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.