Computer Emergency Response Team (CERT), which focuses on the main infrastructure sectors and responds to computer security attacks at a national level. A format closer to the concept of "special forces" is the Intervention Teams created by the Computer Services Directorate/C4I of the IDF. See Israel Defense, "Ready for Any Scenario: Military or Civil," *Israel Defense*, February 24, 2014, http://www.israeldefense.co.il/en/content/ready-any-scenario-military-or-civil.

efforts between Israel and international partners have been established,[50] as well as growing international cooperation between CERTs, by using special tools to share information, joint learning, and operation.[51] This trend, however, needs to be enhanced significantly. In this line of reasoning, prominent former security figures in Israel have hinted that the cooperation between the United States and Israel in the field is not optimal and there is a need for the creation of a "joint mechanism for integrating technological and intelligence capabilities." They mentioned that "operational partnerships between Israel and the United States have been around for decades, but there are different levels of cooperation in various fields," and "the best model to imitate is the cooperation in the field of missile defense, which spawned the development of the Arrow, Iron Dome, and Magic Wand."[52]

One possible model to follow could be the structure of international collaboration in the financial realm, of combating both money laundering and financing terrorism through a network of international organizations, like the Financial Action Task Force (FATF)[53] at the global level and the Financial Crimes Enforcement Network (FinCEN) at the national level.[54] This analogy by itself could serve as a subject of research for future studies.

It is not far reaching to suggest that, due to the special characteristics of the problem of cyber security, the two last recommendations of developing international as well as tactical collaborations may at some point converge.

[50] Israel Defense, "Israel's New National Cyber Operations Center," *Israel Defense,* November 13, 2014, http://www.israeldefense.co.il/en/content/israel%E2%80%99s-new-national-cyber-operations-center.

[51] Israel Defense, "IAI: Cyber R&D Center in Singapore," *Israel Defense*, February 13, 2014, http://www.israeldefense.co.il/en/content/iai-cyber-rd-center-singapore.

[52] Ran Dagoni, "Amos Yadlin: Cyber Defense includes Cyberattack," *Globes*, April 29, 2015 (in Hebrew), http://www.globes.co.il/news/article.aspx?did=1001031543.

[53] FATF is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. In 2001 the purpose expanded to include combating the financing of terrorism. It monitors countries' progress in implementing the FATF recommendations by engaging in peer reviews (mutual evaluations) of member countries. The FATF Secretariat is housed at the headquarters of the OECD in Paris. For more details, see www.fatf-gafi.org/.

[54] FinCEN is a bureau of the US Department of the Treasury, which collects and analyzes information about financial transactions in order to combat domestic and international money laundering, financing of terrorism, and other financial crimes. For more details, see www.fincen.gov/. Secretariat is housed at the headquarters of the OECD in Paris. For more details, see www.fatf-gafi.org/.

Because of the complexity, scale, and variation of the challenge, future cooperation could grow from the mere information exchange to integration and joint operations, perhaps even including the creation of joint task forces or the interchange of representatives in operational commands and units to act as collaborative officers.

## Conclusion

Analogies are vital instruments in facing new challenges. Threats in cyberspace are an enormous, technologically intensive, and rapidly evolving field that has a natural "calling" for using analogies and metaphors. Terror is not only a similar-sized conceptual phenomenon, isomorphic in its nature, and destructive in its impact on daily life but also an arena in which states have gained considerable experience and expertise.

This paper has tried to compare the cyber threat and the terror threat in a less intuitive manner, and a more analytical one. In accordance, the resolution of comparison was increased from "terror" to "terror ballistics" and limited to the Israeli context. The conclusion is that without disregard to caveats such as speed, scope, and unpredictability, much can be learned from the analogy.

The paper explored three main propositions. The first one is that key assumptions about the future of cybersecurity should be revisited. The second proposition is the possibility of adapting the "six Ds" counterterror framework—defense, detection, deterrence, defeat, denial, and diplomacy—to the cyber world. The third point is at the organizational level where the analogy highlights the need to create new flexible operational configurations, as well as international collaborative structures.

Furthermore, this framework leaves room for more inquiries. The most important ones should address the application of the concepts. For example, how can we translate concepts such as "deny" to cyber tactics? Is a security entity better in handling the national cybersecurity efforts than a civilian one? Other critical thinking could focus on how to assemble new forces and units, such as, what should be the components of these units and how should responsibilities and resources be distributed among them? In general, these questions illustrate the paper's main point, that the analogy between cyberthreats and terror should not only support advocacy for certain policies but should also open the door for a rich and relevant discourse, which will influence the creation of new concepts and ideas for action.

Finally, the conundrum introduced by the senior Israeli officer quoted at the beginning of this work still lingers. In hindsight, it is easy to see the development of the ballistic threat, and its system, components, and dynamics; nevertheless, operational cyber thinking is just at its beginning, especially at the level of the non-state actors. Thus, it is hard to imagine its exact character, leaving the question of what shape it would take and how to preempt its development as a key issue to address.

# Cyber, Intelligence, and Security

## Call for Papers

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

**Articles may relate to the following issues:**

- Global policy and strategy on cyber issues
- Cyberspace regulation
- National cybersecurity resilience
- Critical infrastructure cyber defense
- Cyberspace force buildup
- Ethical and legal aspects of cyberspace
- Cyberspace technologies
- Military cyber operations and warfare
- Military and cyber strategic thinking
- Intelligence, information sharing, and public-private partnership (PPP)
- Cyberspace deterrence
- Cybersecurity threats and risk-analysis methodologies
- Cyber incident analysis and lessons learned
- Techniques, tactics, and procedures (TTPs)

Articles submitted for consideration should not exceed 6,000 words (including citations and footnotes), and should include an abstract of up to120 words and up to ten keywords. Articles should be sent to:

Hadas Klein
Coordinator, ***Cyber, Intelligence, and Security***
Tel: +972-3-6400400 / ext. 488
Cell: +972-54-4510411
hadask@inss.org.il

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

**The Institute for National Security Studies – Cyber Security Program**
40, Haim Levanon St, POB 39950, Ramat Aviv, Tel Aviv 61398 | Tel: +972-3-6400400 | Fax: +972-3-7447588