Israel – Hamas 2023 Symposium – Cyberspace – the Hidden Aspect of the Conflict

lieber.westpoint.edu/cyberspace-hidden-aspect-conflict

November 30, 2023

by Tal Mimran | Nov 30, 2023

The armed conflict between Israel and Hamas is a multi-arena war in two respects. First, in terms of geography, there are active hostilities in Gaza, Lebanon, the West Bank, and even Syria and Yemen. Second, there are several domains of hostilities, including ground, aerial, naval, and cyberspace. While much has been said about the ground, aerial, and naval aspects of this war (and the geo-political considerations surrounding it) the battleground in cyberspace has received little attention, notwithstanding its implications.

In this post, I discuss some of the hostile activities undertaken both by Israel and Hamas in the cyber domain. On one side, the pro-Palestinian hacking operations on various Israeli sites, and on the other side, Israel's actions in relation to Gaza Strip Internet infrastructure and, most notably, the imposition of a telecommunications blackout. In doing so, I identify relevant international legal considerations under international humanitarian law (IHL) and their application in the ongoing cyber-battle between Israel and Hamas.

Hacking Operations

As research by the Israeli cyber security company Check Point indicates, during the first weeks of the Israel-Hamas war, there was an increase of cyber attacks on targets in Israel. Most notably, there was an emphasis on attacks against the government and particularly the security sector, for obvious reasons, with a 52 percent increase in the number of cyber attacks.

These operations used several techniques including: distributed denial of service (DDoS) operations; wiper malware; and the exploitation of other vulnerabilities that facilitated the spread of disinformation about rocket attacks to frighten the population. The extent and nature of these operations raised the question of whether they only originated from Palestinian groups and hackers, or whether other players such as Iran (a tech-savvy State in terms of cyberspace) had joined in. As time went by, it became obvious that other actors indeed were supporting the efforts of Hamas against Israel in the cyber realm.

DDoS operations are designed to shut down a website or to halt its functionality due to "flooding" the site with many entry requests. The idea is to overload the website with false requests from a very large number of computers, sometimes by harnessing "innocent" computers that can be used in the operation without the owner's knowledge. As indicated by a Cloudflare report, on October 7, several DDoS attacks were launched against Israeli websites, leading at times to as many as millions of requests per second.

Newspaper and other media sites, software companies, banking, financial services and insurance and government administration websites all fell prey to such events. One particularly successful DDoS targeted the *Jerusalem Post* website, which was unable to operate for two days. The "Team_insane_Pakistan" and "Anonymous Sudan" hacking groups, known as religious hacktivist groups also linked to pro-Russian groups such as "Killnet," claimed the operation.

Hackers have also used wiper malware, a more sophisticated approach that is designed to erase data from files by overwriting or renaming them, or by creating random strings. One wiper malware example was named BiBi for political reasons (to provoke the Israeli government and the man leading it, Benjamin "Bibi" Netanyahu.) The malware was discovered both for Linux and Windows systems, indicating sophisticated capabilities on the part of the originator. From what is known thus far, most of these operations failed, though they had destructive potential and were attributed to the Arid Hamas-affiliated group. Their failure likely reflects the strength of cyber security in Israel, including in the private market, rather than lack of resolve or sophistication on the part of the group.

Of course, as with any government, Israeli cybersecurity has limited means to deal with hostile or malevolent cyber operations. Israel must contend with events from many hostile vectors which target a multitude of websites, both public and private. For example, some

successful practices of “hack and leak” have been documented, including one that leaked personal information of students of Ono Academic College, a private college in Israel. That event also caused the temporary closure of the college website.

Another successful attack was directed against the Israeli Rocket alarm application “Red Alert.” Red Alert is an open-source application used by Israeli citizens to receive notifications of incoming rockets attacks. The pro-Palestinian hacktivist group AnonGhost exploited a vulnerability in the app and sent fake notifications erroneously stating that a “nuclear bomb is coming.” This attack, which highlighted the danger of misinformation, was part of a broader misinformation effort designed to shape international discourse regarding the war and to promote the absurd notion that Zionism is connected to Nazism. It is worth noting that such actions bear concerning similarity to the Russian misinformation regarding the war in Ukraine.

Finally, vulnerabilities were exploited to hack digital billboards and present the Palestinian flag. One can only imagine what could have happened if the attackers would have used the successful take-over of the billboards to display some of the horrific videos documenting inhumane attacks against civilians on October 7. Some of the assaults (including murder, rape, removal of limbs and other atrocious means of causing harm) were filmed using the cell phones of the victims, which were later put back in the victims’ pockets for the families to find later. These tactics increased the sense of terror in Israel by forcing innocent victims and their families to relive, time and again, the horrors and atrocities committed by Hamas.

Telecommunications Blackouts

On October 27, the Internet connectivity rate in the Gaza Strip fell drastically for about 34 hours as Gaza experienced a telecommunications blackout. This has occurred more than once since the Israel Defense Forces’ (IDF) ground operations in the Gaza Strip began. In fact, even after Gaza’s Internet access was restored, data reveals that the connectivity rate lingered at around 15 percent of its usual connectivity.

The telecommunications blackout imposed by Israel was condemned by several international organizations. For example, the Director General of the World Health Organization (WHO) stated that the blackout made it “impossible for ambulances to reach the injured.” The Palestine Red Crescent Society offered a similar view, claiming that it completely lost contact with its operations room in the Gaza Strip. Criticisms were also voiced by other groups such as the American Near East Refugee Aid.

The act of imposing a blackout by Israel raises interesting legal issues, especially given the role of Israel in providing—at least partially—Internet services in Gaza. Alongside Palestinian corporations like Jawwal, some Israeli telecommunications companies provide both Internet and cellular services, and supply the necessary infrastructure for such services, in the Gaza Strip and the West Bank. This unique situation raises novel legal questions regarding the

responsibility of sides to an armed conflict in the context of humanitarian relief. It also invites discussion of the proper understanding of terms like “basic necessities” and “humanitarian relief” in the digital age.

Legal Perspective

States have been cautious about invoking international law in the context of cyber operations. They tend to refrain from denouncing cyber operations against them as violations of international law, or from attributing them to other States. Such reluctance appears to derive primarily from political and operational considerations. Further, it is feared that enhancing the regulatory role of international law in cyberspace may impede or impugn espionage activities resorted to by all States and limit the response options of victim States. Legal reluctance may also be attributable to the lack of credible international attribution mechanisms for hostile cyber operations.

This state of affairs appears to be changing, however. While there are disagreements as to the way that international law applies in cyberspace, some common understandings have emerged about key international law norms. States like Australia, France, Germany, Israel, the Netherlands, and the United Kingdom have articulated their legal positions on how international law applies in cyberspace. As is evident from such declarations, and from additional sources like the *Tallinn Manual*, cyber operations constitute an integral part of the reality of armed conflicts, and there is little question that the laws apply to armed conflicts.

Hostile Cyber Operations against Israel

While the incidents in the present case may raise general international law questions, for example concerning the principle of non-intervention, a customary law provision that is anchored in the UN Charter, I will focus on IHL norms in the context of the Israel-Hamas war.

Whereas a few States, like Iran, express reservations concerning the application of IHL to cyberspace, the majority of States to do not contest its application. Rather, they disagree on specific questions relating to its exact manner of operation. One notable disagreement concerns the question whether data can be regarded as a “protected object”. The position of the *Tallinn Manual*, which is supported by some States, is that only tangible things can constitute objects. But other States, like France, maintain that civilian data can constitute a protected object (see also, Giovannelli’s recent post on *Articles of War*).

Some protections under IHL are particularly relevant to cyber operations or attacks. For example, IHL prohibits attacks that are not directed against military targets, based on the principles of military necessity and distinction. Additionally, cyber attacks expected to cause harm to civilians and civilian objects that exceed their military utility (in light of the principle of proportionality) are prohibited. Cyber attacks directed at critical computer system infrastructure supporting objects indispensable for the survival of the civilian population, such as food or water supplies, have the potential to violate all the aforementioned principles.

Nevertheless, cyberspace presents a difficult challenge for distinguishing between military and civilian objects given the dual use of cyberspace and the integrated nature of its infrastructure. For example, civilian transportation vehicles and traffic controls are equipped with navigation tools that depend on global navigation satellite systems, which also serve governmental armed and security forces. Hence, even if a cyber-attack was designed to harm a particular military system that relied on satellite navigation infrastructure, a spill-over effect disrupting a vast number of other systems and networks dependent on the same infrastructure would be likely to occur. Additionally, it is almost impossible to delimit the impact of malware used in cyber attacks, because some may spread quickly to computers across many geographical regions.

Recent cyber operations against Israel bring the threshold for what constitutes an attack under IHL into question. Israel, for example, is of the view that in the cyber context, IHL attack rules are triggered only by operations that result in a kinetic consequence. Hence, a mere loss or impairment of functionality to infrastructure is insufficient to implicate IHL attack rules. Also, in Israel's view, only *tangible* things can constitute objects, thus civilian data are not protected by IHL attack rules. Therefore, under the interpretation adopted by Israel, operations aimed at leaking personal data or impeding governmental functions, do not amount to attacks under IHL and, as such, do not violate IHL principles like distinction. Of course, even if a hostile cyber operation does not constitute an attack, other international legal protections apply, such as the requirement to safeguard medical facilities.

It may seem that Israel is limiting itself with the legal policies and interpretations it promotes. For instance, it cannot claim that Hamas cyber operations violate IHL rules it deems inapplicable. Still, this approach is far from surprising for two reasons. First, Israel seems confident that it can deal with cyber threats relatively well. While DDoS operations can cause harm, far greater danger comes from more sophisticated attacks, like those directed against critical infrastructure and those that require a higher level of expertise and preparation to counter. Second, Israel may wish to maintain freedom of action for itself in cyberspace by setting high thresholds for the application of international law generally, and IHL in particular, to counter allegations of unlawfulness against Israeli operations in cyberspace.

Israel's Imposition of a Telecommunications Blackout

As recognized by the International Committee of the Red Cross (ICRC), "Medical personnel exclusively assigned to medical duties must be respected and protected in all circumstances." While Israel did not intend to attack medical personal or facilities by imposing a communications blackout, it nevertheless impacted them. The temporary blackout seemed to prevent some medical teams from performing their important functions temporarily. On the other hand, Israel has invoked mediating factors such as force protection, which is a legitimate consideration under international law (as recognized in the context of the NATO intervention in the former Yugoslavia), and has highlighted the temporary nature of the Internet blackout and its general efforts to accommodate medical needs in Gaza.

It appears that the communications blackout hindered some humanitarian relief (an obligation recently analyzed here). The obligation to admit humanitarian aid is customary, and it includes the obligation to "allow and facilitate rapid and unimpeded passage of humanitarian relief." Therefore, legal and practical solutions should have been identified prior to the blackout for example in the form of technical arrangements. It seems that Israel invests efforts in this regard, and this is important to strengthen cooperation with humanitarian organizations operating in Gaza and with international organizations.

Article 57(2)(c) of Additional Protocol I to the Geneva Conventions enshrines the (customary) obligation to provide an effective advance warning to "attacks which may affect the civilian population, unless circumstances do not permit." Therefore, it is worth asking whether the blackout interfered with the obligation of precaution, as the blackouts were performed amid the expansion of the ground operation in Gaza. In this regard, it should be mentioned that the IDF uses numerous methods of warning, like leaflets, social media, text messages, phone calls and television broadcasts to warn the civilian population (see e.g., Schmitt, *Articles of War*). While some of the forms of providing warning prior to an attack are impacted by the blackout (like notices in social media) there are still many forms that do not require an Internet connection. As such, it seems that Israel attempts to meet its obligation to warn prior to attacks.

Lastly, due to the crucial humanitarian nature of connection to the Internet (allowing families to make sure that they are safe, allowing a connection with international organizations, and providing an option to organize to move to a safer area), and the unique role of Israel in the facilitation of Internet services to the Gaza strip (see here, para. 19), it should be asked whether some duty to maintain the Internet connection is formed. On the one hand, the *Tallinn Manual* suggests that the Internet cannot be considered as an object indispensable to the survival of the civilian population. On the other hand, it seems that the connection to the Internet in Gaza means much more, as it impacts not only the well-being of people in Gaza, but also their personal security, their connection with their family, and the ability to receive medical attention if necessary. As such, even if an Internet service by itself does not deserve protection, there is still a duty incumbent on Israel not to impede deliberately the delivery of humanitarian relief.

Of special interest, there is the matter of the unique relationship between Israel and the Gaza strip, after decades of prolonged occupation and since Gaza depends on Israel for basic necessities. In the past, the Israeli Supreme Court recognized that Israel is obligated to supply Gaza with electricity, even after it left the strip and terminated the occupation. This logic, established in the *Al-Bassiouni* case, derives from the fact that the Gaza Strip was significantly dependent upon the supply of electricity from Israel, notwithstanding the lack of any legal rule that actually obligates Israel to do so (not IHL, nor from other fields).

It is interesting to consider whether a similar logic can be applied in relation to Internet services as well. In any case, as can be seen from the declaration made by the Israeli Defense Minister, the IDF is gaining effective control of Gaza with every day that passes, and as such the discussion may soon need to be conducted with another regime in mind, that of occupation law. Once established, the occupation will increase Israel's obligations towards the civilian population in Gaza, and in our context, might implicate a duty to facilitate Internet and cellular access in the area.

Conclusion

The Israel-Hamas war demonstrates the growing role of cyberspace in warfare. Further, the conflict impacts the ongoing political discussion over the regulation of cyber operations in the context of armed conflicts. It also shows the significance of taking a stance as to the application of international law, in the sense of obliging oneself to the interpretation presented. In this case, given Israel's desire to maintain freedom of action in cyberspace for itself, it cannot invoke IHL against numerous hostile cyber actions conducted by Hamas thus far.

In addition, this conflict raises novel questions as to the ability to harness Internet and telecommunications supremacy against opponents on the battlefield. In particular, the decision of Israel to impose telecommunications blackouts might impact its ability to meet its own responsibilities under IHL, such as the duty of precaution or the prohibition on interfering with the provision of humanitarian relief. For now, it seems that Israel is aware of this issue, and is dedicating efforts in upholding its obligations.

These challenges are only made more complex given the unique relationship between Israel and Gaza, even after the termination of decades of occupation (based on the view of the Israeli Supreme Court in the *Al-Bassiouni* case) and the possibility of a future Israeli occupation of Gaza in the aftermath of the current conflict.

***

Dr. Tal Mimran is an adjunct lecturer at the Hebrew University of Jerusalem and at the Zefat Academic College. He is the Academic Coordinator of the International Law Forum of the Hebrew University, and the Research Director at the Federmann Cyber Security Research Center in the Law Faculty of the Hebrew University.

Photo credit: Unsplash

The Legal Context of Operations Al-Aqsa Flood and Swords of Iron

by Michael N. Schmitt

October 10, 2023

–

Hostage-Taking and the Law of Armed Conflict

by John C. Tramazzo, Kevin S. Coble, Michael N. Schmitt

October 12, 2023

–

Siege Law and Military Necessity

by Geoff Corn, Sean Watts

October 13, 2023

–

The Evacuation of Northern Gaza: Practical and Legal Aspects

by Michael N. Schmitt

October 15, 2023

–

A “Complete Siege” of Gaza in Accordance with International Humanitarian Law

by Rosa-Lena Lauterbach

October 16, 2023

–

The ICRC’s Statement on the Israel-Hamas Hostilities and Violence: Discerning the Legal Intricacies

by Ori Pomson

October 16, 2023

–

Beyond the Pale: IHRL and the Hamas Attack on Israel

by Yuval Shany, Amichai Cohen, Tamar Hostovsky Brandes

October 17, 2023

–

Strategy and Self-Defence: Israel and its War with Iran

by Ken Watkin

October 18, 2023

–

The Circle of Suffering and the Role of IHL

by Helen Durham, Ben Saul

October 19, 2023

–

Facts Matter: Assessing the Al-Ahli Hospital Incident

by Aurel Sari

October 19, 2023

–

Iran's Responsibility for the Attack on Israel

by Jennifer Maddocks

October 20, 2023

–

Inside IDF Targeting

by John Merriam

October 20, 2023

–

A Moment of Truth: International Humanitarian Law and the Gaza War

by Amichai Cohen

October 23, 2023

–

White Phosphorus and International Law

by Kevin S. Coble, John C. Tramazzo

October 25, 2023

–

After the Battlefield: Transnational Criminal Law, Hamas, and Seeking Justice – Part I

by Dan E. Stigall

October 26, 2023

–

The IDF, Hamas, and the Duty to Warn

by Michael N. Schmitt

October 27, 2023

–

After the Battlefield: Transnational Criminal Law, Hamas, and Seeking Justice – Part II

by Dan E. Stigall

October 30, 2023

–

Assessing the Conduct of Hostilities in Gaza – Difficulties and Possible Solutions

by Marco Sassòli

October 30, 2023

–

Participation in Hostilities during Belligerent Occupation

by Ioannis Bamnios

November 3, 2023

–

What is and is not Human Shielding?

by Michael N. Schmitt

November 3, 2023

–

The Obligation to Allow and Facilitate Humanitarian Relief

by Ori Pomson

November 7, 2023

–

Attacks and Misuse of Ambulances during Armed Conflict

by Luke Moffett

November 8, 2023

–

Distinction and Humanitarian Aid in the Gaza Conflict

by Jeffrey Lovitky

November 13, 2023

–

Targeting Gaza's Tunnels

by David A. Wallace, Shane Reeves

November 14, 2023

–

Refugee Law

by Jane McAdam, Guy S. Goodwin-Gill

November 17, 2023

–

After the Conflict: A UN Transitional Administration in Gaza?

by Rob McLaughlin

November 17, 2023

–

The Law of Truce

by Dan Maurer

November 21, 2023

–

International Law “Made in Israel” v. International Law “Made for Israel”

by Yuval Shany, Amichai Cohen

November 22, 2023