

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

# Israel's Attack on *Hamas*' Cyber Headquarters Under Customary International Humanitarian Law

*GIAC (GLEG) Gold Certification*

Author: Jonathan Matkowsky, RiskIQ, jonathan-m@riskiq.com
Advisor: Chris Walker
Accepted: Nov. 21, 2019

Author's Note

Thanks to Serge Droz, Judah Ari Gross, Maarten Van Horenbeeck, Michael Peil, and Mark Seiden for valuable feedback, which improved the quality of this paper. Views expressed in the paper do not necessarily represent those of RiskIQ or any contributor.

Abstract

During intense military fighting in May 2019, Israel stopped the *Hamas* organized-armed-group from harming Israeli sites as part of establishing offensive cyber capabilities in the Gaza Strip tied to its war effort. Israel attacked the headquarters from which *Hamas*' cyber unit operated, including any information systems and related cyber-infrastructure in the facility. Under customary international humanitarian law, the attack on *Hamas*' headquarters appears to be a cyber-specific example of a lawful military objective due to its inherent nature, as suggested by Prof. R. Chesney (2019). This paper discusses the principles of international humanitarian law—military necessity, humanity, distinction, and proportionality—applicable from an Israeli law perspective to the targeted strike on the *Hamas*' cyber headquarters, including support that the principles have achieved the status of customary international humanitarian law. Israel did not disclose whether *Hamas* only used the facility for intelligence gathering tied to the war effort alone, or if that intelligence was also being used to develop cyber weapons. Both are inherently lawful military objectives under customary international humanitarian law, according to Prof. Dinstein (2016). A key takeaway is that applying the principles of customary international humanitarian law may sometimes favor using traditional military force, and other times favor using cyber activity.

© 2019 The SANS Institute Author retains full rights.

# 1. Introduction

Where applicable, this paper interprets customary international humanitarian law (CIHL) from an Israeli law perspective. Generally, decisions of national courts bear on "the existence and content of rules of customary international law" (ILC Draft, 2018, p. 149 [Conclusion 13]; ILC Memo, 2016).

The paper does not evaluate Israel's attack on the facility from which *Hamas*' cyber unit operated (*Hamas*' cyber headquarters) (IDF Statement, 2019) according to applicable international treaty obligations. Treaty provisions are referenced, however, to the extent they reflect CIHL (Targeted Killings, 2006, paras. 19, 20).

For example, Israel is a party to the Hague Regulations (1907), which has a status of CIHL (Targeted Killings, 2006, para. 20). Israel is also a party to the Fourth Geneva Convention (1949) (Targeted Killings, 2006, para. 20), and its customary provisions are part of Israeli law even without any implementing legislation (Targeted Killings, 2006, para. 20). Israel is not a party to AP I (1977); however, Israel abides by its provisions as reflecting rules of CIHL (Targeted Killings, 2006, para. 20). The International Court of Justice (ICJ) (1996) held that rules in AP I bind all States, which, when adopted, were "merely the expression of the pre-existing CIHL…" (para. 84).

The first section of the paper (*infra*, sect. 2.1) describes the targeted strike on *Hamas'* cyber headquarters. The next part (*infra*, sects. 2.2-2.4) discusses the principles of CIHL applicable to the targeted strike—military necessity, humanity, distinction, and proportionality—including support that the principles have achieved the status of CIHL. The following section of the paper (*infra*, sect. 2.5) applies the CIHL principles to the targeted strike. The final section (*infra*, sect. 3) concludes with some general observations.

# 2. The Targeted Strike is a Cyber-Specific Illustration of a Proper Military Objective According to CIHL

## 2.1. The Targeted Strike

The Israel Defense Forces (IDF) cleared for publication on May 5, 2019 that *Hamas* was attempting to establish offensive cyber-capabilities within the Gaza Strip

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

(IDF Statement, 2019). The IDF stated (IDF Statement, 2019) that after thwarting *Hamas*' cyber activity, including a recent operation that same weekend to harm Israeli sites, the IDF approved a targeted airstrike on *Hamas*' cyber headquarters (Targeted Strike).

The Military Advocate General's Corps. (MAG), the unit within the IDF responsible for implementing the rule of law (IDF Website, *n.d.*), would have approved the Targeted Strike. MAG is subordinate only to the Israeli Attorney General (Merriam and Schmitt, 2015, p. 87), subject to the authority of the Supreme Court in Israel sitting in the first and last instance as a High Court of Justice (HCJ) against government actions (*e.g.*, Yesh Din, 2018, para. 61; Dinstein, 2019, paras. 79-86). MAG approved the Targeted Strike based, in part, on the IDF establishing, to its satisfaction, that the military object was, in fact, *Hamas*' cyber headquarters. The IDF determined that *Hamas*' cyber unit are formal members of *Hamas*—or at least functioning as members, such as in terms of the tasks being carried out, or being subject to the same chain of command as other *Hamas* formal members (*cf*. Shamir-Borer, 2018, p. 966). Israel then also "politically attributed" the thwarted cyber operation and related cyber-activity to *Hamas* in Gaza supported by the technical attribution associating the software, computer and networking artifacts, and intelligence (Romanosky & Boudreaux, 2019, p.4).

Before the Targeted Strike, the last-known airstrike against military objects or combatants in response to harmful cyber-activity was the U.S. assassination of ISIL hacker, Junaid Hussain, in Raqqa, Syria (Hamid, 2018). Hussain had uploaded the personal contact data of U.S. military and government personnel to actively recruit "lone wolf" targeted assassinations of the individuals in their homes (Cronk, 2015).

*Hamas* and *Palestinian Islamic Jihad* attacked Israel with more than six hundred and ninety rockets the first weekend in May 2019 (48 Hr. Update). Israel responded during that same weekend with focused strikes against not only *Hamas*' cyber headquarters, but approximately three hundred and fifty military targets in Gaza (48 Hr. Update).

The IDF confirmed that its Targeted Strike neutralized the then-current cyber capabilities of *Hamas* in Gaza (Gross, 2019a), but did not target any individuals in



© 2019 The SANS Institute Author retains full rights.

*Hamas*' cyber-unit with the "know-how" to rebuild (A. Gross, personal communication, Sept. 22, 2019).

In contradistinction to the attack on *Hamas*' cyber headquarters, the IDF cleared for release the targeted assassination of Iran's "money man" in Gaza held responsible for funding the rockets to attack Israel (Target Tweet, 2019).

If the IDF did not target the *Hamas*' cyber unit but attacked the facility in which it operated, it is reasonable to infer that if members of *Hamas*' cyber unit were in the facility just before the attack took place, they were successfully warned to evacuate (*cf.* Sharvit-Baruch and Neuman, 2011).



(*Photo of attacked Hamas*' *cyber headquarters; Source: IDF*)

There is no basis to presume that *Hamas*' cyber unit was developing or had "cyber means of warfare" in the facility—that is, cyber activity against Israel that would cause injury to, or death of, persons or damage to, or destruction of, objects (TM2, r. 103, para. 2). The thwarted *Hamas*' cyber operation was part of *Hamas*' cyber activity from the attacked facility to develop offensive cyber capabilities against Israel (IDF Statement, 2019). The IDF did not release any details on the kind or type of offensive cyber



© 2019 The SANS Institute Author retains full rights.

capabilities because any more detail might reveal to *Hamas* details about Israel's cyber capabilities (Gross, 2019a).

In 2017, however, the IDF cleared for release that *Hamas* installed malware on IDF soldiers' cellphones, allowing *Hamas* to "download contacts and files, GPS data, photographs, collect text messages and install additional applications on the device" (Gross, 2017). *Hamas* was technically capable of recording images of what was happening on IDF bases by controlling soldiers' phones (Gross, 2017). It had full control, including the ability to take pictures of offices, the insides of tanks or computer screens, and then to transfer the files to any server (Gross, 2017).

In 2018, ClearSky Cyber Security firm published that *Hamas* was trying to install a counterfeit of the official Code Red rocket warning app; this would give *Hamas* command and control to "track the device, take pictures, record sound and make calls and send messages" (Gross, 2018).

Two weeks after the Targeted Strike, on May 15, 2019, an Israeli broadcaster attributed to *Hamas* a several minute interruption to its live stream of the Eurovision Song Contest the night before (Gross, 2019b). The defaced stream displayed a spoofed IDF alert falsely warning viewers within 1.2km of the Eurovision venue in north Tel Aviv to immediately seek shelter from an imminent rocket attack (Gross, 2019b). At the time, the Israeli National Cyber Directorate confirmed that the Eurovision operation appeared to be attributable to *Hamas* (Gross, 2019b). It is unclear, however, whether *Hamas*' cyber unit in Gaza quickly re-deployed after the Targeted Strike or if the Targeted Strike had neutralized different cyber-means of warfare in the facility. Even if attributable to *Hamas*, nobody stated the spoofed alert was from rebuilt Gazan capabilities; for example, perhaps it was a foreign *Hamas* cell.

Based on *Hamas*' cyber activities described above, perhaps *Hamas*' attempt to harm Israeli sites during the first weekend in May 2019 was designed to spread terror by causing some unpleasant cognitive effect on Israeli civilians.

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

## 2.2. Applicable Law

There is a "continuous state" of armed struggle for decades between Israel and *Hamas* to which the law of international armed conflict (LOIAC)—international humanitarian law—applies, even though it is not a conflict between two states (Targeted Killings, 2006, para. 16; Yesh Din, 2018, para. 38).[1] According to the HCJ, during periods of combat between Israel and whoever is controlling the Gaza Strip, LOIAC should be upheld regarding the conduct of hostilities—not just law enforcement principles (Yesh Din, 2018, para. 39). LOIAC includes the laws of belligerent occupation, but also applies to every case of an armed conflict of an international character, *i.e.*, crossing the border, regardless of whether the place where the armed conflict is occurring is subject to a belligerent occupation (Targeted Killings, 2006, para. 18; *cf.* Comm'n Inquiry, 2018, para. 68).

There is no consensus on whether non-State actors may initiate an armed attack (TM2, r. 71, para. 3). There is also no consensus on the degree of organization required by non-State actors as a matter of law to qualify as an armed attack by the same group (TM2, r. 71, para. 21); however, the international community notably characterized the 9/11 attacks by *Al Qaeda* on the U.S. as an 'armed attack' (TM2, r. 71, para. 21). The HCJ found that according to LOIAC, changes that occur on the ground may necessitate an "individual examination" of the appropriate "action paradigm for each concrete use of force": Sometimes the "law enforcement" paradigm applies where the authority of responsive force is "more limited" to enforce order, and other times, a "conduct of hostilities" paradigm applies, where potentially lethal force may be used in order to obtain specific objectives, and as the "last resort after the use of less harmful means has been exhausted" (Yesh Din, 2018, para. 3).

"The fact that the terrorist organizations and its members do not act on behalf of a state does not make the struggle merely an internal matter of the state" (Targeted

[1] *Background_facts*. (*n.d.*) are available from the author for those that want broader historical context on the armed conflict, which changed in 2005 from an Israeli-law perspective when Israel lost sufficient capability to enforce order and manage civilian life in Gaza.



© 2019 The SANS Institute Author retains full rights.

Killings, para. 21). Their military capacity may exceed even the capacity of a State, so dealing with these dangers cannot possibly be limited to the internal affairs of a state and its criminal law (Targeted Killings, 2006, para. 21). Israel security forces do not possess any "policing and enforcement" means, such as arrest and interrogation, in Gaza (Yesh Din, 2008, para. 8).

Given the increased hostilities over the May 5-6 weekend, the "conduct of hostilities" paradigm appears to be the generally appropriate paradigm applicable to the Targeted Strike, according to international humanitarian law.

## 2.3. Consolidated Norms of Customary International Law

CIHL is part of customary international law. Most of LOIAC has "consolidated over the decades as norms of customary international law" (Dinstein, 2016, para. 43).

Customary rules of international law are "state practices recognized by the community at large as laying down patterns of conduct" that must be followed (Shaw, 2017, p. 5). "It is possible to detect two basic elements in the make-up of a custom. There are the material facts, that is, the actual behavior of states, and the psychological or subjective belief that such behavior is 'law'" (Shaw, 2017, p. 55). "Customary international law is unwritten law deriving from practice accepted as law" (ILC Draft, 2018, para. 66[3]). "Israel attributes great importance to the adoption of a thorough and rigorous approach to the identification of customary norms" (ILC Comments, 2018, p. 6).

Currently, it is challenging to "identify any cyber-specific customary international law" because there is not enough transparency by State actors (TM2, p. 3). "States whose practices in cyberspace are transparent may, therefore, benefit from the ability to control and steer the development of customary international law toward a desirable direction" (Kilovaty, 2019, p. 90).

## 2.4. CIHL Principles Applicable to the Targeted Strike

According to the International Court of Justice (ICJ), rules of CIHL (traditionally called "laws and customs of war") are based partly upon the St. Petersburg Declaration of 1868 as well as the results of the Brussels Conference of 1874 (ICJ Nuclear, 1996, para. 75). The St Petersburg Declaration (1868) prohibits by international agreement, the use



© 2019 The SANS Institute Author retains full rights.

of certain weapons in war. The Declaration confirms the customary rule that specific types of arms, projectiles, and material of a nature to cause unnecessary suffering are prohibited (St Petersburg Decl., *n.d.*). At the Brussels Conference, European States met on the initiative of Czar Alexander II of Russia to examine the draft of an international agreement related to the laws and customs of war submitted to them by the Russian Government (Brussels Decl., 1874). The Brussels Declaration is a primary source of the Hague Regulations (Brussels Commentary, *n.d.*).

CIHL requires that there be counsel available to military commanders to understand the CIHL principles and that the principles be disseminated not only to combatants but also to as many civilians as possible (Dinstein, 2016, para. 109). CIHL principles include (a) Military Necessity, (b) Humanity, (c) Distinction, and (e) Proportionality.

Military Necessity during armed conflict permits any amount and kind of force to keep one's forces safe and compel the complete "submission of the enemy" using measures not otherwise forbidden by international law (Corn et al., 2019, pp. 50, 136; Dinstein, 2016, para. 27). Humanity prohibits causing unnecessary suffering to combatants (Dinstein, 2016, paras. 191-96). Distinction requires each side to distinguish civilians and civilian inanimate objects from combatants and inanimate military objects (TM2, r. 93; Robertson, 2017; Corn et al., p. 55). Proportionality requires "limiting the scope, intensity, and duration of attack to that which is reasonably necessary to counter the attack or neutralize the threat" (Corn et al., 2019, p. 22), and to forego attack if it is expected to "cause loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive when compared with the concrete and direct military advantage anticipated" (Corn et al., 2019, pp. 57-58) (citing AP I, 1977, para. 5(b)).

Applying the principles of CIHL requires fact-finding. These findings should be in scope of what a reasonable military commander "by dint of training and experience, would foresee and assess the anticipated military advantage and the expected collateral damage" of attacking a target in a specific domain (air, land, sea, space, cyber) (Henderson & Reece, 2018). The HCJ in Targeted Killing (2016, para. 57) uses a



© 2019 The SANS Institute Author retains full rights.

"reasonable military commander" standard (quoting HCJ 2056/04 *Beit Sourik Village Council v. Government of Israel* [2004]). Of course, the operational environment bears on this assessment (Merriam & Schmitt, 2015).

Each of the principles is elaborated on below, including support that they are a part of CIHL (*infra*, sects. 2.4.1 - 2.4.4).

### 2.4.1. Military Necessity

The principle of Military Necessity may be traced at least as far back as an 1863 "detailed code of rules followed by Union forces" during the American Civil War written by Prof. Lieber of Columbia College and promulgated by U.S. President Abraham Lincoln (Corn et al., 2019, pp. 44-45). A State is entitled by this principle to use combat power in any way that it believes is necessary to win a war but only within the bounds of LOIAC (Dinstein, 2016, para. 27).

"Military objective," as a "component of military necessity" (Corn, 2019, p. 261), is "widely accepted" to express CIHL (Dinstein, 2016, para. 276).

Reflective of CIHL on targeting (ICRC, 2019), Article 52(2) of AP I (1977) contains a definition of "military objective" that is generally considered to be customary as "those objects which *by their nature, location, purpose or use* make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage" (quoted by Corn et al., 2019, p. 261) (emphasis added). Israel's *Manual on the Rules of Warfare* used in the IDF School of Military Law (2006) (ICRC, 2019) incorporates this principle.

The term "nature" emphasized above in Article 52(2) of AP I is defined in the Commentary to AP I (1987) as "all objects directly used by the armed forces" (para. 2020) (cited by Corn et al., 2019, p. 261). "The key to this category of targetable items is that the very nature of the object…was to serve a military purpose….The object has a certain status because of its nature, not because of any other actions or uses" (Corn et al., 2019, p. 261).



© 2019 The SANS Institute Author retains full rights.

The majority point of view is that objects that satisfy the "nature" criterion are always targetable, subject to other applicable rules of LOIAC (TM2, r. 100, para. 16). Because they are military objects, the objects are deemed to contribute to military action; attacking a military object yields a definite military advantage because it is deemed to contribute to military action of enemy forces.

According to Prof. Dinstein, a non-exhaustive catalog of specific illustrations of inherent military objectives avoids vagueness and helps operationally to anticipate future scenarios (Dinstein, 2016, para. 278). "No abstract definition standing by itself (unaccompanied by actual examples) can offer a practical solution to real problems that have to be wrestled with – often with dismaying rapidity – on the battlefield" (Dinstein, 2016, para. 278). Prof. Dinstein's list includes an R&D facility for weapons and an intelligence-gathering center tied to the war effort (Dinstein, 2016, para. 296).[3]

In contradistinction to the term "purpose" in Article 52(2) of AP I, the term "use" is defined in the Commentary as those objects that become military objectives through their actual role or "present function" under the circumstances for military purposes even though they started out serving civilian functions (Commentary to AP I, 1987, para. 2022) (quoted by Corn et al., 2019, p. 263). Article 52(2) of AP I uses the term "purpose" to cover scenarios where "the intended future use of an object" qualifies the object as a military objective (Commentary to AP I, 1987, para. 2022) (quoted by Corn et al., 2019, p. 262). The object acquires the status of a military objective "as soon as such a purpose becomes clear; an attacker need not await its conversion to a military objective through use" (TM2, r. 100, para. 13).

[3] There is no consensus, however, as to whether remote cyber espionage, such as exfiltrating classified data from another State's military cyber system without consent, violates LOIAC (TM2, r. 32, para. 8). It is generally challenging to draw the line between cyber espionage and offensive cyber operations; they both usually require penetration of a system, often by the introduction of malware or a successful phishing operation (TM2, r. 32, para. 13).

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

### 2.4.2. Humanity

Apart from the principle of Distinction, the prohibition against causing unnecessary suffering, which means any "harm greater than that unavoidable to achieve legitimate military objectives," is the only other "cardinal" principle of CIHL according to ICJ Nuclear (1996, para. 78). The principle of Humanity is to be observed by all States irrespective of whether they have ratified the Geneva[4] and Hague Conventions[5] that embody them (ICJ Nuclear, 1996, para. 79) (references added).

As early as 1899, the preamble to Hague IV (known as the "Martens Clause" in recognition of the Russian diplomat who proposed the language) expressly references the "laws of humanity, and the requirements of the public conscience" (Corn, 2016, pp. 44-46). The ICJ cites the Martens Clause as a source of this CIHL principle (along with the principle of Distinction, and article 1(2) of AP I as the "modern" version of the Martens Clause). Article 1(2) of AP I states that the "principles of humanity" are part of CIHL.

ICJ Nuclear (1996) explains that the Nuremberg International Military Tribunal found in 1945 that the humanitarian rules included in the Hague Regulations are "regarded as being declaratory of the laws and customs of war" (para. 80) (internal citation omitted).

Targeted Killing (2016) does not explicitly state Article 1(2) of AP I reflects CIHL; however, the HCJ emphasizes that the balance between humanitarian and military considerations is the entire basis for LOIAC (para. 22).

---

[4] See generally Treaties, states parties, and commentaries - Geneva Conventions of 1949 and Additional Protocols, and their Commentaries (*n.d.*). Retrieved from https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp Archived at https://perma.cc/H2XG-RC39

[5] See generally Treaties, states parties, and commentaries - Hague Convention (IV) on War on Land and its Annexed Regulations, 1907 (Hague IV) (*n.d.*) Retrieved from https://ihl-databases.icrc.org/ihl/INTRO/195 Archived at https://perma.cc/HCF9-9PJJ



© 2019 The SANS Institute Author retains full rights.

### 2.4.3. Distinction

The St. Petersburg Declaration (1868) provides that "the only legitimate object" that States should endeavor to accomplish during war is to "weaken the military forces of the enemy..." This principle is sometimes referred to as the "grandfather of all principles and is the application of the balancing of humanity and military necessity in targeting" (Corn et al., p. 252). The principle is "that military attacks should be directed at combatants and military targets, and not civilians or civilian property" (Corn et al., p. 252). The ICJ (1996) views the principle of Distinction prohibiting States from making civilians the object of attack, as the only other "cardinal" principle apart from the prohibition against causing unnecessary suffering to combatants that always applies without any exception under CIHL (ICJ Nuclear, paras. 78, 79). The HCJ states that AP I (Article 51(2)) reflects this customary principle, and "gives rise to the duty to do everything to minimize the collateral damage to the civilian population when carrying out attacks on 'combatants'" (Targeted Killings, 2006, para. 26) (internal citation omitted).

Furthermore, according to the HCJ, Article 48 ("to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall…distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives") of AP I (1977) is a "fundamental" distinction that is part of CIHL (Targeted Killings, 2006, para. 23).

For purposes of applying the principle of Distinction, the HCJ refers to Article 50(1) ("In case of doubt whether a person is a civilian, that person shall be considered…a civilian") of AP I (1977) to support generally classifying unlawful combatants as civilians and not as combatants (Targeted Killings, 2006, para. 26).

Also, in applying the principle of Distinction, "the rules for the targeting of individuals are more restrictive" than those about targeting inanimate objects (ICRC Report, p. 32 n.87). Although *Hamas*' cyber unit was not itself targeted, as formal members of *Hamas*, they would not be immune from attack as they are directly participating in the armed conflict. "[CIHL] provides that a civilian who takes a direct



© 2019 The SANS Institute Author retains full rights.

part in the hostilities does not at the same time enjoy the protection given to a civilian who is not taking a direct part in those acts" (Targeted Killings, 2006, para. 26).

The HCJ points out that the Int'l Criminal Tribunal for the former Yugoslavia has held that Article 51 of AP I (1977) is part of CIHL (Targeted Killings, para. 30) (internal citation omitted). The HCJ accepts the position of the Red Cross that all of Article 51(3) of AP I, which affords protective enjoyment on civilians "unless and for such time as they take [a] direct part in hostilities" (1977), is part of CIHL (Targeted Killings, 2006, para. 30).

Partaking in "hostile" acts under CIHL embodied in Article 51(3) of AP I, for purposes of being considered DPIH applies to all acts that by their nature or purpose are intended to cause harm to armed forces or civilians (Targeted Killings, 2006, para. 33). There is no "clear and uniform definition of [what qualifies as] "direct" participation in hostilities as adopted from CIHL in art. 51(3) of AP I and each case must be judged on its own merits (Targeted Killings, 2006, para. 34). The test for DPIH is whether the decision conforms to what a "reasonable military commander" would have decided under the circumstances (Targeted Killings, 2006, para. 57). One example that satisfies the DPIH threshold is "someone who collects information about the armed forces, whether in the spheres in which the hostilities are being carried out…or whether outside the spheres" (Targeted Killings, 2006, para. 35) (internal citation omitted). "[DPIH] does not only include acts inflicting harm on the enemy by direct attack, but also attempts at hindering its military operations in any way," including "intelligence gathering" (Corn et al., 2019, p. 496) (internal citation omitted).

The HCJ also found that there is no consensus with regard the scope of the expression "for such time" under CIHL embodied in Article 51(3) of AP I. If someone becomes a member of an organized armed group, however, the group becomes his "home" whereby the time in between acts of hostilities is preparation for the next hostile act, and therefore, part of the same time such person is DPIH (Targeted Killings, para. 39). In the grey zone, where "[CIHL] has not yet been formulated," each case must be examined on its own merits (Targeted Killings, para. 40) (finding that in doing so, there



© 2019 The SANS Institute Author retains full rights.

must be certain kind of correctly verified and reliable information related to the identity and activity of the civilian who is claimed to be DPIH).

### 2.4.4. Proportionality

Under the principle of Proportionality, a civilian should not be attacked even when they are taking DPIH if it is possible to use less harmful measures, including, preferably, resort to the justice system, such as by arresting, interrogating, and prosecuting them (Targeted Killings, 2006, para. 40). Notably, these less harmful ways may have been more of an option before Israel withdrew from Gaza in 2015.

The HCJ (2006) points to ICJ Nuclear (1996, para. 41) for support that AP I embodies the principle of Proportionality, which "applies in every case where civilians who are not taking a direct part in hostilities at the time are harmed" (Targeted Killings, 2006, para. 43). The principle of Proportionality is part of CIHL as embodied in Articles 51(5)(b) and 57 of AP I (Targeted Killings, 2006, para. 42).

Article 51(5)(b) of AP I (1977) states that "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" is considered a kind of "indiscriminate" attack.

Article 57 of AP I requires, among other things, that a State "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (para. 2(a)(3)). The military commander must cancel or suspend any operation expected to cause "incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" (para. 2(b)). Article 57 also requires adequately warning of attacks that may affect the civilian population unless circumstances do not permit (para. 2(c)). "When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and… civilian objects" (para.



© 2019 The SANS Institute Author retains full rights.

3). Each Party must "…take all reasonable precautions to avoid losses of civilian lives and damage to civilian objects" (para. 4).

## 2.5. Applying the Principles to the Targeted Strike

The IDF does not publicly disclose the "specific command and control or doctrinal decision-making processes" used for airstrikes; however, IDF lawyers "figure heavily" in the target development process (Merriam and Schmitt, 2015, p. 75). Its International Law Department is involved, and CIHL experts participate when necessary (Merriam and Schmitt, 2015, p. 75). "Target development, target assessment, and pre-strike controls continue until the moment of attack" (Merriam and Schmitt, 2015, p. 81).

*Hamas*' cyber headquarters was a proper military objective because it was, by definition, established to contribute to *Hamas*' military action; therefore, it is not surprising that neutralizing it during active armed conflict offers a definite military advantage.

Because the thwarted cyber-operation was in the middle of an active armed conflict, it does not matter whether it independently rose to the level of a "cyber attack" under LOIA, meaning "reasonably expected to cause injury or death to persons or damage or destruction to objects" (TM2, r. 92).

When there is no active armed conflict, a State may exercise its right to respond to harmful cyber-operations in self-defense, for example, only if the cyber activity rises to the "level of an armed attack" (TM2, r. 71). Advisors look to the extent of the "reasonably foreseeable consequences of a cyber operation" to decide if it qualifies as an "armed attack" (TM2, r. 71, para. 13). For instance, targeting a water purification plant naturally causes sickness and death (TM2, r. 71 para. 13). If the primary purpose of the cyber activity is to cause "severe mental suffering" among a civilian population "tantamount to injury" (TM2, r. 92 para. 8), it may also qualify as a "cyber attack" (TM2, r. 98). On the other hand, targeting a State's choice of a "political, economic, social and cultural system, and the formulation of foreign policy," *i.e.*, *domain réservé*, by hacking into an actual election system to change the result or cast doubt on the veracity of the system through a cyber campaign, would likely amount to a legally prohibited intervention, but not constitute an "armed attack" triggering the right to self-defense



© 2019 The SANS Institute Author retains full rights.

during peacetime (Corn et al., 2019, pp. 526-27). The U.S., however, takes a more liberal view that any illegal use of force automatically rises to the level of an attack triggering the right to self-defense (Corn et al., 2019, p. 27) subject to other requirements, such as the principle of Proportionality (TM2, r. 71, para. 23).

Not every war-supporting effort, on the other hand, poses a direct threat to the enemy (Targeted Killings, 2006, para. 35). Some look to whether an operation is directed against critical infrastructure that causes severe effects (even if the effects are not destructive, *per se*) (TM2, r. 71, para. 13). For instance, a cyber operation against a major international stock exchange that would cause the market to crash would naturally cause loss of a catastrophic magnitude (TM2, r. 71, para. 12).

During peacetime, there is no settled way to differentiate activities that have reached the level of use of force to be considered an *attack* from an LOIA perspective from activities that would merely inconvenience or irritate (TM2, r. 71, para. 14, such as a temporary denial of service (TM2 r. 69, para. 10).

In terms of choosing between viable military objectives, all else being equal, attacking the *Hamas'* cyber headquarters may be compelling if *Hamas*' cyber offensive-capabilities may be further developed in a way that could cause severe harm.

If *Hamas*' cyber headquarters were being used to research and develop cyber means of warfare, then it would be analogous to an R&D facility for new weapons, which would make the facility a proper military objective by its very nature. In the context of what is known about *Hamas*' recent cyber operations, *Hamas'* cyber headquarters was being used to conduct cyber activity, such as possibly probing for weaknesses or testing defenses in Israel from Gaza as part of developing offensive cyber capabilities against Israel. Therefore, *Hamas*' cyber headquarters is analogous to a traditional intelligence-gathering center tied to a war effort, which is another quintessential illustration of a proper military objective by its very nature (irrespective of whether the facility was also being used to develop cyber means of warfare).

At the time that the IDF approved the Targeted Strike, the projected damage to the facility was not necessarily excessive as compared with the concrete and direct



© 2019 The SANS Institute Author retains full rights.

military advantage anticipated from neutralizing *Hamas*' cyber headquarters. The nature of *Hamas*' cyber headquarters was to serve a military purpose. It does not matter whether, at the time of the Targeted Strike, *Hamas*' cyber headquarters was in fact, gathering intelligence tied to the war effort or being used to develop a cyberweapon; the facility qualifies as a military objective if only by its nature—not requiring additional consideration of its use, purpose, or location.

As far as targeting individuals, *Hamas*' members are not lawful combatants under CIHL, partially because they do not observe the laws of war, and they do not distinguish themselves from civilians (*Targeted Killings*, 2006, para. 2). *Hamas* wears uniforms only during military parades; in combat, *Hamas*' militants disguise themselves as civilians and travel in civilian vehicles (Alon, 2018, p. 758). CIHL classifies *Hamas*' unlawful combatants as civilians (*Targeted Killings*, 2006, para. 31).

To target the *Hamas*' cyber unit (and not just its facility), members of the unit would have to be considered as highly likely to directly cause damage to the Israeli military operations and capacity of its military force, inflict death or injuries, or cause destruction to Israeli civilians (*Yesh Din*, 2018, para. 45).

Whether formal membership in an organized armed group qualifies for DPIH divides the international law community. For instance, there is some controversy whether the Israeli administration's adoption of a formal membership approach to targeting in the Gaza Conflict Report (2014) deviates from Targeted Killing (2018), which arguably took a functional approach—as opposed to a formal membership or status-based approach—to DPIH (Shereshevsky, 2018). However, "[i]n the locution of the Judgment in the *Targeted Killings*…an organized armed group becomes the 'home' of the person concerned for whom a respite – interposing between acts of hostilities – merely means preparation for the next round." (Dinstein, 2019, para. 319). "[They] may be targeted even when not personally associated with any specific hostile act, simply due to [their] membership in such a group, provided that the affiliation is in evidence and it does not lapse" (Dinstein, 2019, para. 319).

The U.S. also uses a functional membership approach to identify members of organized armed groups that may be targeted at any time; indicators of functional



© 2019 The SANS Institute Author retains full rights.

membership include whether someone is "carrying arms, exercising command over the armed group…carrying out planning related to the conduct of hostilities," or "performing tasks under a command structure of an organized armed group similar to those provided in a combat, combat support, or combat service support role in the armed forces of a State" (Corn et al., 2019, p. 159).

A reasonable Israeli military commander may have decided at the time that (a) the Targeted Strike would weaken *Hamas* and that (b) the nature or purpose of the cyber activity in the facility was intended to cause harm to Israeli forces or civilians. Developing cyber offensive capabilities to collect information about the IDF standing-alone constitutes DPIH.

The status of *Hamas*' cyber unit as DPIH (regardless of whether such members are actively participating in a hostile act at any specific moment) is what makes the facility capable of being deemed military by its very nature and not only a military objective through its use. If the members were only DPIH when they were actively participating in the hostilities, then the facility would only be considered '*Hamas*' cyber headquarters' for such time when it is actively being used by *Hamas*' cyber unit.

Perhaps *Hamas*' cyber unit (as opposed to *Hamas'* cyber headquarters) was not targeted because in applying the principle of Proportionality, an Israeli military commander determined that targeting the facility would be adequate to end the increased hostilities. There was no incidental damage to civilian objects in the facility to possibly be considered excessive when weighed against the concrete and direct military advantage anticipated from the Targeted Strike.

Perhaps there was a choice between the Targeted Strike and other military objectives, and MAG approved the Targeted Strike because it was expected to cause less danger to civilians or civilian objects. There is no evidence to support that the IDF did not take all reasonable precautions to avoid losses of civilian lives and damage to civilian objects.

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

## 3. General Observations

Israel demonstrated accountability to the international community by transparently releasing during wartime that it is treating *Hamas*' cyber headquarters as a military objective. While Israel did not disclose whether *Hamas*' cyber headquarters was used for intelligence gathering tied to the war effort alone, or if that intelligence was also being used to develop cyber weapons, both are inherently lawful military objectives under CIHL.

There is no wooden rule that either traditional military force or cyber activity is more appropriate under the principles of CIHL during armed conflict. For example, in response to downing a U.S. UAC (uncrewed-aerial-vehicle) on a reconnaissance mission in the Gulf of Oman, in late June 2019, the U.S. responded to the Iranian military strikes by targeting the missile command and control systems of the Islamic Revolutionary Guard Corps. with a cyberattack, rather than responding with traditional military force, to avoid killing one hundred and fifty people (Diamond, Star and Sullivan, 2019). This arguably "heralded a fundamental shift in the U.S. approach to cyberwarfare," reflecting a willingness to respond to physical attacks through cyberwarfare under new guidelines that President Trump put into place last year (Stratfor, 2019). The "offensive U.S. cyber doctrine" reflected in its 2018 Command Vision strives to "defend forward as close as possible to the origin of the adversary activity" (Stratfor, 2019). For instance, this past February, the U.S. Cyber Command took the Internet Research Agency offline in St. Petersburg to thwart cyber-attempts to interfere with U.S. mid-term elections (Nakashima, 2019).

The British starting point is that it will "not always react identically to every individual incident, and a cyber attack will not necessarily encounter a cyber response" (Foreign & Commonwealth Office, 2019). Just like CIHL principles may favor one domain of warfare over others, depending on the circumstances, "[d]eterrence in the cyber age will [also] not be a one-size-fits-all strategy. Instead, it will be a complicated, multilayered strategy that determines what each adversary hopes to gain from attacks and what each adversary values" (Carlin and Graff, 2018, p. 400).



© 2019 The SANS Institute Author retains full rights.

# References

Alon, N. (2018). Operational challenges in ground operations in urban areas: an IDF perspective. *Vanderbilt Univ. Journal of Transnat'l Law*, *51*(3). Retrieved from https://wp0.vanderbilt.edu/jotl/2018/05/operational-challenges-in-ground-operations-in-urban-areas-an-idf-perspective/ Archived at https://perma.cc/BAJ3-BSAL

*Background_facts*. (*n.d*.). Available from author at https://sites.google.com/a/matkowsky.com/background_facts/ Archived at https://perma.cc/AJ35-6CDS

Carlin, J.P. with Graff, G.M. (2019) *Dawn of the code war : America's battle against Russia, China, and the rising global cyber threat* (Kindle Ed.). New York : PublicAffairs.

Chesney, R. (2019, May 9). Crossing a cyber rubicon? overreactions to the IDF's strike on the Hamas cyber facility [Web log post]. Retrieved from https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility Archived at https://perma.cc/4QSX-4KTS

Cronk, T.M., U.S. Dep't of Defense. (2015, Aug. 28). Iraq progresses in ISIL fight, key extremist confirmed dead [Web log post]. Retrieved from https://dod.defense.gov/News/Article/Article/615305/iraq-progresses-in-isil-fight-key-extremist-confirmed-dead/ Archived at https://perma.cc/6GRN-PS49

Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18



© 2019 The SANS Institute Author retains full rights.

Oct. 1907 (Hague Regulations) Retrieved from https://ihl-databases.icrc.org/ihl/INTRO/195 Archived at https://perma.cc/SN6T-8BGU

Convention (IV) Relative to the Protection of Civilian Persons in Time of War. Geneva, 12 Aug. 1949 (Fourth Geneva Convention) Retrieved from https://ihl-databases.icrc.org/ihl/385ec082b509e76c41256739003e636d/6756482d86146898c125641e004aa3c5 Archived at https://perma.cc/5YXC-KZR7

Corn, G.S., Hansen, V., Jackson, R., Jenks, M.C., Jensen, E.T., & Schoettler, J.A. (2019). Air, space & cyberwarfare. In *The law of armed conflict:an operational approach* (Kindle Ed. 2nd ed., pp. 523-24) (Aspen casebook series). NY: Wolters Kluwer.

Diamond, J., Starr, B., & Sullivan, K. (2019, June 21). Trump says US was 'cocked and loaded' to strike Iran before he pulled back. *CNN*. Retrieved from https://www.cnn.com/2019/06/21/politics/trump-military-strikes-iran/index.html Archived at https://perma.cc/NTL8-KULM

Dinstein, Y. (2016). *The Conduct of Hostilities under the Law of Int'l Armed Conflict* [Kindle] (3rd ed.). UK: Cambridge Univ. Press.

Dinstein, Y. (2019). *The International Law of Belligerent Occupation* [Kindle] (2nd ed.). doi:10.1017/9781108671477

Foreign & Commonwealth Office & The Rt Hon Jeremy Hunt MP. (2019, March 7). *Deterrence in the cyber age: foreign secretary's speech*. Retrieved from https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary Archived at https://perma.cc/627X-7PLC

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

Gaggioli, Gloria, ed. (2013*). The use of force in armed conflicts: interplay between the conduct of hostilities and law enforcement paradigms.* Expert Meeting, Report. Geneva: ICRC (ICRC Report). Retrieved from https://www.icrc.org/en/doc/assets/files/publications/icrc-002-4171.pdf Archived at https://perma.cc/TXZ3-AF5Z

Gross, J. A. (2017, Jan. 11). IDF: Hamas hacked soldiers' phones by posing as pretty girls. *The Times of Israel*. Retrieved from https://www.timesofisrael.com/idf-hamas-hacked-soldiers-phones-by-posing-as-pretty-girls/ Archived at https://perma.cc/4A3Q-6BPQ

Gross, J. A. (2018, Aug. 10). IDF: Hamas tries to hack Israelis with fake rocket warning app. *The Times of Israel*. Retrieved from https://www.timesofisrael.com/hamas-tries-to-hack-israelis-with-fake-rocket-warning-app/ Archived at https://perma.cc/NQ73-TSJD

Gross, J. A. (2019, May 5). IDF says it thwarted a Hamas cyber attack during weekend battle. *The Times of Israel* (2019a). Retrieved from https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/ Archived at https://perma.cc/7YDS-H8P6

Gross, J. A. (2019, May 15). Israeli-broadcaster-points-to-Hamas-as-perpetrator-of-eurovision-broadcast-hack. *The Times of Israel* (2019b). Retrieved from https://www.timesofisrael.com/israeli-broadcaster-points-to-hamas-as-perpetrator-of-eurovision-broadcast-hack/ Archived at https://perma.cc/WN83-LA3X

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

Hamid, N.N. (2018). The British hacker who became the Islamic state's chief terror cybercoach: a profile of Junaid Hussain. (2018). *CTC Sentinel*, 11(4). Retrieved from https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/ Archived at https://perma.cc/SR7X-2HF4

HCJ 769/02 *Public Comm. Against Torture in Israel v. Gov't of Israel*, Dec. 13, 2006 (Isr.) (Targeted Killings), English tr. available at https://casebook.icrc.org/case-study/israel-targeted-killings-case Archived at https://perma.cc/A92L-QZ8T

HCJ 3003/18, 3250/18, *Yesh Din v. IDF Chief of Staff* (Isr.) (Yesh Din), English tr. available at https://supreme.court.gov.il/sites/en/Pages/FullCase.aspx?&CaseYear=2018&CaseNumber=3003 Archived at https://perma.cc/8KL5-DMK4

Henderson, I. & Reece K., "Proportionality under Int'l Humanitarian Law: The Reasonable Military Commander Standard and Reverberating Effects" (2018) 51 Vand. J. Trans. L. 836. Retrieved from https://cdn.vanderbilt.edu/vu-wp0/wp-content/uploads/sites/78/2018/06/07015455/11.-HendersonReece_Final-Review_Formatted.pdf Archived at https://perma.cc/U9HZ-Y4A9

ICRC (2019). Practice relating to rule 8. definition of military objectives (ICRC). Retrieved from Int'l Humanitarian Law Database, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule8 Archived at https://perma.cc/R8Y2-Q8GQ

Israeli Defense Forces (IDF). (*n.d.*). About the MAG corps. Retrieved from https://www.idf.il/en/minisites/military-advocate-generals-corps/about-the-mag-corps/ (IDF Website) Archived at https://perma.cc/G2NR-9LKV

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

IDF Spokesperson's Unit (Foreign Press Branch). (2019, May 5). Thwarted Hamas cyber activity (IDF Statement). Retrieved from https://app.activetrail.com/S/eiwixdzxwxd.htm Archived at https://perma.cc/J5AT-HRGM

IDF (May 5, 2019). PRECISION STRIKE…Iran will need to find a new money man in Gaza. [Twitter post] (Target Tweet). Retrieved from https://twitter.com/idf/status/1125081985578409989 Archived at https://perma.cc/7PCC-VA6R

IDF (2019, May 7). 48 hours of terror from Gaza [Web log post] (48 Hr. Update). Retrieved from https://www.idf.il/en/articles/hamas/48-hours-of-terror-from-gaza/ Archived at https://perma.cc/E4V4-RWTH

Int'l Law Commission (ILC), "Identification of customary int'l law The role of decisions of national courts in the case law of int'l courts and tribunals of a universal character for the purpose of the determination of customary int'l law," Memorandum by the Secretariat, 68th session (2 May-10 June and 4 July-12 Aug. 2016), United Nations A /CN.4/69 1* General Assembly Distr.: General 9 Feb. 2016) (ILC Memo) Retrieved from http://legal.un.org/ilc/dtSearch/Search_Forms/dtSearch.html Archived at https://perma.cc/ND7W-CBCA

ILC, "Draft conclusions on identification of customary int'l law and commentaries thereto," Report of the Int'l Law Commission, 70th Session (30 Apr.-1 June and 2 July-10 Aug. 2018), U.N. Doc. A/73/10 (2018) (ILC Draft) Retrieved from



© 2019 The SANS Institute Author retains full rights.

http://legal.un.org/ilc/dtSearch/Search_Forms/dtSearch.html Archived at https://perma.cc/6VN8-5YYJ

ILC, "Identification of customary int'l law: comments and observations received from governments," Report of the Int'l Law Comm'n, Seventieth Session (30 Apr.-1 June and 2 July-10 Aug. 2018), U.N. A /CN.4/716 General Assembly Distr.: General 14 Feb. 2018 (ILC Comments). Retrieved from http://legal.un.org/ilc/dtSearch/Search_Forms/dtSearch.html Archived at https://perma.cc/N2V3-6ECH

Independent Int'l Comm'n, "Report of the UN Comm'n of Inquiry on the 2018 protests in the OPT," Human Rights Council Fortieth sess'n (18 Mar. 2019), A/HRC/40/CRP.2 (Comm'n Inquiry). Retrieved from https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf Archived at https://perma.cc/3A6G-S4X8

Kilovaty, I. (2019). The Elephant in the Room: Coercion. AJIL Unbound, 113, 87-91. doi:10.1017/aju.2019.10 Retrieved from https://www.cambridge.org/core/journals/american-journal-of-international-law/article/elephant-in-the-room-coercion/341847EAE494AB617E5B5899D8400C63 Archived at https://perma.cc/3AUN-JKWM

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226 (ICJ Nuclear). Retrieved from https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf Archived at https://perma.cc/7NET-PCDT

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute, Author Retains Full Rights

© 2019 The SANS Institute Author retains full rights.

Merriam, J.J. and Schmitt, M.N., "The tyranny of context: Israeli targeting practices in legal perspective", U. Pa J. Int'l L. Vol. 37, No. 1, 2015. Retrieved from https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1905&context=jil Archived at https://perma.cc/STK7-4HZC

Nakashima, E. (2019, Feb. 27). U.S. cyber command operation disrupted internet access of Russian troll factory on day of 2018 midterms. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html? Archived at https://perma.cc/C2X6-W77P

Project of an Int'l Decl. concerning the Laws and Customs of War (Brussels Decl.), Brussels (1874). Retrieved from https://ihl-databases.icrc.org/ihl/INTRO/135 Archived at https://perma.cc/R93X-LGPX

Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I), 8 June 1977. Retrieved from https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=D9E6B6264D7723C3C12563CD002D6CE4 Archived at https://perma.cc/4P7R-5WGK

Robertson, H.B, Jr. (2017). The principle of the military objective in the law of armed conflict. *The Development and Principles of International Humanitarian Law*, *72*, 531-557. doi:10.4324/9781315086767-19

Jonathan Matkowsky, Jonathan-m@riskiq.com

© 2019 The SANS Institute Author retains full rights.

Romanosky, S., & Boudreaux, B. (2019). Private sector attribution of cyber incidents: benefits and risks to the U.S. government. *Rand Nat'l Security Research Div*. Retrieved from https://www.rand.org/pubs/working_papers/WR1267.html Archived at https://perma.cc/6KDQ-M3SJ

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the int'l law applicable to cyber operations*. United Kingdom: Cambridge Univ. Press (Kindle ed.) (TM2)

Shamir-Borer, E. (2018). Fight, forge, and fund: three select issues on targeting of persons. *Journal of Transnational Law*, *51*(3). Retrieved from https://cdn.vanderbilt.edu/vu-wp0/wp-content/uploads/sites/78/2018/06/07024021/18.-Shamir-Borer_Final-Review_Formatted.pdf Archived at https://perma.cc/Z55L-KCU2

Sharvit-Baruch, P., & Neuman, N. (2011). Warning civilians prior to attack under int'l law: theory and practice the law of armed conflict in asymmetric urban armed conflict. *Int'l Law Studies*, *87*(1). Retrieved from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1086&context=ils Archived at https://perma.cc/GRP7-3MYE

Shaw, M. N. (2017). *Int'l Law* [Kindle ed.] (8th ed.). doi:10.1017/9781316979815

Shereshevsky, Y. (2018). Targeting the targeting killings case – int'l lawmaking in domestic contexts. *Michigan Journal of Int'l Law*, *39*(2). Retrieved from https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3150324_code2377032.pdf?abstractid=3098492&mirid=1 Archived at https://perma.cc/FC48-EPQX

State of Israel. (2015, June 14). *The 2014 Gaza conflict: factual and legal aspects*. Retrieved from https://mfa.gov.il/MFA/ForeignPolicy/Issues/Pages/Special-



© 2019 The SANS Institute Author retains full rights.

Report-by-Israel-The-2014-Gaza-Conflict-Factual-and-Legal-Aspects.aspx Archived at https://perma.cc/8MXF-H8SE

Treaties, States parties, and Commentaries - St Petersburg Declaration relating to Explosive Projectiles, 1868. (*n.d.*) (St Petersburg Decl.). Retrieved from https://ihl-databases.icrc.org/ihl/full/declaration1868 Archived at https://perma.cc/H6JW-QKXS

Treaties, States parties, and Commentaries - Brussels Decl. (Brussels Commentary), 1874. (*n.d.*). Retrieved from https://ihl-databases.icrc.org/ihl/INTRO/135

Treaties, States parties, and Commentaries - Additional Protocol (I) to the Geneva Conventions, 1977 - 52 - General protection of civilian objects - Commentary of 1987. (*n.d.*) (Commentary to AP I). Retrieved from https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=5F27276CE1BBB79DC12563CD00434969. Archived at https://perma.cc/9UJF-6WJM



© 2019 The SANS Institute Author retains full rights.