Law and National Security: Selected Issues

Pnina Sharvit Baruch and Anat Kurz, Editors

Memorandum 138

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

Law and National Security:
Selected Issues

Pnina Sharvit Baruch and Anat Kurz, Editors

Law and National Security: Selected Issues

Pnina Sharvit Baruch and Anat Kurz, Editors

Memorandum No. 138 July 2014

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

משפט וביטחון לאומי:
סוגיות נבחרות

פנינה שרביט ברוך וענת קורץ, עורכות

Graphic design: Michal Semo-Kovetz, Yael Bieber
Cover design: Yael Kfir
Printing: Elinir

Institute for National Security Studies (a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556

Tel. +972-3-640-0400
Fax. +972-3-744-7590

E-mail: info@inss.org.il
http://www.inss.org.il

July 2014

ISBN: 978-965-7425-64-0

Table of Contents

Preface

> *When the cannons roar, the muses are silent. But even under the roar of the cannons, the Military Commander must uphold the law. The strength of society in withstanding its enemies is based on its recognition that it is fighting for values that are worth defending. The rule of law is one of those values.*
>
> Israel High Court of Justice Case 168/91
> Morcos v. Minister of Defense

These words, written more than two decades ago by Justice Aharon Barak, former President of the Israeli Supreme Court, underscore the reality that law and national security do not detract from each other but rather complement one another in crucial ways. In democratic societies these concepts have become intertwined.

Legal aspects play an increasingly important role in the international arena and influence inter-state relations, as well as the way states act or are expected to behave. A state that regards itself as a member of the international community must therefore address the legal aspects of its national security policies in order to be prepared for the legal discourse that penetrates the international political sphere. Understanding the legal context will also enable the state to exhaust potential legal measures available to it in the defense of its national security interests.

This compilation of articles seeks to illustrate various aspects of the interface between law and national security in both the domestic and international arenas. Because national security is a broad concept, encompassing many dimensions, the law dealing with security also covers a broad range of topics, as indicated by the selection of articles in this volume.

The publication opens with an article discussing one aspect of the law of armed conflict, namely, the legality of the use of force between states, known

as *jus ad bellum*. Authors Pnina Sharvit Baruch and Brandon Weinstock focus specifically on the legality of the decision to use force against Syria, following the use of chemical weapons against civilians by the Assad regime during the ongoing civil war.

The other main aspect of the law of armed conflict pertains to the legal rules of warfare, namely *jus in bello*, and is addressed in the next three articles in the volume. Robbie Sabel discusses situations where one side to the armed conflict does not comply with the applicable legal framework, focusing specifically on conflicts between a state and a non-state actor. Ido Rosenzweig's article discusses the legal dilemmas regarding the practice of targeted killing in high and low intensity warfare. Ziv Bohrer then discusses the role of the military legal advisor in formulating operative decisions in wartime.

In recent years, cyberspace has emerged not only as the next frontier of technological advancement but also as a growing potential theater of conflict. Awareness of the dangers inherent in this theater is increasing, which naturally gives rise to complex legal questions. Eitan Diamond's article discusses the application of the law of armed conflict to cyber warfare, while Deborah Housen-Couriel analyzes the legal aspects of regulating governance of the internet and the consequences of such regulation as it pertains to security in cyberspace.

Another pressing topic with far reaching economic consequences is the protection of offshore oil and gas drilling platforms in the open sea. In his article, Assaf Harel examines the legal framework applicable to the protection of such platforms in search of adequate defensive measures to possible threats, particularly from terrorist attacks.

An important facet of the interrelation between law and security is the need for courts to strike a balance between the rights of litigants and legitimate security concerns. Galit Raguan's article illustrates one of the increasingly pressing aspects of this subject: the challenge of dealing with evidence that has been classified by the state for reasons of national security.

The range of subjects covered by the articles compiled here is evidence of the wide interplay between law and security: legal decisions are influenced by national security concerns, and security decisions are affected by legal considerations. Decision makers ought to formulate policies that take all relevant aspects into account. The law is one of those aspects, and developing an understanding of the legal framework underlying security issues is

therefore essential. Failure to address the legal dimension is liable to lead to decisions that might have negative political and security repercussions, just as ignoring essential operational aspects would prejudice national security.

It is our hope that the multifaceted examination of the relationship between law and national security presented here, as it applies to states in the domestic and international arenas, will serve to inform our readers about both the specific issues discussed in the articles themselves and, more generally, the way that these two fields have become integrated.

Special thanks go to Adam H. J. Broza for his extensive assistance in editing this volume and helping prepare it for publication.

Pnina Sharvit Baruch and Anat Kurz
June 2014

The Use of Chemical Weapons against the Syrian People: Does It Justify Forceful Intervention?

Pnina Sharvit Baruch and Brandon Weinstock

On August 21, 2013 the Syrian government used chemical weapons against its own civilians, killing over 1,000 in a single attack.[1] Following this horrific incident, some Western states, most notably the United States, contemplated attacking Syria without United Nations Security Council (UNSC) authorization, raising a heated debate among legal experts over the legal basis for such an attack under international law. Ultimately, an intended military campaign was called off at the last minute. Intense diplomatic processes were initiated to prevent the use of force and to begin removing Syria's stockpiles of chemical weapons, leading to the adoption of UNSC Resolution 2118 on September 27, 2013.[2] The resolution mandated, *inter alia*, the expedited disclosure and destruction of all Syrian chemical weapons and determined that in the event of non-compliance, measures will be imposed under Chapter VII of the United Nations Charter. Chapter VII allows for both forceful (Art. 42) and non-forceful (Art. 41) means and measures by the Security Council against a state. According to Resolution 2118, then, the imposition of forceful measures against Syria in the event of non-compliance will require another Security Council resolution. Such a resolution would still be subject to a veto by the permanent members of the Security Council, among them China and Russia, which are likely to continue to block any authorization to use force against Syria. Thus, if no such resolution is adopted in the face of Syrian non-compliance, the option

Pnina Sharvit Baruch is a senior research fellow at the Institute for National Security Studies. Brandon Weinstock is a research assistant at the Institute for National Security Studies.

The authors would like to thank Adam H. J. Broza for his helpful comments.

to use military force by the United States and its allies against Syria may reemerge, reviving the debate over the legality of such an action.

From the beginning of his presidency, President Obama has stated his preference for adhering to international standards, underlining the importance of the United States setting an example for the international community.[3] Hence, while an American decision on whether to use force in Syria is, as in other situations, inevitably based on strategic as well as moral considerations, it is also clearly premised on legal guidelines. Furthermore, the legal aspects to the potential use of force in Syria are relevant to similar dilemmas elsewhere where the use of force might be contemplated.

The legal basis in international law for a military attack against Syria without UNSC authorization is far from clear-cut. Indeed, the Obama administration has refrained from officially stating its position on the legal basis for such an attack. Many scholarly legal opinions seem to conclude that there is no formal legal basis in international law for military intervention in Syria.[4] Others argue that such action is allowed, either based on the concept of humanitarian intervention or on other legal justifications. Still others claim that existing international law – specifically the norms regarding the use of force – does not suit a situation such as that in Syria, and therefore new legal standards should be developed. The following essay analyzes these different positions. It should be noted that the essay focuses solely on the legality of the use of force in the context of Syria's use of chemical weapons against its civilians, and does not address arguments related specifically to the implications of potential Syrian non-compliance with UNSC Resolution 2118.

The Use of Force under the UN Charter

Article 2(4) of the UN Charter sets forth the basic rule on the legality of using force, prohibiting the "threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[5] Accordingly, any use of force against Syria is prohibited unless a valid basis is found in international law. Notably, Article 2(4) not only prohibits the actual use of force but also the "threat" of using force. Therefore, the ensuing analysis bears relevance to the pronouncements made by President Obama as well as other US and non-US officials on the intention to strike Syria, notwithstanding the fact that military force was eventually not employed.

Article 2(4) does not prohibit a state from using force internally (i.e., a state against an organized armed group in that state), nor does it prohibit a request by a state for other states to use force on its territory. Thus, it could be argued that if the Syrian opposition forces had enough effective control over Syria to be legally regarded as the new government (or otherwise satisfy the criteria for such status), they could request other states to assist them in their fight against the "former Assad regime." Under such a circumstance, forcible intervention would not be prohibited under Article 2(4).

In earlier stages of the Syrian conflict, some countries recognized the National Coalition of Syrian Revolutionary and Opposition Forces as the sole legitimate representative of the Syrian people. It is doubtful, however, whether existing or further recognition of the Syrian opposition is anything more than a political act, mainly due to the opposition's apparent lack of cohesiveness, insufficient territorial control over Syria, and inability to govern. As was noted by the United States State Department with regard to Libya:

> International law focuses on the question of recognition, and recognition tends to follow facts on the ground, particularly control over territory. As a general rule, we are reluctant to recognize entities that do not control entire countries because then they are responsible for parts of the country that they don't control, and we're reluctant to derecognize leaders who still control parts of the country because then you're absolving them of responsibility in the areas that they do control.[6]

Furthermore, even explicit *political* recognition of the opposition does not necessarily remove *legal* recognition from the Assad regime, especially given that many states continue to have diplomatic relations with the regime and consider it as the legitimate government.[7] Hence, forcible intervention inside Syria against the Assad regime in support of armed opposition groups would probably be considered as regulated by Article 2(4) of the UN Charter.[8]

Exceptions to the Prohibition on the Use of Force Based on the UN Charter

The UN Charter contains two exceptions to the general prohibition on the use of force. The first is use of force authorized by the Security Council under Chapter VII of the Charter, when "necessary to maintain or restore international peace and security."[9] Examples were the authorizations by

the Security Council to use force against Iraq (1990)[10] and the NATO-led operation in Libya in 2011.[11] To date, however, Russia and China have blocked every attempt of the Security Council to authorize the use of force against Syria, rendering this exception inapplicable.

The second exception is self-defense. Article 51 of the UN Charter reaffirms the "inherent right of individual or collective self-defence if an armed attack occurs."[12] In other words, if a state has been attacked, it has the right to respond with force. The article also recognizes the notion of "collective self-defense," namely the use of force by one or more states that were requested to assist an attacked state to defend itself. At the moment, neither the United States nor any of its allies in the region has been the subject of an armed attack by Syria.[13] The Syrian civilians attacked by their own government do not have the legal right under Article 51 to request forcible intervention in self-defense on their behalf.

The fact that an actual armed attack has not taken place is not the end of the story. It is widely accepted that under certain conditions, the use of force against anticipated attacks is permitted. President Obama seemed to allude to this notion when claiming that "if fighting spills beyond Syria's borders, these [chemical] weapons could threaten allies like Turkey, Jordan, and Israel."[14] According to his statement, the threat is not necessarily limited to the use by Syria of chemical weapons against these states, but also to the threat that they might fall into the hands of terrorist groups that might use them.[15] The common view is that a valid claim of anticipatory self-defense – prior to an actual armed attack – is based on establishing that there is a need to use force in order to thwart an imminent armed attack. The Caroline Affair (1837)[16] is widely regarded as delineating the conditions necessary for anticipatory self-defense, whereby a state must show "necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation."[17] Therefore, to claim anticipatory self-defense, the threat must be concrete and it must be clear that using force is the only viable option.[18] Furthermore, the traditional view of anticipatory self-defense equates "imminence" with "immediacy," meaning that the threat must be immediate in order to justify a preemptive strike. Clearly the potential risk described above does not meet this requirement of the criterion of imminence. There was no immediate threat that Syrian chemical weapons were to be used against neighboring countries, either by Syria itself or by terrorist

organizations – neither when the United States was considering attacking Syria, nor at the present.

There is, nonetheless, a growing understanding that stretches the notion of imminence, whereby preemptive use of force may be justified when failure to act would deprive a state of the ability to defend itself from an attack in the future.[19] In other words, "the potential victim State may take forceful action if the 'window of opportunity' to mount an effective defense is about to close."[20] In the commentary to the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), the concept of the "window of opportunity" is clarified:

> This window may present itself immediately before the attack in question, or, in some cases, long before it occurs. The critical question is not the temporal proximity of the anticipatory defensive action to the prospective armed attack, but whether a failure to act at that moment would reasonably be expected to result in the State being unable to defend itself effectively when that attack actually starts.[21]

The fulfillment of the criteria of this wider interpretation of imminence, however, is likewise questionable with regard to the Syrian situation. At the time the United States was considering an attack, the chemical weapons remained in the hands of the Assad regime and there was no concrete threat that they would be used against US forces or US allies. Nor was there any particular indication that the chemical weapons were about to come under the control of terrorist groups that might use them in such a way.[22] Thus, it seems that the threat described above was neither concrete nor imminent enough to justify the use of preemptive self-defense at the time that the use of force against Syria was being contemplated.

Another argument based on the notion of preemptive self-defense in the Syrian case focuses on the use of force against the general threat of facing chemical weapons in future conflicts. President Obama put forward this rationale, stating:

> If we fail to act, the Assad regime will see no reason to stop using chemical weapons. As the ban against these weapons erodes, other tyrants will have no reason to think twice about acquiring poison gas, and using them. Over time, our troops would again

> face the prospect of chemical warfare on the battlefield. And it could be easier for terrorist organizations to obtain these weapons, and to use them to attack civilians.[23]

This, according to John B. Bellinger III, former Legal Advisor for the US State Department under President George W. Bush, could provide the basis for preemptive military action under the collective self-defense regime. Bellinger suggests that because the Syrian regime used chemical weapons against its own people, this triggers the right to use collective self-defense to maintain international peace and security in the name of deterring future incidents of chemical weapons use.[24] However, this argument does not seem to be based on the existing customary legal regime applicable to the notion of self-defense. Rather, the underlying rationale of the notion of preemptive use of force is that force may be used against a state only when there is a threat that the state will carry out an armed attack. It cannot serve to justify using force against a state merely to deter that state, let alone other states, from using certain means of warfare in the future.

Humanitarian Intervention

Over the last two decades, legal scholars have debated whether there are other exceptions to the prohibition on the use of force without prior UNSC authorization aside from self-defense. Some suggest the acceptance of an exception of "humanitarian intervention," which justifies the unilateral or multilateral use of force against a state in extreme cases to prevent a humanitarian catastrophe or to stop widespread human rights abuses.[25]

The United Kingdom has long been an ardent advocate of the doctrine of humanitarian intervention and, unlike the United States, publicly stated its view that humanitarian intervention offers the legal justification to use force in Syria, even without Security Council authorization. On August 29, 2013, the British government released a document that states:

> If action in the Security Council is blocked, the UK would still be permitted under international law to take exceptional measures in order to alleviate the scale of the overwhelming humanitarian catastrophe in Syria by deterring and disrupting the further use of chemical weapons by the Syrian regime. Such a legal basis is available, under the doctrine of humanitarian intervention, provided three conditions are met: (1) there is

> convincing evidence…of extreme humanitarian distress on a large scale requiring immediate and urgent relief; (2)…there is no practicable alternative to the use of force if lives are to be saved; and (3) the proposed use of force must be necessary and proportionate…and must be strictly limited in time and scope…All three conditions would clearly be met in this case.[26]

The main precedent cited as the basis for the justification to use force for humanitarian purposes without UNSC authorization is the NATO intervention in Kosovo in 1999. There are different views as to whether or not the intervention in Kosovo has indeed created a general norm of humanitarian intervention. Rather than explicitly outlining the legal justifications for their use of force in Kosovo, various NATO members (including the US) proffered a narrow list of factors (e.g., violations of previous Security Council resolutions, failure to cooperate with the International Criminal Tribunal for the former Yugoslavia, hundreds of thousands of displaced persons, etc.) that, taken together, justified military force to be used in Kosovo notwithstanding the language of the UN Charter. This approach, limiting the use of force to these unique circumstances, is sometimes referred to as the "factors" approach.[27]

Others claim that the NATO intervention in Kosovo actually set a much broader precedent. Sir Daniel Bethlehem, former principal legal advisor of the UK Foreign and Commonwealth office, argues that although most NATO states did not publicly provide legal justifications for intervening, let alone claim humanitarian intervention as the legal basis for doing so, they nonetheless were indeed intervening on that basis.[28] Bethlehem analyzes several legal elements and precedents and concludes that a principle of humanitarian intervention has emerged in customary international law beyond the specific circumstances of the Kosovo precedent.[29] However, this position is not universally accepted. There are many states that contend that humanitarian intervention has not matured into an accepted legal exception to the prohibition on the use of force of Article 2(4).[30] Furthermore, the fact that the United States declined to base its threat to use force against Syria on this rationale, leaving the UK alone in formally asserting this justification, serves as a clear indication of America's reluctance to accept the existence of a norm in international law permitting humanitarian intervention.

The concept of humanitarian intervention is sometimes confused with the notion of the "Responsibility to Protect (R2P)." R2P is a soft-law doctrine[31] that began to develop in the early twenty-first century, was stipulated in the outcome document of the UN World Summit of 2005,[32] and was subsequently adopted by the Security Council.[33] R2P determines that "each individual State has the responsibility to protect its populations from genocide, war crimes, ethnic cleansing and crimes against humanity. This responsibility entails the prevention of such crimes, including their incitement, through appropriate and necessary means."[34] In the event that a state does not offer such protection, or is in fact the perpetrator of such violence, the international community has the obligation to intervene to put an end to the atrocities being committed, using either peaceful or military means.[35] This doctrine is widely accepted as justifying a decision by the Security Council to authorize the use of force. It is highly doubtful, however, whether the R2P doctrine can serve as a legal basis to allow for humanitarian intervention without Security Council authorization.

One of the problems of relying on the doctrine of humanitarian intervention in the Syrian context is that if this was indeed the rationale for intervening, then the thrust of the operation should be on relieving the humanitarian crisis in Syria. According to the aforementioned official statement of the British government, however, the United Kingdom did not appear to be basing its legal justification to forcibly intervene in Syria on the widespread violence against Syrian civilians per se. Rather, in a somewhat contradictory manner, it limited its focus to the suffering caused only by the use of chemical weapons that, while deplorable, has caused far fewer fatalities than those caused by conventional weapons.[36] President Obama also clearly focused on deterring Assad from using chemical weapons and not on relieving the suffering of the Syrian population. It is doubtful, therefore, whether military action in Syria that is solely intended as deterrence against the future use of chemical weapons adequately fulfills the factual basis for a claim of humanitarian intervention.

Using Force in Response to the Unlawful Use of Chemical Weapons?

In the draft legislation submitted by the Obama administration to Congress regarding authorization for the use of the US armed forces in connection with the conflict in Syria, the stated rationale of the operation focused on the

unlawful use of chemical weapons. The preamble explains, "The objective of the United States' use of military force in connection with this authorization should be to deter, disrupt, prevent, and degrade the potential for, future uses of chemical weapons or other weapons of mass destruction."[37]

This then raises the question whether the use of force could have been permitted based on the Syrian breach of the prohibition against the use of chemical weapons – a prohibition that is universally accepted as binding customary international law.[38] It has been asserted that using force to enforce this norm is justified because the prohibition against using chemical weapons is considered a *jus cogens* norm, a norm so fundamental in international law that no derogation is permitted.[39] But this position is disputed on the grounds that it contradicts the concept that force cannot be used to enforce international obligations and that any military action taken against Syria under this rationale would thus amount to a forcible reprisal, which is widely accepted as prohibited under international law.[40] Moreover, the undisputed *jus cogens* norm of the prohibition of the use of force is more widely acknowledged than the prohibition regarding chemical weapons.[41]

Break the Law to Remake the Law?

The discussion thus far has looked at the issue from a formal international law perspective, reading the black letter *lex lata.* Some scholars argue, however, that even if the law forbids the use of force in a case such as Syria, using force could still have been justified under a rationale of "illegal but legitimate." As one commentator noted, "Those who argue that international legality is the *sine qua non* for legitimate action in the international arena ignore the fact that there are situations of extreme necessity in both domestic and international law where obeying the strict letter of the law may allow a greater harm to occur."[42] Accordingly, in certain cases, moral considerations or concerns related to existential threats could form a basis to justify an act that violates existing legal norms.[43]

A similar approach to international law looks at the law, or at least to the rules governing the legality of the use of force, as a flexible and pragmatic body of norms that must be interpreted in a way that takes into account changing realities. Such a pragmatic approach to international law also entails, to some extent, disregarding the formal letter of existing law, as in the "illegal but legitimate" approach, but unlike that approach, does not

suggest disregarding the law, but rather applying a flexible interpretation to the relevant norms.[44]

The United States seems to adopt such a position.[45] Harold Koh, the former Legal Advisor for the US State Department, outright rejects what he terms "the absolutist approach" with regard to the legal basis for the use of force, namely a formal, rigid, and strict approach to interpreting the rights of states under the UN Charter. According to Koh, "the absolutist position does not acknowledge that the U.N. has multiple purposes – including protecting human rights, promoting regional security, and ending the scourge of war – instead flattening those purposes to a single goal: protecting sovereignty."[46] He argues, rather, that international law is flexible enough, and indeed has come to accept military action based on moral grounds, such as preventing atrocities that result from the deliberate use of chemical weapons.[47] In some respects, Koh's analysis of a potential approach to the use of force in Syria resembles the "factors-based" approach applied in the case of NATO in Kosovo. These factors include "the catastrophic humanitarian situation, the likelihood of future atrocities, the grievous nature of already-committed atrocities that amount to crimes against humanity and grave breaches of the Geneva Conventions, the documented deliberate and indiscriminate use of chemical weapons against civilians in a way that threatens a century-old ban, and the growing likelihood of regional insecurity."[48] Based on Koh's stance and the factors approach regarding Kosovo, it could be argued that if the cumulative circumstances are grave enough, military action could be justified on moral grounds in extreme humanitarian situations and that international law should be interpreted accordingly.

Moreover, applying a flexible and pragmatic approach to international law can lead to the modification of existing law, adapting it to new realities. Indeed, customary international law develops through the combination of state practice (i.e., the way states behave) and *opinio juris*, which is the legal reasoning underlying a state's behavior.[49] Therefore, when a state acts in a way that contradicts existing international law, it may be contributing to the development of a new customary norm that will replace the previous rule. This is the paradox of customary law: "the only way to change it is to break it."[50] Malcolm Shaw, a well-known international law expert, explains in his book that "behaviour contrary to a custom contains within itself the seeds of a new rule and if it is endorsed by other nations, the previous law will disappear and be replaced, or alternatively there could be a period of

time during which the two customs co-exist until one of them is generally accepted."[51] It follows that if forcible action is taken in circumstances such as the Syrian case, and this action is justified as legal and consequently endorsed by other states, a new legal norm might be said to emerge.

One of the main arguments against an approach that permits the use of force that is morally legitimate, despite contradicting formal legal rules, is that it could encourage violating international law at will. Based on their sense of what is moral and legitimate, other states could use force under the pretext of applying flexible interpretations or of creating new rules that reflect their own concept of "pragmatism" and "flexibility." This could lead to an increase in situations in which force is used and ultimately to the collapse of the entire legal prohibition on the use of force between states.[52]

On the other hand, strictly maintaining and applying a formal and narrow legal approach to the use of force arguably falls short of adequately addressing emerging threats, such as the use of weapons of mass destruction. In this context, a comment by Rosalyn Higgins, a former judge in the International Court of Justice, is noteworthy:

> If international law was just "rules," then international law would indeed be unable to contribute to, and cope with, a changing political world. To rely merely on accumulated past decisions (rules) when the context in which they were articulated has changed – and indeed when their content is often unclear – is to ensure that international law will not be able to contribute to today's problems and, further, that it will be disobeyed for that reason.[53]

Conclusion

An international legal basis for striking Syria in response to its use of chemical weapons against its civilians, without Security Council authorization, is far from clear. One possible legal justification may have been to apply the doctrine of humanitarian intervention, yet relying on this doctrine is controversial. Moreover, the military strikes contemplated by the Obama administration and the justification for intervention by the United Kingdom appear to have only been a deterrent for further chemical weapons use, rather than having been designed to end the humanitarian catastrophe that has already claimed over 100,000 lives. This has the effect of undermining,

at least to a certain degree, the fundamental basis of applying the doctrine of humanitarian intervention.

Alternatively, an attack against Syria based on the extreme suffering of civilians and on the deplorable use of chemical weapons could have been carried out without regard to the formal rules of international law, relying instead on moral and ethical arguments and on a flexible approach to the law. Applying a flexible interpretation to the law could also lead to the creation of new norms since international law develops through both the practice of states and the way they legally justify their actions (*opinio juris*). It is therefore unfortunate that the United States has to date refrained from presenting an official position on the legal justification for an attack in Syria (including on the legal basis for a future attack in case of non-compliance with Resolution 2118). Because the United States has not provided the requisite *opinio juris*, the possibility of further developing a rule into customary international law is hindered.

The approach calling for the flexible application of the rules on the use of force raises serious counter claims that if the United States and its allies are willing to disregard the existing law, then other states may use the same justification to use force in the future, risking the erosion of an already fragile international legal structure. On the other hand, accepting the notion that international law, based on a narrow and strict interpretation of the UN Charter, blocks states from using force in situations where logic, ethics, and moral considerations demand the use of force, could eventually lead to the frustration of the fundamental goal of the Charter: maintaining international peace and security.

Ultimately, the broad discussion regarding the legal basis of striking Syria, as well as the legal justifications provided, reflects a significant debate in international law dealing with the legality of the use of force. This debate consists of two opposing positions: those who believe that the law should be stringently adhered to lest the collapse of the entire legal structure becomes at risk; and those who believe that such a rigid interpretation of the law, allowing for immoral or illogical consequences, would ultimately result in the law being disregarded and hence lead to such a collapse anyway. While both positions hold merit, the latter is more persuasive and thus a flexible approach to international law governing the use of force is not only preferable, but also required.

Notes

1 Joby Warrick, *More than 1,400 killed in Syrian chemical weapons attack, U.S. says*, The Washington Post, August 30th, 2013, http://articles.washingtonpost.com/2013-08-30/world/41606663_1_obama-administration-u-s-intelligence-analysts-syrian-government; Sam Dagher, Farnaz Fassihi, Adam Entous, *U.S. Suspects Syria Used Gas*, The Wall Street Journal, August 21st, 2013, http://online.wsj.com/news/articles/SB10001424127887324165204579026123332790830.

2 S.C. Res. 2118, U.N. Doc. S/RES/2118 (Sep. 27, 2013).

3 See, for example, President Obama's Nobel Prize address: "To begin with, I believe that all nations – strong and weak alike – must adhere to standards that govern the use of force. I – like any head of state – reserve the right to act unilaterally if necessary to defend my nation. Nevertheless, I am convinced that adhering to standards, international standards, strengthens those who do, and isolates and weakens those who don't." (President Barack Obama, *A Just and Lasting Peace*, Nobel Lecture (Dec. 10, 2009)).

4 See, for example, the following: Julian Ku, *Would Syria's Use of Chemical Weapons Change the Legality of U.S. Intervention?*, Opinio Juris, December 7th, 2012; Deborah Pearlstein, *So Was Congress Thinking of Authorizing Force in Syria?*, Opinio Juris, April 26th, 2013; John Quigley, *Syria Insta-Symposium: John Quigley on Intervention*, Opinio Juris, August 31st, 2013; Shane Darcy, *Military force against Syria would be a reprisal rather than humanitarian intervention, but that doesn't make it any more lawful*, Blog of the European Journal of International Law, September 1st, 2013); Oona A. Hathaway and Scott J. Shapiro, *Authorization for action in Syria*, The Washington Post, August 28th, 2013; Carsten Stahn, *On 'Humanitarian Intervention', 'Lawmaking' Moments and What the 'Law Ought to Be'–Counseling Caution Against a New 'Affirmative Defense to Art. 2(4)' After Syria*, Opinio Juris, October 8th, 2013, http://opiniojuris.org/2013/10/08/guest-post-humanitarian-intervention-lawmaking-moments-law-counseling-caution-new-affirmative-de/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+opiniojurisfeed+%28Opinio+Juris%29.

5 U.N. Charter Article 2, para. 4.

6 US Senate, Committee on Foreign Relations, Libya and War Powers, Hearing, S. Hrg. 112–189, 28 June 2011, 39 (www.gpo.gov/fdsys or http://www.fas.org/irp/congress/2011_hr/libya.pdf).

7 Dapo Akande, *Self Determination and the Syrian Conflict – Recognition of Syrian Opposition as Sole Legitimate Representative of the Syrian People: What Does this Mean and What Implications Does it Have?*, Blog of the European Journal of International Law, December 6th, 2012, http://www.ejiltalk.org/self-determination-and-the-syrian-conflict-recognition-of-syrian-opposition-as-sole-legitimate-representative-of-the-syrian-people-what-does-this-mean-and-what-implications-does-it-have/.

8 Such intervention might also be considered a violation of the principle of non-intervention; *see* Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.), 1986 I.C.J. 14, 205 (June 27).

9 U.N. Charter Article 42.

10 S.C. Res. 678, U.N. Doc. S/RES/678 (Nov. 29, 1990).

11 S.C. Res. 1973, U.N. Doc S/RES/1973 (Mar. 17, 2011). Interestingly, Russia and China have voiced reservations over the interpretation of this Resolution as authorizing the use of force.
12 U.N. Charter Article 51.
13 There have been minor cross-border incidents, such as stray shelling into the territories of both Turkey and Israel. However, it is questionable whether these amount to an "armed attack" by Syria against these states, and, in any event, these States have not requested US assistance in defending themselves.
14 President Barack Obama, Remarks by the President in Address to the Nation on Syria (September 10, 2013). Daniel Bethlehem points out in this regard that "the recent request by Turkey under the framework of NATO, now agreed, to be provided with Patriot missile batteries to protect against the risk of a Syrian use of chemical weapons, suggests the possibility of a collective self-defence rationale for military intervention to address such a threat." (Daniel Bethlehem, *A Brief Reply on the Legal Bases for Intervention in Syria*, Opinio Juris, December 8th, 2012, http://opiniojuris.org/2012/12/08/a-brief-reply-on-the-legal-bases-for-intervention-in-syria/).
15 The President refers to this possibility, saying that "…it could be easier for terrorist organizations to obtain these weapons, and to use them to attack civilians" (*ibid*.). *See also* Ashley Deeks, *Syria, Chemical Weapons, and Possible U.S. Military Action*, Lawfare, December 10th, 2012.
16 The Caroline incident had its origins in a rebellion against British rule in Canada in 1837. British forces destroyed the steamer Caroline, which was being used to transport men and munitions, while it was in a United States port, killing two people. In a letter of 24 April 1841, United States Secretary of State Daniel Webster insisted that for the raid to have been lawful, the British government had to show a "necessity of self-defence, instant, overwhelming, leaving no choice of means and no moment for deliberation' and that, even if such a necessity existed, 'the act, justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it" (Max Planck Encyclopedia of Public International Law).
17 R.Y. Jennings, *The Caroline and McLeod Cases*, 32 The American Journal of International Law 82, 89 (1938).
18 "We must recognize that there may well be situations in which the imminence of an attack is so clear and the danger so great that defensive action is essential for self-preservation…But we should avoid interpreting the customary law as if it broadly authorized preemptive strikes and anticipatory defense in response to threats." (Oscar Schachter, *The Right of States to Use Armed Force*, 82 Michigan Law Review 1620, 1634 (1984)).
19 Michael Schmitt, *The Syrian Intervention: Assessing the Possible International Law Justifications*, 89 U.S. Naval War College, International Law Studies 744, 744 (2013). For a general analysis see, for example, Sean D. Murphy, *The Doctrine of Preemptive Self-Defense* 50 Villanova Law Review 699, (2005).
20 Schmitt, *ibid*. at 748.
21 Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt, gen. ed., 2013), http://www.ccdcoe.org/249.html.

22 Schmitt, *supra* note 20. *See also* Deeks, *supra* note 16.
23 President Barack Obama, *supra* note 15.
24 John B. Bellinger III, *A Tough Case For Strikes on Syria*, Council on Foreign Relations, September 10th, 2013, http://www.cfr.org/syria/tough-case-strikes-syria/p31375.
25 For a short general analysis of the concept see Malcolm Shaw, International Law (6th ed., 2008) 1155 – 1158.
26 For the official full text, see: https://www.gov.uk/government/publications/chemical-weapon-use-by-syrian-regime-uk-government-legal-position/chemical-weapon-use-by-syrian-regime-uk-government-legal-position-html-version. Eventually the UK Parliament rejected the UK government's request to authorize the use of force in Syria. However this rejection was not based on reference to legal considerations, and therefore does not seem to affect the validity of the legal thesis of the UK government.
27 Deeks, *supra* note 16.
28 Sir Daniel Bethlehem, *Stepping Back a Moment – The Legal Basis in Favour of a Principle of Humanitarian Intervention*, Blog of the European Journal of International Law, September 12th, 2013, http://www.ejiltalk.org/stepping-back-a-moment-the-legal-basis-in-favour-of-a-principle-of-humanitarian-intervention/.
29 Bethlehem, *ibid.* With regard to Syria, Bethlehem submits that beyond the general analysis of the conditions to assert a claim of humanitarian intervention, a full analysis would require consideration of a whole host of other legal issues, including at least: (a) the legal effect of the Security Council's failure to act, (b) the legal effect that attaches to the use of chemical weapons, as distinct from other massive humanitarian violations that have occurred previously; (c) the legal effect of resolutions of the Arab League; (d) the legal effect of the opposition of Russia, China, Iran and others to the suggestion of intervention; and (e) the legal effect of the massive cross-border refugee flows into Turkey, Jordan and elsewhere.
30 See, for example, Dapo Akande, *The Legality of Military Action in Syria: Humanitarian Intervention and Responsibility to Protect*, Blog of the European Journal of International Law, August 28th, 2013, http://www.ejiltalk.org/humanitarian-intervention-responsibility-to-protect-and-the-legality-of-military-action-in-syria/. Akande contends that there is "very little State support for the view that international law permits States to use force extraterritorially on humanitarian grounds." Furthermore, after NATO's intervention in Kosovo, the G77 (composed of 133 member States of the UN) declared their rejection of "the so-called 'right' of humanitarian intervention, which has no legal basis in the United Nations Charter or in the general principles of international law." (Declaration of the South Summit from the Group of 77 South Summit (April 2000), para. 54, http://www.g77.org/summit/Declaration_G77Summit.htm).
31 Soft-law is a term referring to instruments (i.e., resolutions, treaty text not in force, international reports, etc.) and norms that "all share a certain proximity to law and have a certain legal relevance, but at the same time they are not legally binding per se as a matter of law." (Max Planck Encyclopedia of Public International Law).
32 2005 World Summit Outcome, G.A. Res. 60/1, U.N. Doc. A/RES/60/1 (Sept. 16, 2005).

33 S.C. Res. 1674, U.N. Doc. S/RES/1674 (Apr. 28, 2006).
34 2005 World Summit Outcome, *supra* note 33, para.138.
35 The operative paragraph of the World Summit Outcome document states: "The international community, through the United Nations, also has the responsibility to use appropriate diplomatic, humanitarian and other peaceful means, in accordance with Chapters VI and VIII of the Charter, to help protect populations from genocide, war crimes, ethnic cleansing and crimes against humanity. In this context, we are prepared to take collective action, in a timely and decisive manner, through the Security Council, in accordance with the Charter, including Chapter VII, on a case-by-case basis…" (2005 World Summit Outcome, *ibid.* at para. 139).
36 Bethlehem, *supra* note 29. Bethlehem, who acknowledges that humanitarian intervention could potentially serve as a legal basis to attack Syria, cautions that "[w]hether any intervention on humanitarian grounds would ultimately be assessed to be lawful would also be heavily contingent on the facts (including the soundness of the evidence relied upon) and the appreciations of the proper purpose of any such action and likelihood that such a purpose would be achieved."
37 Text of draft legislation regarding Authorization for Use of United States Armed Forces in connection with the conflict in Syria, http://www.whitehouse.gov/sites/default/files/docs/aumfresolutiontext.pdf.
38 This prohibition also appears in the 1993 Chemical Weapons Convention (CWC) but Syria was not, at the time of the attack on August 21, 2013, a party to this convention (Syria ratified the CWC on September 14, 2013). In addition, Syria was bound by the 1925 *Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare* that prohibits the use of such methods of warfare in international armed conflicts.
39 Kenneth Anderson, *Legality of Intervention in Syria in Response to Chemical Weapon Attacks*, American Society of International Law, August 30th, 2013, http://www.asil.org/insights/volume/17/issue/21/legality-intervention-syria-response-chemical-weapon-attacks.
40 Anderson, *ibid. See also* Carsten Stahn, *Syria and the Semantics of Intervention, Aggression and Punishment*, Blog of the European Journal of International Law, September 19th, 2013, http://www.ejiltalk.org/syria-and-the-semantics-of-intervention-aggression-and-punishment/.
41 Anderson, *supra* note 40.
42 Michael Ignatieff, *How to Save the Syrians*, The New York Review of Books, September 13th, 2013.
43 Anderson, *supra* note 40. See also Jack Goldsmith, *More on the UN Charter, Syria, and "Illegal but Legitimate"*, Lawfare, September 5th, 2013, http://www.lawfareblog.com/2013/09/more-on-the-un-charter-syria-and-illegal-but-legitimate/.
44 Kenneth Anderson, *Five Fundamental International Law Approaches to the Legality of a Syria Intervention*, Lawfare, September 5th, 2013, http://www.lawfareblog.com/2013/09/five-fundamental-international-law-approaches-to-the-legality-of-a-syria-intervention/.
45 Anderson, *supra* note 40, writing that "(t)he United States by and large adopts a pragmatic view of international law, and this provides perhaps the best, or at least most plausible, argument in favor of intervention to address violations of the

norm against chemical weapons use by the Assad regime. The argument is that the United States acts to defend a norm that, while lacking formal expression in a strictly legalistic sense, has long endured as a profound humanitarian constraint."

46 Harold Koh, *Syria and the Law of Humanitarian Intervention (Part III – A Reply)*, Just Security, October 10th, 2013, http://justsecurity.org/2013/10/10/syria-law-humanitarian-intervention-part-iii-reply/.

47 Harold Koh, *Syria and the Law of Humanitarian Intervention (Part II: International Law and the Way Forward)*, Just Security, October 2nd, 2013, http://justsecurity.org/2013/10/02/koh-syria-part2/; *see also* Jens Iverson, *Guest Post: The New Haven School on Syria–Observing Professors Koh and Stahn*, Opinio Juris, October 16th, 2013, http://opiniojuris.org/2013/10/16/jens-iverson-guest-post-new-haven-school-syria-observing-professors-koh-stahn/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+opiniojurisfeed+%28Opinio+Juris%29.

48 Koh, *ibid*.

49 Professor Malcolm Shaw (*supra* note 26) explains that "…the substance of customary law must be looked for primarily in the actual practice and *opinio juris* of states" (at 74). With regard to state practice, Shaw notes that "[t]here are a number of points to be considered concerning the nature of a particular practice by states, including its duration, consistency, repetition and generality." (*ibid.,* 76) And *opinio juris,* focuses on "how the state views its own behavior." As he explains, "The *opinio juris* or belief that a state activity is legally obligatory, is the factor which turns the usage into a custom and renders it part of the rules of international law. To put it slightly differently, states will behave a certain way because they are convinced it is binding upon them to do so." (*ibid.*, 84). In this context, also see Akande, *supra* note 31. Akande explains that this is why for the UK to see its vision of international law on humanitarian intervention established, it has to insist that that vision is already established. This is what the *opinio juris* aspect of custom requires.

50 Akande, *supra* note 31.

51 Shaw, *supra* note 26, 91.

52 For detailed criticism on the approach of Koh, see Carsten Stahn, *On 'Humanitarian Intervention', 'Lawmaking' Moments and What the 'Law Ought to Be'–Counseling Caution Against a New 'Affirmative Defense to Art. 2(4)' After Syria*, Opinio Juris, October 8th, 2013, http://opiniojuris.org/2013/10/08/guest-post-humanitarian-intervention-lawmaking-moments-law-counseling-caution-new-affirmative-de/. For a comparative analysis of the positions of Koh and Stahn, see Iverson, *supra* note 47.

53 Rosalyn Higgins, Problems and Process: International Law and How We Use It 3 (1994).

Reciprocity in the War against Terrorism?

Robbie Sabel

Reciprocity is an accepted aspect of the laws of treaties and a recognized element of state responsibility. "No state is obliged by customary international law to remain passive when another state takes action inimical to its legally protected interests."[1] Countermeasures are likewise a recognized act of enforcement in international law, and the International Law Commission draft on the subject reads:

> The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State.[2]

A material breach of a treaty by one party even enables the other party to "invoke it as a ground for suspending the operation of the treaty in whole or in part."[3]

One of the much admired aspects of the law of armed conflict, or modern international humanitarian law applicable in armed conflict (IHL), however, is that it lacks any such aspect of reciprocity.[4] Soldiers are taught that the legal obligations of IHL are binding even if the other party to the conflict grossly violates them. The principle behind this rule is that even if the enemy were, for instance, to commit genocide or conduct bestial acts against innocent civilians, such behavior would not justify similar reciprocal behavior by the opposing state. The rationale behind the rule of denying reciprocity is to increase civilian protection in armed conflict, and the rule receives further support from the increasing tendency to blur the distinction between IHL

Robbie Sabel is a Professor of International Law at the Hebrew University of Jerusalem Faculty of Law.

and the human rights law. It is universally accepted that human rights norms are absolute and reciprocity is irrelevant. People are entitled to such rights by virtue of their humanity and not by virtue of reciprocity, state behavior, the existence of an international element, or even state recognition of such rights. However, it is worth questioning whether this lofty principle of the absence of reciprocity has in fact contributed to the protection of civilians in armed conflict.

Traditionally, one of the factors motivating armed forces to comply with IHL has been the element of reciprocity, both in its positive and negative sense. Positive, for example, because decent and correct treatment of enemy civilians, the wounded, and POWs is likely to encourage the enemy to behave in a similar fashion. Negative in the sense that if, for example, one side to the conflict executes POWs, the likelihood increases that its own soldiers will not receive a high standard of treatment should they be captured.

The question of reciprocity becomes particularly salient in an armed conflict where a regular army, complying with the laws of war, confronts irregular fighters who deliberately attack civilians, a scenario that often prompts a blending of IHL and human rights law. However, a disturbing result of this merger is that international human rights organizations tend at times to presume automatically that any civilian death caused by a regular army in an armed conflict is a violation of IHL, while simultaneously attributing (and thus implicitly excusing) civilian deaths caused by irregular forces to inferior weapons or the exigencies of power asymmetry vis-à-vis their better-equipped and more organized state adversary. Similarly, it is often claimed that it is legitimate for irregular forces to attack the "soft underbelly" of their enemy, namely civilians. The effect that merging of human rights law with IHL has in this phenomena is the presumption against the state's right to use force (which is very limited under human rights law), and an intuitive (but false) sense that states are subject to more stringent rules.

At the same time, there is little utility in analyzing what rules of international law are applicable to terrorist groups, although this issue is debated much in academic journals. The very raison d'être of armed groups using terror tactics is to achieve their political aims by means that flout norms of law and humanitarian behavior. It is highly unlikely that the late Osama Bin Laden or his colleagues consulted legal textbooks on international law prior to engaging in their nefarious activities.

Thus the question remains as to what legal measures states can use to deter acts of terrorism.[5] The UN General Assembly has declared that acts of terrorism "are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them."[6] Over the years, the international legal community has created an impressive network of treaties that require states to prosecute or extradite persons who have committed acts of terrorism. The reality, however, is that there has been a dearth of actual prosecutions. By its nature, the International Criminal Court can deal with very few cases and thus exerts only limited effect and influence. The increasing reliance on the principle of universal jurisdiction seems to have been used mainly as a political tool to demonize Israel and the US, rather than to prosecute individuals from groups that deliberately target civilians.

Democratic states are faced with the question of what measures of enforcement can be legally applied against irregular forces that deliberately target civilians. Such forces exploit the fact that the regular army of a democratic state will comply with the law of armed conflict. The UN Security Council has recognized that in addition to criminal prosecutions, states have a right of self-defense against terrorism – a right that includes the use of armed force.[7] The International Court of Justice gave its opinion that a right of self-defense exists only if the attack comes from the territory of another state. There has, however, been strident academic criticism of this legal opinion, and it is reasonable to assume that a right of self-defense exists against terrorist attacks even if the attack does not emanate from a foreign state. At what point the right of self-defense kicks in would seem to be dependent on the scale and intensity of the hostilities.

Assuming that a state is involved in armed conflict with an armed group that deliberately attacks civilians, the question then arises as to whether that state can take countermeasures that would otherwise be illegal in order to prevent further attacks against its civilians. It can be argued that the laws of war are inadequate when they attempt to address a situation where one party, which is a regular army, implements the laws of war while the other party, which is not a regular army, deliberately acts against the laws of war and bases its military tactics on the exploitation of the fact that the state adversary facing it abides by this legal framework. International law, and in particular IHL, has very limited means of enforcement, and the desire

for mutuality is one of the elements that motivates hostile parties to respect the law of armed conflict.

Countermeasures in armed conflict, which are commonly referred to as "reprisals" or "belligerent reprisals," have been defined as:

> Acts of retaliation in the form of conduct which would otherwise be unlawful, resorted to by one belligerent against enemy personnel or property for acts of warfare committed by the other belligerent in violation of the laws of war, for the purpose of enforcing future compliance with the recognized rules of civilized warfare.[8]

It has been argued that it was the fear of reprisals in kind that led the Axis States to refrain from using poison gas during the Second World War. By way of another example, the Third Geneva Convention requires the release of all prisoners at the end of "active hostilities."[9] The language of the Convention does not authorize states to demand reciprocity with regard to the release of prisoners, yet common sense dictates reciprocity, and indeed that is what happens in practice. The International Committee of the Red Cross (ICRC) has never demanded from one state that it release prisoners except against a reciprocal release by the other party involved.

However, in most circumstances the modern law of armed conflict appears to reject the legality of reprisals. The modern rule, included in the 1977 Protocol to the Geneva Conventions (Protocol I), is that "attacks against the civilian population or civilians by way of reprisals are prohibited."[10] According to the International Criminal Tribunal for the former Yugoslavia, "the bulk of this body of law lays down absolute obligations, namely obligations that are unconditional or in other words not based on reciprocity."[11]

At the same time, the outlawing of reprisals against civilians may not be as clear cut as would appear. The right to carry out acts of reprisal – apart from a number of absolute prohibitions such as the murder of prisoners of war[12] – has been recognized in the past, and was the legal basis to the justification of the air bombardment of German cities by Allied forces during the Second World War.

The 1949 Geneva Conventions did not reject reprisal actions against civilians in enemy territory, and the modern rule quoted above is an innovation.[13] During the debate at the diplomatic conference that drafted Protocol I, some states expressed reservations as to the prohibition on acts of reprisal

against civilian targets. The US representative remarked that "by denying the possibility of a response and not offering any workable substitute, the Protocol is unrealistic and, in that respect, cannot be expected to withstand the test of future armed conflict."[14] One leading academic commentary states that customary and "existing conventional law does not prohibit reprisals against enemy combatants and enemy civilians in territory controlled by the enemy."[15] When the British government ratified Protocol I, it added a reservation stating that the UK retains the right to attack the enemy's civilians or civilian targets in reprisal against such attacks against it, solely in order to force the enemy to cease from such attacks. The reservation adds that such attacks can only be undertaken after the enemy has been warned, and that the decision to carry out an act of reprisal must be made at the highest levels.[16] This reservation is reflected in the order found in the British Army Manual whereby reprisals "may not be undertaken by UK armed forces without prior authorization at the highest level of government," thus clearly not rejecting the actual legality of acts of reprisal.[17] Germany and Italy also added a statement that was similar to the British reservation, though couched in vaguer terms and not in the form of a reservation. The German and Italian statements assert that they retain the right to respond to an attack on civilians with all the means allowed to them by international law.[18] No state sent an objection to the British reservation.

This silence is especially meaningful since during the diplomatic conference, a significant number of states expressed their opinion that the Article promulgating the rule itself regarding the defense of citizens is so important that reservations to it should not be permitted. The International Criminal Tribunal for the former Yugoslavia examined the legality of reprisal acts against civilians and eventually rejected the legality, but commented that, *inter alia*, "the protection of civilians and civilian objects provided by modern international law may cease entirely or be reduced or suspended ... at least according to some authorities, when civilians may legitimately be the object of reprisals."[19] The Tribunal added "that at any rate, even when considered lawful, reprisals are restricted."[20] The Tribunal proceeded to give details of the conditions for permitting acts of reprisal.[21]

It is thus clear that the innovative prohibition against acts of reprisal is not considered a rule of *jus cogens* (a customary rule that is immutable and inalienable and thus not subject to exceptions), and is not considered by some as representing customary law.[22] The ICRC study on the customary

law of war does not contend that the rule prohibiting reprisals has solidified into custom, but rather refers to "the *trend* towards outlawing reprisals."[23] The Tallinn Manual on the International Law Applicable to Cyber Warfare also reaches the conclusion that although certain objects (e.g., medical units) enjoy immunity from being the object of reprisals, no blanket prohibition on reprisals exists.[24] International legal scholar Yoram Dinstein argues that:

> If Contracting State A commits atrocities against the civilian population of Contracting State B, the latter is not allowed to retaliate in kind against the civilian population of State A. But what do the framers of the Protocol expect State B to do? Turn the other cheek? That is a religious tenet rather than a serious military or political proposition. Since the Protocol does not provide State B with any practical alternative response, what is likely to happen is that Article 51, Para. 6 will remain a dead letter and – notwithstanding the paragraph's lucid language – State B will resort to belligerent reprisals against the civilians of State A.[25]

However, cogent arguments can be made against allowing reprisals. A reprisal means deliberately killing civilians not participating in hostilities in order to pressure terrorists and other violators; in other words, reprisals are a form of collective punishment. Frits Kalshoven points out the "dubious efficacy" of such tactics, as terrorist organizations may well be callously indifferent to their own civilian losses, and indeed welcome such losses as part of their "lawfare" against democratic societies.[26] Furthermore, the ICRC recalls that "on the pretext that their own population had been hit by attacks carried out by the adversary, [the Second World War belligerents] went so far, by way of reprisals, as to wage war almost indiscriminately, and this resulted in countless civilian victims."[27] Allowing reprisals against civilians can clearly become a slippery slope, reducing the arguments about legality to "who started it."

Israel has never had a policy of deliberately attacking civilian targets as an act of reprisal, and it is not suggested that this policy should be changed. In one of his rulings former president of the Israel Supreme Court Aharon Barak wrote that "democracies fight wars with one hand tied behind their backs." Israel can be proud of belonging to that small group of states that fights wars with one hand tied behind their backs. Nevertheless, it is worth

examining how far IHL allows vigorous action where terrorists deliberately use civilians as human shields. One avenue that may be explored is to interpret the terms "civilians" and "civilian targets" in a narrower sense than is currently adopted by the ICRC. The destruction of governing executive or financial institutions is likely to yield a distinct military advantage to the attacking party. Clearly, obviously civilian institutions such as health, welfare, or justice institutions are not included here. Ingrid Detter writes that "it is questionable whether government buildings are excluded under any clear rule of law from enemy attack."[28] The ICRC also recognizes that a factory that produces for the civilian market can provide support for a military effort, and therefore, there is a military advantage to be gained by its destruction.[29]

In a draft version presented to the diplomatic conference that drew up the 1977 Protocols to the 1949 Geneva Convention, the ICRC suggested defining civilian targets to include facilities and means of transport that were planned for the civilian population, "except if they are used mainly in support of the military effort."[30] The ICRC definition did not relate to government institutions.[31] The ICRC draft was not accepted and the version that was accepted stated, in the negative, that a civilian object target is not a military target.[32] Protocol I states, "In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used."[33] The list of civilian objects that possess civilian status does not include broadcasting stations, means of transport, or government institutions.[34] An indirect definition of permitted targets appears in the 1954 Hague Convention, concerning the protection of cultural places, that notes that cultural treasures may not be stored near "industrial centers, an aerodrome, broadcasting station, establishment engaged upon work of national defense, a port or railway station of relative importance or a main line of communication."[35] It could be well argued that such objects are legitimate targets, and even if not, they would be legitimate objects for reprisals, thus making a distinction between reprisals against semi-civilian governing bodies and reprisals against civilians and indisputably civilian objects.

Conclusion

Democratic societies must find a way to deter terrorist forces from attacking civilians without adopting the very tactics they are trying to deter. In accordance with customary law, in the past reprisals against civilians were accepted as legal in times of armed conflict, subject to the conditions of being proportional and being used only to force the enemy to desist from attacking one's own civilians. Modern IHL tends to prohibit all reprisals. By their very nature reprisals entail applying collective punishment to innocent civilians, and a policy of reprisals is vulnerable to abuse and is often ineffective.

How else can democratic societies deter attacks against their civilians? The rarely applied possibility of post factum criminal prosecution has not proved itself a sufficient a deterrent. Another avenue could be to exclude executive bodies from the definition of civilians, thus allowing their categorization as legitimate targets, and certainly legitimate objects for reprisals aimed at deterring terrorist attacks against civilians.

Notes

1 Oppenheim's International Law 417 (Sir Robert Jennings & Sir Arthur Watts, eds., 9th ed., Volume I, 1996).
2 International Law Commission, 53rd Session, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Article 22, U.N. Doc. A/56/10 (August 2001).
3 Vienna Convention on the Law of Treaties, Article 60 (2) (b) 1969.
4 Vienna Convention on the Law of Treaties, Article 60 (5) 1969.
5 There is no universally accepted definition of terrorism; however, the U.N. General Assembly has defined terrorism as "criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes." G.A. Res. 51/210, para. 2, U.N. Doc. A/RES/51/210 (December 17, 1996).
6 *Ibid.*
7 *See* Security Council Resolution 1368, U.N. Doc. S/RES/1368 (September 12, 2001) (recognizing the right to self-defense while condemning the terrorist attacks of 9/11/01); Security Council Resolution 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001) (reaffirming the right to self-defense while deciding states should take steps necessary to prevent the financing of terrorism).
8 U.S. Department of the Army, FM 27-10, Department of the Army Field Manual: The Law of Land warfare, para. 497 (1956); *See also* Naulilaa Case (Portugal v. Germany), (Portuguese-German Mixed Arbitral Tribunal, 1928) 8 Trib. Arb. Mixtes 409, 422–25, *reprinted in* 2 R.I.A.A. 1011, 1026.
9 Geneva Convention Relative to the Treatment of Prisoners of War, Article 118, August 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

10 Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Article 51(6), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter First Protocol].
11 Prosecutor v. Kupreškić, Case No. IT-95-16-T, Judgment, para. 517 (International Criminal Tribunal for the Former Yugoslavia, January 14, 2001) (criminal tribunal commenting on humanitarian law).
12 Geneva Convention Relative to the Treatment of Prisoners of War, Article 2, July 27, 1929, 47 Stat. 2021, 118 L.N.T.S. 343 ("[Prisoners of war] shall at all times be humanely treated and protected, particularly against acts of violence . . . [and m]easures of reprisal against them are forbidden.).
13 *See* Mark Osiel, The End of Reciprocity, Terror, Torture and the Law of War 36 (2009). Further on in the same page, Osiel writes that, "There may be a difference between ordinary armed conflicts, in which reciprocity enforces legal norms, and extraordinary wars, in which it cannot." He adds that, "The 1949 treaties do not bar reprisal, for instance, against enemy civilians and civilian property unprotected by the Fourth convention."
14 *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts*, 58th plen. mtg, (Vol. VII) U.N. Doc. CDDH/SR58, para. 81 at 294 (Geneva, 1974-1977).
15 Michael Bothe et al., New Rules for Victims of Armed Conflict 312 (1982).
16 *See* Letter from Christopher Hulse, HM Ambassador of the United Kingdom, to the Swiss Government, *available at* http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (providing a correct copy of the letter dated 28 Jan. 1998) [hereinafter UK Declaration to Geneva Protocol I].
17 U.K. Ministry of Defence, Manual of the Law of Armed Conflict 65 (2004).
18 Declaration of the Federal Republic of Germany upon ratification of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Reg. No. A-17512, August 14, 1991, *available at* http://www.icrc.org/ihl.nsf/NORM/3F4D8706B6B7EA40C1256402003FB3C7?OpenDocument ("The Federal Republic of Germany will react against serious and systematic violations of the obligations imposed by Additional Protocol I and in particular its Articles 51 and 52 with all means admissible under international law in order to prevent any further violation."); Declaration of Italy upon ratification of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Reg. No. A-17512, November 20, 1990, *available at* http://www.icrc.org/ihl.nsf/NORM/E2F248CE54CF09B5C1256402003FB443?OpenDocument ("Italy will react to serious and systematic violations by an enemy of the obligations imposed by Additional Protocol I and in particular its Articles 51 and 52 with all means admissible under international law in order to prevent any further violation.").
19 Prosecutor v. Kupreškić, Case No. IT-95-16-T, Judgment, para. 522 (International Criminal Tribunal for the Former Yugoslavia, January 14, 2000), http://www.haguejusticeportal.net/eCache/DEF/6/117.html
20 *Ibid.,* para. 535.
21 *Ibid.*

22 Osiel, *supra* note 13, 55–56; Theodor Meron, *The Humanization of Humanitarian Law,* 94 American Journal of International Law 239, 250 (2000); The Commander's Handbook of Naval Operations, NWP-1-14M, para. 6.2.3.3 (1995), *available at* http://www.lawofwar.org/naval_warfare_publication_N-114M.htm (last visited September 30, 2010) ("The President alone may authorize the taking of a reprisal action by U.S. Forces.").

23 *See* International Committee of the Red Cross, Customary International Humanitarian Law, Vol. I, Rule 145 (Reprisals) (Jean-Marie Henckaerts and Louise Doswald-Beck eds., 2005) (emphasis added), http://www.icrc.org/customary-ihl/eng/docs/v1-rul-rule145 (last visited September 30, 2010) (the online version of the ICRC's Study on Customary International Humanitarian Law, conducted by the ICRC and published by Cambridge University Press in 2005).

24 Tallinn Manual on the International Law Applicable to Cyber Warfare Rule 46, paras.4-5 (Michael N. Schmitt, gen. ed. 2013), http://www.ccdcoe.org/249.html.

25 Yoram Dinstein, *Comments on Protocol I,* 320 International Review of the Red Cross 515 (1997), http://www.icrc.org/web/eng/siteeng0.nsf/html/57JNV5 (last visited Sept. 30, 2010).

26 Frits Kalshoven, Belligerent Reprisals 26 (1971).

27 International Committee of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, commentary to Article 51(6), 626 para. 1982 (Yves Sandoz, Christophe Swinarki & Bruno Zimmerman eds., 1987).

28 Ingrid Detter, The Law of War 294 (2nd ed. 2000).

29 *See* commentary to Article 52(2), 636 para. 2023, *supra* note 27 ("Other establishments or buildings which are dedicated to the production of civilian goods may also be used for the benefit of the army. In this case the object has a dual function and is of value for the civilian population, but also for the military. In such situations the time and place of the attack should be taken into consideration, together with, on the one hand, the military advantage anticipated, and on the other hand, the loss of human life which must expected among the civilian population and the damage which would be caused to civilian objects").

30 *See* commentary to Article 52, 633 para. 2004*, ibid.*

31 *Ibid.* ("Consequently, objects designed for civilian use, such as houses, dwellings, installations and means of transport, and all objects which are not military objectives, shall not be made the object of attack, except if they are used mainly in support of the military effort.").

32 *See* First Protocol, *supra* note 10, Article 52.

33 *Ibid.,* Article 52(3).

34 *See* Articles 53–56 (limiting protection of civilian objects to cultural objects and places of worship; objects related to survival, such as foodstuffs and granaries; the natural environment; and dangerous power supply installations, such as dams and nuclear power plants), *ibid.*

35 *See* Convention for the Protection of Cultural Property in the Event of Armed Conflict Article 8(1), May 14, 1954, 249 U.N.T.S. 240 ("There may be placed under special protection a limited number of refuges intended to shelter movable

cultural property in the event of armed conflict, of centres containing monuments and other immovable cultural property of very great importance, provided that they (a) are situated at an adequate distance from any large industrial centre or from any important military objective constituting a vulnerable point, such as, for example, *an aerodrome, broadcasting station, establishment engaged upon work of national defence, a port or railway station of relative importance or a main line of communication*; (b) are not used for military purposes." (emphasis added)).

Targeted Killings during High and Low Intensity Warfare

Ido Rosenzweig

Introduction

Recent years have seen an increase in targeted killings around the world. This tool, which is reputed to have been developed by Israel, is today one of the major means in the global war on terror. While the common perception is that targeted killings involve an attack against a person from a plane or an unmanned aerial vehicle (UAV), a more expansive definition of this type of attack could include the attack on Osama bin Laden by the United States and the attack on Mahmoud al-Mabhouh, (allegedly) by Israel, in January 2010 in Dubai.

Israel, which brought this modus operandi to the public's attention early in the twenty-first century,[1] was initially widely condemned internationally. Notwithstanding this criticism, other countries and militaries began to make use of this tactic over the years. The extensive use of targeted killings by the United States in recent years as part of its international war on terror has placed the question of this method's legality at the center of the international legal debate, and within the United States, at the center of political-constitutional

---

Ido Rosenzweig is the Chairman and Founder of ALMA - the Association for the Promotion of International Humanitarian Law, and a researcher at the Minerva Center for the Rule of Law Under Extreme Conditions. This paper is based on a presentation "Pillar of Defense & IHL – Targeted Killings, Military Objectives, Proportionality etc." that was presented in the Joint IHL Forum of ALMA and Radzyner School of Law in the Interdisciplinary Center, Herzliya.

The author wishes to thank Keren Michaeli, Adv. Ady Niv, and Prof. Amichai Cohen for their helpful comments to earlier drafts. Responsibility for any errors remains with the author.

discourse (mainly in context of the targeted killings of US citizens in Pakistan and other countries).[2]

This article reviews the legal frameworks that apply to targeted killings during warfare and examines what relevance, if any, the intensity of an armed conflict may have for the application of the targeted killing definition. Focusing on Israel, the article examines the legal frameworks that govern Israel when it carries out targeted killings, examines a number of case studies, and analyzes the results and implications of these instances. To that end it begins by building a framework for the discussion, and defining what constitutes targeted killing and what legal frameworks apply.

General

Targeted killings can be defined in various ways, based on the modus operandi, the identity of the target, the identity of those who perform the action, and the purpose of the action; every possible definition has political, legal, and operational implications. In fact, there is no single definition in any international treaty or state law that defines positively what constitutes targeted killing. The tendency is to examine each case individually and to rely, *inter alia*, on official declarations concerning the use of this tool by the states that employ it. This article uses a definition based on that of Philip Alston, the former UN special rapporteur on extrajudicial, summary, or arbitrary executions, in his report on targeted killings: "A targeted killing is the intentional, premeditated and deliberate use of lethal force, by States or their agents acting under colour of law, or by an organized armed group in armed conflict, against a specific individual who is not in the physical custody of the perpetrator."[3] This definition is not intended to determine the legality of the targeted killing, but only to set the framework for discussion. For the purposes of this definition, there is no significance to the means of attack, which could be carried out long distance (for example, using a plane, helicopter, or UAV), from a medium distance (for example, sniper fire), or from a short distance (pistol fire, knife, and the like).

This definition distinguishes between an attack on an identified target and an anonymous attack. When we refer to an attack on an identified target, this does not necessarily mean that the personal identity of the target is known, but also when that person's operational role is known. Thus, an operation to kill the senior commander in the military wing of a terrorist organization will conform to this definition even if the strike force does not know the

target's name. At the same time, an attack of this kind raises questions about the reliability of the information and the certainty about the target's role. These and other questions are addressed below.

The Legal Framework

Two legal frameworks apply simultaneously to targeted killings: international law and domestic law.

International Law

International law has two frameworks that regulate, *inter alia*, the use of lethal force, whether in combat or on a regular, non-combat basis: international humanitarian law (the law of armed conflict) and international human rights law.

As a rule, international humanitarian law (IHL) applies only during combat. It is intended in part to regulate the use of force by warring parties during armed conflicts and to ensure that protected populations (such as civilians, the wounded, religious figures, and medical personnel) are in fact protected. Without going into the legal discussion in depth, we can note that according to the rules of IHL, although there is a total ban on directly attacking protected civilians, it is permissible to attack a combatant who belongs to enemy forces or a civilian taking direct part in the hostilities, as long as the attack is not expected to cause collateral damage disproportionate to the direct military benefit anticipated.[4]

In the context of targeted killings, IHL poses a number of questions: (a) Is the target legitimate (namely, an enemy combatant or a civilian taking direct part in the hostilities)? (b) Is the attack expected to cause harm to a civilian population or to civilian buildings? (c) If such harm is anticipated, is it proportionate to the direct military advantage that can be expected? If the targeted killing passes these tests, it is in compliance with IHL and it is permissible to carry it out.

It is worth noting that with regard to these tests IHL does not distinguish between an international armed conflict (namely, a "classic" conflict between two or more states) and a non-international armed conflict (for example, a civil war) or a cross-border asymmetric conflict between a state and an organized armed group. Furthermore, IHL is not subject to the various conditions of reciprocity, and therefore the argument that the enemy is violating these rules does not constitute grounds for corresponding violations

or provide any exemptions or allowances whatsoever with respect to the principles of distinction and proportionality noted above. These rules are part of customary international law, and they therefore apply to all regular armies and to guerrilla organizations as well, and violating them may be tantamount to committing a war crime.

International human rights law is a more general framework, which applies with full force in peacetime and to a certain extent in wartime as well. As a rule, international human rights law does not regulate the use of lethal force in combat, but only in cases involving law enforcement and the imposition of law and order (although the rules do not necessarily address the use of force by law enforcement officials only). International human rights law prohibits the arbitrary deprivation of life, and thus severely limits the ability to lawfully use force against an individual. However, the right to life is not absolute, and there are two exceptions that permit infringement of this right. The first exception is the death penalty, under which a person may lose his life on the basis of a punishment prescribed by law, though only after due process. The second exception that permits the use of lethal force is self-defense or protection of the public – and even then, only as a last resort and when the use of alternative, non-lethal means is not feasible.[5] In cases in which lethal force is used under international human rights law, there is a need to examine whether in fact the case was such as to justify active measures and whether, based on the circumstances, there was a possibility of choosing a less lethal approach. When the use of deadly weapons is not consistent with these requirements, in practice, this is an infringement of the target's right to life without due process, which in turn constitutes a flagrant violation of international human rights law.

The interface between IHL and international human rights law is complex, and the transition between them is especially delicate and significant. For example, the law on killing in one framework is not identical to the law on killing in another. As such, killing an enemy combatant in a combat situation (under IHL) does not in and of itself constitute a criminal offense or even grounds for opening an investigation, unless there is suspicion, for example, that the action was accompanied by disproportionate collateral damage or that the target was not a legitimate target at the time of the attack. By contrast, in the framework of human rights law, an action that leads to loss of life must be examined in order to ascertain whether there was, in fact, justification for the use of lethal force for purposes of self-defense.[6] While

international human rights law applies at all times (*lex generalis*), IHL applies only during and in connection with armed conflicts. Furthermore, at the time of its application, IHL has precedence (*lex specialis*) over international human rights law.[7] As noted, this does not mean that human rights law ceases to apply during combat, but that it is the secondary, complementary framework, which covers the angles that IHL does not address. In addition, human rights law serves as an auxiliary interpretative tool in cases where IHL is not sufficiently clear concerning the manner of its implementation.

Accordingly, when the legality of a targeted killing is examined according to international law, the framework in which the action took place (international humanitarian law or international human rights law) must be examined first, since this has numerous implications for the analysis of the action and the manner in which it was performed. Only then can one examine whether the use of lethal force against the target was in accordance with the restrictions set forth in the relevant framework of international law.

Domestic Law

In addition to international law, every state also has domestic laws regulating the use of lethal force in the state itself or by the agents of the state. In many cases – though not always – this is more restrictive than international law. Domestic law can comprise local legislation as well as legal rulings and local custom. In certain cases, international conventions that constitute a kind of domestic law also wield influence (for example, the European Convention on Human Rights).

In Israel, the issue of targeted killings has been examined directly and in-depth by the High Court of Justice (HCJ), in a petition that has been called the "targeted killings case" (HCJ 769/02).[8] According to a judgment written by then-President of the Supreme Court Justice Aharon Barak, targeted killings are not inherently illegal, and they should be examined on a case-by-case basis. However, the Court's determination of this method's legality was based on the assumption that it is used in an international armed conflict, and therefore it is an act of combat to which IHL applies, and not an act of law enforcement or self-defense by the state. In its ruling, the court clarified that the following criteria apply in carrying out a targeted killing: (1) Targeted killings must be preventative and not punitive; they are not meant to address acts committed in the past, but to prevent an attack. (2) The targeted killing must be carried out against a person taking direct

part in the hostilities, that is, not against a protected civilian. (3) The use of targeted killing will be permitted only when there is no less lethal alternative that will not pose an excessive risk to Israeli forces. (4) Disproportionate collateral damage must be avoided. (5) After the attack (*ex post facto*), the collateral damage caused to uninvolved civilians ought to be reviewed by a special objective examination committee to be established for this purpose.

This indicates that according to the HCJ, there are two bases for gauging the legality of targeted killings. First, the targeted killing must be a preventative act of combat against a person who is directly taking part in acts of combat. In other words, the targeted killing must take place within the framework of IHL. In so stating, the HCJ created the main normative framework and the minimum standards for carrying out targeted killings. Furthermore, the court stated that less lethal alternatives should be considered and that any collateral damage should be reviewed. Here, in effect, the Court creates the addition that constitutes the narrower domestic framework and imposes limitations beyond those required by IHL. Such law does not create an obligation to use a less lethal method for attacking combatants or civilians directly taking part in the fighting and does not require that each case of collateral damage be examined. Rather, this obligation is triggered only where there is concern that there has been a violation of the rules of IHL (that is, when there is concern that the collateral damage is not proportionate).

The establishment of a commission to examine targeted killings, along with its mandate to review, does not connote that there is a problem with targeted killings per se (as noted, targeted killings were not rejected by the HCJ). Furthermore, in contrast to the investigations carried out according to the rules of IHL that are based on concerns that a crime has been committed, the commission's review is automatic in any case in which uninvolved civilians have been killed as a result of the attack. According to the Court, the commission has the authority to review targeted killings carried out after publication of the Court's ruling in December 2006, and it is not obligated to review targeted killings retroactively. As a result, one of the most famous targeted killings – that of Salah Shehadeh, head of the military wing of Hamas, in 2002, which was also part of the basis for the petition on targeted killings – is outside the commission's purview.

However, in the Court's deliberation of the petition by Yoav Hess (HCJ 8794/03),[9] which dealt directly with the legality of Shehadeh's killing, the state agreed to the establishment of an external, objective investigatory

commission. In January 2008, the "Special Investigatory Commission to Examine Targeted Killing – Salah Shehadeh" was established. In March 2010, retired justice Tova Strasberg-Cohen was appointed to head the commission, replacing the original chairman, former military advocate general attorney Tzvi Inbar, who died during the commission's term. An analysis of the commission's decision is not the purpose of this article. Suffice it to say that the commission determined that although the collateral damage (thirteen uninvolved civilians, including women and children) was not proportionate to the (great) benefit of Shehadeh's killing, since the damage anticipated at the time the attack was ordered was significantly lower, there was no violation of the rules of international humanitarian law. The commission also addressed the question of a less harmful alternative and determined that the method chosen (a one-ton bomb) was legitimate given the circumstances, and that in light of the conditions on the ground, there was no less-lethal alternative that would not have posed excessive risk to IDF forces.[10]

For clarification, two preliminary conditions must be met in order to initiate the commission's review. The first requirement is that a targeted killing took place, that is, the premeditated and deliberate use of lethal force against an identified target. The second is that the targeted killing resulted in collateral damage to uninvolved civilians. Hence, in cases of "regular" attacks during combat or targeted killings that didn't result in any collateral damage, such operations are not subject to the review of the commission.

The importance and the impact of establishing an independent, objective commission to examine Shehadeh's killing can be seen in the decision of the Spanish court that ruled on a private complaint against senior Israeli officials for their involvement in Shehadeh's killing. According to the Spanish court, since Israel undertook an independent, legitimate investigation, there is no room to implement Spain's universal jurisdiction in the case and it should be dismissed.[11]

Clearly, the legal framework applicable to targeted killings is far from simple. It consists of a number of elements, some of which are intertwined, and some of which contradict each other. Moreover, while there is great importance in understanding the appropriate legal framework for examining targeted killings, this is not enough since, even within each of the various frameworks, there are situations that distinguish themselves from one another.

The Question of Intensity, Proximity, and Control

What follows is a discussion of distinctions among situations that are subject to IHL, and particularly the conditions of the fighting in which the targeted killing takes place.

One of the recurring questions in the context of targeted killings in the framework of IHL is the circumstances in which the killing takes place. Of particular focus is the question of proximity to the armed conflict and the intensity of the conflict. This approach distinguishes between a surgical strike that takes place outside the cycle of combat or during low intensity fighting and targeted killings carried out during high intensity combat or even on the battlefield itself.

Two examples will be cited here. On November 14, 2012, at the outset of Operation Pillar of Defense, Israel killed Ahmed Jabari, head of the military wing of Hamas, by attacking his car from an aircraft.[12] The attack took place during a relatively quiet period in Israel's conflict with Hamas since the outbreak of the second intifada in 2000. On November 18, 2012, during Operation Pillar of Defense (which had reached an especially high level of intensity that day), the IDF targeted Yahia Rabia, head of the Hamas rocket unit. This occurred during one of the most serious escalations in the region in recent years (and certainly since Operation Cast Lead, which took place in December 2008-January 2009).

On the face of it, it might appear that while the targeting of Jabari, which took place during a quiet period, is a clean, classic example of targeted killing, the targeting of Rabia constitutes a regular combat action, and is therefore not subject to the complex legal framework of targeted killings as presented above. However, according to the selected definition of targeted killings – an attack on an identified target – the intensity of the fighting and the circumstances in which the killing takes place have no significance. While they could be very significant in determining the legal framework we use to examine the action and its legality, they do not affect the initial determination of whether this is a targeted killing.

The ruling by the HCJ on targeted killings did not discuss intensity as a relevant criterion for defining a targeted killing. The Court discussed the circumstances, such as the extent of Israeli control in the area (the Gaza Strip) as a criterion that, for example, allows an examination of possible alternative, less lethal measures. However, its decision does not rule out application of the legal frameworks to targeted killings that take place

during high intensity combat, to the extent that they enter the realm of the definition of targeted killing.

Many of the targeted killings in the Israeli context have been carried out in connection with Israel's belligerent occupation of the West Bank. This has led to the mistaken perception that the ruling by the HCJ on the issue of targeted killings applies only to those carried out in the context of belligerent occupation. Nevertheless, in applying Israeli law to Israeli actions, including the ruling on targeted killings, the extent of Israel's control of the territories is not directly relevant. Rather, the significance of the actual level of control is likely to be manifested in the examination of the less lethal alternatives available to the IDF when it decides whether to employ targeted killing. In order to explain this issue, the two cases will be examined more closely.

The targeting of Ahmed Jabari can be examined under the two applicable legal frameworks – IHL and Israeli law. According to IHL, by virtue of his position in the military wing of Hamas, Jabari was *prima facie* a civilian who took a direct part in the hostilities, and therefore constituted a legitimate military target. Since the armed conflict between Israel and Palestinian armed organizations, particularly those in the Gaza Strip, was still ongoing (albeit at low intensity), there was nothing preventing this attack, and the claims against Israel in this context are liable to be against the proportionality of the attack in relation to the collateral damage.

There are allegations that, at the time of the killing, Jabari was actually involved in attempts to promote discussions on a ceasefire with Israel and was not engaged in military activity. Theoretically, such allegations could weaken the legal legitimacy of Jabari's targeted killing by raising doubts about his being a civilian taking direct part in the hostilities at the time of the killing. However, due to his senior position in the military wing of Hamas, which is an organized armed group in all respects, in order for him to benefit from the status of a protected civilian, he would have had to actively and clearly show that he was no longer taking direct part in the hostilities. In this instance, it would appear that this was not the case.

When we take into account the Israeli legal framework established by the HCJ ruling, we must also ascertain that a less lethal alternative was not available. In addition, if the action harmed uninvolved civilians, the action must be examined by the special commission established as a result of the ruling.

In the case of Yahia Rabia as well, it appears that the target was legal and legitimate, according to both IHL and Israeli law. However, here the targeting of Rabia led to collateral damage, harming eleven uninvolved people, including four children and five women.[13] We therefore must also examine the information that was available to the relevant officials at the time the targeted killing was approved, about Rabia's being at the targeted location and the anticipated collateral damage. Under IHL, a situation could arise in which collateral damage is greater than expected, and even disproportionate damage would not be considered a violation. This is because the decision to carry out an attack must be examined *ex post facto* on the basis of the information available prior to the attack (*ex ante*), in accordance with the standard of the "reasonable commander."

However, Israeli law, according to the targeted killing ruling above, indicates that because of the collateral damage – the death of uninvolved civilians – the case must be transferred to the special commission, and no importance is attached to the fact that the action took place during a high intensity conflict, since it was an attack on an identified target.

Conclusion

Two frameworks of international law can be applied to targeted killings: the law of armed conflict (international humanitarian law) and international human rights law. Each has its own guidelines that regulate and restrict the legality of the use of deadly weapons. In addition, every state has its own domestic laws that usually regulate the legality of the use of force, whether during combat or in general.

By definition, targeted killings during combat are different from "regular" killings during combat because they are an attack on a specific, identified target (whether identified personally or on the basis of the operational role). The intensity of the fighting has no significance in defining an action as a targeted killing, and it therefore has no significance in determining the appropriate legal framework.

In addition, according to the ruling on targeted killing by the Israeli HCJ, in every instance of targeted killing in which uninvolved civilians are harmed, whether in the course of a high intensity conflict such as Operation Pillar of Defense or during a long term low intensity armed conflict, Israel has an obligation to transfer the case to the special commission, established to examine the legality of targeted killings, even when the collateral damage

is proportionate and legal. The fact that the targeted killing is reviewed by the commission does not mean it is inherently problematic. On the contrary, there can certainly be situations in which the commission carries out a review and decides that there were no less lethal alternatives that would not have posed an excessive risk to IDF forces. However, the review should start automatically and immediately when there is collateral damage to the civilian population. In the test cases cited above, the commission would of course take into account Israel's lack of control (or limited control) over the Gaza Strip in terms of collecting information, finding possible alternatives, and reducing the collateral damage, and would reach a decision on the action's legality.

In conclusion, even if Israel is to fight "with one hand tied behind its back,"[14] it must have two "clean hands" displayed openly that shed light on any examination of the legality of the actions carried out during the fighting.

Notes

1 Mordechai Kremnitzer, *Is everything kosher when confronting terrorism — on Israeli preventative killing (targeted killing) in Judea, Samaria and Gaza*, Position Paper 60, Israel Democracy Institute, http://www.idi.org.il/media/304725/pp_60.pdf.

2 Joint Letter to President Obama on US Drone Strikes and Targeted Killings (2013), *available at* www.hrw.org/news/2013/04/11/joint-letter-president-obama-us-drone-strikes-and-targeted-killings; Scott Shane, *Targeted Killing Comes to Define War on Terror*, The New York Times, April 7th, 2013, http://www.nytimes.com/2013/04/08/world/targeted-killing-comes-to-define-war-on-terror.html?_r=0; Michael Isikoff, *Justice Department memo reveals legal case for drone strikes on Americans*, NBC News, February 4th, 2013, http://investigations.nbcnews.com/_news/2013/02/04/16843014-justice-department-memo-reveals-legal-case-for-drone-strikes-on-americans?lite; *see* also Hilly Moodrick, *United States Preventative Killing*, *supra* note 1, 47.

3 Philip Alston, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, United Nations Human Rights Council, A/HRC/14/24/Add.6, (May 28, 2010), www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf.

4 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 U.N.T.S. 3 (hereinafter "the First Additional Protocol"), Article 51(5)(b). Israel is not party to the First Additional Protocol, but recognizes that it reflects part of customary international law and thus its application to its conduct. *See* for example the Israel Ministry of Foreign Affairs report following Operation Cast Lead: The Operation in Gaza: Factual and Legal Aspects 44 (2009), http://www.

mfa.gov.il/MFA_Graphics/MFA%20Gallery/Documents/GazaOperation%20w%20Links.pdf.

5 *See* for example United Nations High Commissioner for Human Rights, *General Comment No. 06: the right to life*, http://www.unhchr.ch/tbs/doc.nsf/0/84ab9690ccd81fc7c12563ed0046fae3?Opendocument.

6 Louise Doswald-Beck, The Right to Life in Armed Conflict: Does International Humanitarian Law Provide all the Answers?, 88 International Review of the Red Cross 864 (December 2006).

7 Amichai Cohen and Yuval Shany, *Beyond the Grave Breaches Regime: The Duty to Investigate Alleged Violations of International Law Governing Armed Conflicts,* 14 Yearbook of International Humanitarian Law 37 (2011).

8 Israel High Court of Justice Case 769/02, *Public Committee Against Torture in Israel et al v. the Government of Israel* (2006), available at www.haguejusticeportal.net/Docs/NLP/Israel/Targetted_Killings_Supreme_Court_13-12-2006.pdf.

9 Israel High Court of Justice Case 8794/03, *Yoav Hess et al v. Judge Advocate General* (2008).

10 For an article regarding the commission's decision, *see* N., *The Disproportion in the Shehadeh Commission's Proportionality Test*, Association for the Promotion of International Humanitarian Law, http://www.alma-ihl.org/opeds/the-disproportion-in-the-shehadeh-commission-s-proportionality-test. The commission's report can be found at http://www.pm.gov.il/NR/rdonlyres/DA339745-7D9F-40C7-B20F-4481AAF1F4C7/0/reportshchade.pdf.

11 Ido Rosenzweig and Yuval Shany, *Update on Universal Jurisdiction: Spanish Supreme Court Affirms Decision to Close Inquiry into Targeted Killing of Salah Shehadeh*, 17 Terrorism and Democracy Newsletter (May 2010), http://en.idi.org.il/analysis/terrorism-and-democracy/issue-no-17/update-on-universal-jurisdiction-spanish-supreme-court-affirms-decision-to-close-inquiry-into-targeted-killing-of-salah-shehadeh.

12 A video clip of the operation itself was released to public media, and can be viewed on YouTube at https://www.youtube.com/watch?v=BGQAvmjALdc.

13 Gillie Cohen, *IDF won't open a criminal investigation into the killing of nine family members in Operation Pillar of Defense*, Haaretz, April 13th, 2013, http://www.haaretz.co.il/news/politics/1.1993041.

14 Israel High Court of Justice Case 5100/94, *Public Committee Against Torture in Israel v. The State of Israel et al* (1999).

Lawyers in Warfare: Who Needs Them?

Ziv Bohrer

In recent years, lawyers have become increasingly involved in issues relating to warfare. This manifested itself in both the greater use of legal counsel in real time and in the growth of retroactive enforcement (investigations and prosecutions). The purpose of this article is to respond briefly to some of the criticism of this phenomenon.

"Let the IDF Win"

In Israeli public discourse today it is often said that the increasing involvement of lawyers prevents the IDF from achieving victory. Implicit here is the argument that if in the past lawyers had been as involved as they are today, Israel would not have won the wars it has won thus far.[1] Without denying the fact that there is growing involvement of lawyers and the law in issues concerning warfare, legal involvement in warfare has long been greater than people often think. This is true even in the context that is considered the most damaging to soldiers: criminal prosecution. I will attempt to illustrate this briefly by examining the scope of prosecution during the most difficult war that Israel has experienced thus far: the War of Independence.[2]

On February 10, 1948, even before the establishment of the state, David Ben-Gurion wrote the following to Yaakov Riftin, a member of the Security Committee:[3]

> I have received complaints and serious allegations of revenge and lawlessness among some members of the Palmah: robbing Arabs; murdering Poles[4] and Arabs for no reason or without sufficient reason, and in any case without a trial; unfair actions

Dr. Ziv Bohrer is a faculty member at the Bar-Ilan University Faculty of Law.

> toward Jews; theft; embezzlement of money; torture of Arabs during interrogation; and the like. These acts, if they are true, are a political and moral danger to the organization and to the *yishuv* [the pre-State Jewish community in Palestine] and the harshest measures should be taken to root them out.

Riftin then undertook an examination and subsequently submitted a report to Ben-Gurion that, *inter alia*, raised a number of questions and posited possible answers:[5]

1. How can disturbances be prevented from spreading? How can they be overcome? (a) By increasing educational-informational activities in the organization. (b) By a clear and effective legal procedure.
2. On what do the clarity and the effectiveness of the legal procedure depend? (a) Delivery and receipt of accurate information on crime (b) The possibility of a fast and comprehensive investigation of the complaint (c) Someone to handle the complaint immediately and prosecute if necessary (d) The proper observance of law.

The Riftin report was one of the main factors influencing the establishment of the Military Advocate General (or as it was originally called, the "Legal Service"), which was very active during the War of Independence. The size of Israel's military force in that war was some 70,000 soldiers, and according to a report submitted by Minister of Justice Pinhas Rosen to the Knesset, between July 1, 1948 and June 15, 1949, 2,424 verdicts were handed down by the IDF's Courts-Martial, with seventy-nine of them against officers.[6] In addition, according to a report summarizing the work of the Military Advocate General for 1948, an average of 400 court-martials took place every month.[7] If we assume that not every investigation begun at that time ended in prosecution, we arrive at even more impressive statistics on how often criminal investigations were conducted during the War of Independence. To be sure, it is true that a large number of these legal proceedings did not deal with violations of the laws of war. Furthermore, most of the verdicts that dealt with war crimes (other than those that dealt with pillage) are censored to this day, and therefore it is not possible to know precisely how many prosecutions there were. However, there are various indicators that this was not an insignificant phenomenon[8] – and nonetheless, the war was won.

In other words, there was always a need for relatively extensive legal involvement (including prosecutions) in order to prevent and punish war

crimes, which, as Ben-Gurion put it, "are a political and moral danger" to Israel. Moreover, without denying the increased legal involvement in warfare in recent years, activity of this sort was far from unusual. The underestimation of the scope of legal activity in the past stems in part from the fact that the outcomes of much of this involvement were censored, and thus forgotten.

"In the End, Every Soldier Will Need His Own Personal Lawyer"

Opponents of the growing legal intervention in issues surrounding warfare often say that increasing juridification will lead to a situation in which every soldier needs his own personal lawyer.[9] The implicit argument here is similar to the argument behind the slogan "let the IDF win," i.e., that the growing legal intervention will hurt the effectiveness of the fighting by creating a restraining effect (by making soldiers and commanders fearful about acting and taking the initiative) and a tendency to "see no evil, do no evil" (out of fear of acting and taking the initiative in general, or at least, without obtaining legal advice in advance, which means loss of leadership and harm to the effectiveness and speed of the military response).[10]

There are a number of responses to this argument, and here too the first response is based on history. Those who make use of this slogan assume that today, soldiers and commanders still do not require a personal attorney, and that it is only the growing threat of prosecution (whether by the Israeli justice system or the international community) that is liable to lead to this. However, the sting of this expression is dulled to a large extent when we realize that this claim has been made for many years. The earliest source I located is from 1837, when British officer C. J. Napier wrote a statement to this effect in his book, *Remarks on Military Law and the Punishment of Flogging*.[11] Napier believed that during operational activity (combat and riot-dispersal), the soldier has a duty of absolute obedience to his commander's orders (meaning that he must obey even illegal orders of any kind). He argued that accepting the legal position that there are (illegal) orders that the soldier must refuse to carry out is inappropriate, since

> if this be true, such a principle dissolves the army at once … in such law there is neither sense nor justice. … If such is law, the army must become a deliberative body, and ought to be composed of attorneys, and the Lord Chancellor should be made the commander in chief. [12]

Napier's position was rejected long ago, and although over 175 years have passed since then, the British army remains alive and well.[13] In Israel, the earliest source (known to me) in which this claim is made was during the Kafr Kassem trial.[14] The fact that this expression has such a long pedigree, as well as the fact that it has been used in the past in the context of acts and views that are today perceived as fundamentally unacceptable (i.e., obeying illegal orders to carry out atrocities) indicates that the fear that the day is approaching when a soldier will need a personal lawyer is not justified, and this warning is largely an empty threat.

Nevertheless, there is partial truth in the fear that the increasing involvement of the law could create a chilling effect. Such an effect is a chronic problem in any case in which criminal law is used and enforced. Any law, because it is based on language, is destined to suffer (to one extent or another) from a problem of being overly or insufficiently inclusive.[15] In other words, sometimes, it will prohibit an action in a situation in which most would agree that it is better for the action to be performed, and sometimes it will permit an action to be performed in a situation in which most would agree that it were better not performed. Furthermore, it is as naive to think that completely unambiguous legal rules can be formulated as it is to think that from the outset the law can predict each and every possible situation that may take place.[16] By the same token, it is also naive to think that people (especially those who are not lawyers) will be familiar with every clause of every law.[17] Consequently, people sometimes refrain from performing actions that are perfectly legal for fear of being prosecuted,[18] while at times, individuals break the law without being aware that they are committing a crime.[19]

Precisely given these problems, legal systems attempt to word their laws as clearly as possible.[20] However, such problems have never led legal systems to abandon the use of criminal law[21] because the price is too high. Many times, in the absence of a legal norm accompanied by the threat of prosecution, even good, intelligent, moral people are likely to be tempted to violate core moral precepts. Psychological studies have even shown that the temptation to do so is especially great in times of war, as noted by Muñoz-Rojas and Frésard:[22]

> The perception that there are legal norms is more effective than the acknowledgement of moral requirements in keeping combatants

> out of the spiral of violence … While attempts at justification… can enable combatants to switch off guilt feelings in the face of inhuman acts and to stretch moral values by legitimizing such acts, they cannot confer legality on such behaviour. The norm draws an easily identifiable red line, whereas values represent a broader spectrum which is less focused and more relative.

In addition, the recognition that legislation can never be worded "perfectly"[23] has led modern human societies to actually encourage acquisition of legal knowledge and the use of legal advisors. This encouragement is meant to reduce the uncertainty that the law can create,[24] along with the recognition that many times, without a legal advisor to mention that there is an obligation to obey the law, even good, intelligent, and moral people will be tempted to break it.[25]

As for the fear of a "see no evil, do no evil" tendency, we should distinguish here between two types of concerns: the first is lack of initiative out of a fear of prosecution, and the second is lack of initiative as a result of the over-involvement of lawyers throughout the decision making process. In reality, both types of fear are exaggerated.

Regarding the first type of fear, it is precisely the growth in legal education and the increased involvement of legal advisors in the decision making process in real time that reduces this fear. Thus, for example, Yehuda Meir-Roth, who expressed concern that the increasing use of criminal enforcement could lead to reduced initiative among combatants in the IDF, concluded:[26]

> Since the first intifada, the IDF has been fighting mainly among a dense civilian population, in which the enemy and the uninvolved civilian are very close to each other. These are situations that tend to lead to complications. There is a need to train soldiers to cope in this battlefield. The training must include, among other things, the study of international and criminal law and an analysis of relevant legal precedents. A military lawyer should be permanently attached to any Brigade Staff or Division Staff. His presence on these Staffs is essential in a situation where many military operations are liable to cause criminal or international law-related complications for those who gave the orders and those who carried them out. In other words, there is a need for preventative action. It would be an error to bring a

> military lawyer into the picture only after the incident occurs. Officers should be able to consult in real time with an attorney serving in the Brigade or Division Staff.

As to the concern that commanders will avoid taking the initiative because of real-time involvement by legal advisors, this concern seems to be based on a lack of understanding, both of the nature of the legal advice and the nature of the decision making process in the army. One of the great leaps forward in the development of modern militaries was the establishment of the Staff alongside the commander, which stemmed from an understanding that the commander cannot be an expert in every area of activity that is needed to fulfill the military mission. The role of the commander must be, then, to lead and chart the way on the basis of information provided to him by various experts who are members of the Staff. The existence of the Staff does not harm the leadership status of the commander. On the contrary: it provides the commander with information and tools that allow him to make leadership decisions.[27]

It can be argued that the nature of the relationship between the legal advisor and the commander is different from that between the commander and, say, an artillery officer, because only the legal advisor can tell the commander that he may not perform a particular action and that if he does so, he may be prosecuted. However, this difference is not as great as it appears to be at first glance. First, even an artillery officer will sometimes say to a commander that an action the commander is eager to undertake cannot be carried out, for example, because the necessary ammunition is not available.[28] Second, as anyone who is even minimally familiar with the law knows, legal norms are only rarely phrased in absolutes. Many times, there is a legal gray area where it is not entirely clear whether the action is legally permitted or prohibited, and therefore, the choice of one way rather than another only creates a legal risk (as opposed to a certainty of breaking the law). Furthermore, in many other cases, the law does not prevent or interfere with achieving the result the person seeks (in this case, the commander). Rather, it outlines the different ways in which the desired result can be obtained legally. In these two types of cases (and these represent most cases), there is no concern at all that consulting with a lawyer will harm the commander's status. On the contrary, it provides the commander with a complete picture of the tools available to him and the risks and obstacles he faces.[29]

Perception vs. Legal Reality

"There are elements working to terrorize Israel from this angle [legal warfare]. However, Israel's situation is better than we usually imagine."[30]

Since the 1990s, the international community has undergone a drastic change in mindset regarding the necessity of enforcing the laws of war, and as a consequence, international criminal law has been revived after years of slumber.[31] This revival is manifested primarily in two ways that have ramifications for the Israeli soldier. The first way is the establishment of the International Criminal Court (ICC). Despite the fact that Israel is not party to the treaty under which the ICC was established, under certain circumstances, Israeli officials might find themselves being prosecuted in the ICC.[32] The second way is evidenced by the increasing attempts to bring about the prosecution of Israeli officials in foreign countries by virtue of "universal jurisdiction." According to international law, every country in the world has the authority to prosecute people who are suspected of war crimes, even when the prosecuting state has no connection to the event that led to the suspicion that a crime had been perpetrated. Universal jurisdiction is intended to end impunity for war crimes, and in the past, Israel very much supported the use of this legal doctrine out of a desire to increase the chances that Nazi war criminals will be punished.[33] Since the 1990s, many states have begun to make increasing use of universal jurisdiction. As a result, various Israeli officials have found themselves threatened with prosecution for war crimes in these countries because of actions by a variety of pro-Palestinian organizations that have submitted complaints against them in these countries.[34]

One of the main explanations cited by Israeli legal officials for the need to increase their involvement in areas that relate to warfare is the (aforementioned) changes that have taken place in the international arena. Supreme Court justices explain that they must increase the scope of judicial review on issues concerning warfare in order to reduce the likelihood that IDF officers (and Israeli government ministers) will find themselves candidates for prosecution abroad.[35] In turn, officials from the State Attorney's Office argue that they must be more involved, both for the reason mentioned by the Supreme Court and because, they claim, their involvement reduces the chances that security agencies will "lose" in petitions filed against them in the Israeli Supreme Court.[36]

However, about two decades have passed since international criminal law began once again to flourish and, thus far, no Israeli has found himself prosecuted abroad. If so, has the time not come to wonder whether true cause for concern exists? Have lawyers misled officials in the army and the Israeli government?[37] Is it possible that these officials have enabled lawyers to be increasingly involved in warfare because of an exaggerated or even groundless fear?[38]

Here legal officials suffer the consequences of a known psychological bias, which is that people tend not to attribute sufficient importance to events that have not taken place (non-events).[39] This phenomenon has frequent consequences in politics as well. For example, experience proves that a politician who has failed to prevent war but has led his country to victory in that war usually receives more credit from the public than a politician who, in analogous situations, has succeeded in preventing war at the cost of certain diplomatic concessions. This is true even if the price of victory in war (in the first instance) is heavier than the price of diplomatic compromise (in the second). One of the reasons for this is that while in both cases the price of achieving the result is tangible, only in the first case is the result itself tangible, as noted by Melson:[40]

> A catastrophe averted is likely not to be seen as a catastrophe. A predicted event that fails to materialize is a non-event, something that did not happen, and politicians who have expended wealth and lives on something that failed to happen cannot be expected to reap the rewards of their decisions. On the contrary, politicians who risk lives and wealth to avert catastrophes … run the risk of being vilified and punished for their efforts: To the extent that their actions succeed in averting a catastrophe, there will be no evidence of their success—only of the costs of their efforts.

In reality, a situation in which no Israeli official has been prosecuted outside of Israel is not evidence of legal hysteria. To a large extent, the reason for this is the increased involvement of Israeli lawyers in warfare-related issues. A clear example of the success of legal activity can be seen in connection with lawsuits filed in Spain on the basis of universal jurisdiction against senior Israeli officials for the targeted killing of Saleh Shehadeh. In that case, the proceedings ended with a determination by the Spanish

courts that since the Israeli judicial system had handled the case credibly, the Spanish justice system did not need to intervene.[41]

Conclusion

The involvement of legal officials in warfare-related issues has grown in recent decades. This article has attempted to respond briefly to some of the main arguments raised against this process. The claim that the State of Israel would have lost its wars in the past if lawyers then were involved to the extent that they are today is mistaken, since in practice lawyers' wartime involvement was extensive even in the past, and this did not interfere with Israel's ability to achieve victory. Similarly, Israel need not fear reaching the point where every soldier needs a lawyer, and the fact that this scare tactic has been used for many decades is perhaps the best evidence that it is a false claim. Finally, there is a real need to make use of lawyers: they help commanders in the decision making process and prevent soldiers from yielding to the temptation to break the law. Furthermore, they have succeeded, at least thus far, in protecting Israeli soldiers (and other government officials) from criminal prosecution abroad.

Notes

1 See, for example, Yisrael Harel, *Lawyers vs. Soldiers*, Haaretz, October 29th, 2010, http://www.haaretz.co.il/misc/2.444/1.1227418.

2 The data presented here is part of a more extensive study that is in its very early stages: Ziv Bohrer, *The Normative Implications of the Forgotten War Crimes Trials of 1948* (forthcoming).

3 See Tzvi Inbar, *The Military Advocate General: Historical Aspects*, 15 Mishpat VeTzava 7, 11 (2001), http://www.law.idf.il/SIP_STORAGE/files/8/278.pdf.

4 Apparently, this refers to the murder of a Polish arms dealer.

5 Inbar, *supra* note 3, 13.

6 Tzvi Inbar, Sword and Scales of Justice: the Foundations of Military Law in Israel 130 (vol. 1, 2005).

7 *Ibid*., 243.

8 In my forthcoming article (*supra* note 2), I intend to discuss these indicators. As examples of cases, revealed in recent years, in which soldiers were prosecuted for war crimes during the Israeli War of Independence, see Benny Morris, 1948: The History of the First Arab-Israeli War 189 (2010) (prosecution for rape); Inbar, *supra* note 3, vol. 2, 662 (prosecution for injuring a prisoner of war), but see also the complex case of First Lieutenant Lahis, discussed *ibid.* at 659-661. Concerning the prosecution against acts of pillage, it should be noted that it is sufficient to skim Inbar's book in order to realize the extensiveness of the phenomenon. See also Appeal 147/50 *Sergeant H. and Second Lieutenant R. v. Chief Military Prosecutor*

(1951) *in* Ziv Bohrer, *The Defense of Justification for Obeying an Order and Clearly Illegal Orders in Israeli Law*, 433 (forthcoming, 2014) (a verdict that dealt with a case of rape and murder that occurred several months after the end of the War of Independence and was prohibited from publication until 2005). In another verdict, which dealt with the same incident, the soldiers who were present at the outpost but did not participate in the rape and murder were also punished. These soldiers were placed on trial for the military offense of "failure to prevent a crime," even though their commander was a leading participant in perpetrating the criminal acts. *See* Appeal 49/50 *Corporal B. and Seventeen Others v. Chief Military Prosecutor* (unpublished and prohibited from publication until 2005).

9 For example, Yehoshua Breiner, *Following Investigation of Death of Palestinian in Qusra, IDF Officer Dismissed*, Walla! News, October 24th, 2011 (quoting the position of the 'Council of Samaria Settlers'). *See also*, Akiva Bigman, *Combat Inhibitors*, News1, December 11th, 2011.

10 Government Commission of Inquiry to Examine the Events of the Campaign in Lebanon 2006 488 (Final report - June 2008; in Hebrew; [the Winograd Commission]) ("We fear that the increasing reliance on legal advice during military operations could cause the diversion of responsibility from elected officials and commanders to [legal] advisors, which is liable to disrupt both the fundamental quality of the decisions and the operational activity [itself]"). Yehuda Meir-Roth, *The Phenomenon of 'Seeing No Evil,' in the IDF*, 441 Maarachot 62 (2012).

11 Major-General C. J. Napier, Remarks on Military Law and the Punishment of Flogging (1837).

12 *Ibid*., 22-23.

13 Regarding obedience to orders given during riot-dispersal, the comment by Napier was erroneous even in its time. In regard to obedience to illegal orders given during combat, there is no doubt that at the very least, since the Second World War, Great Britain (like most countries in the world) has rejected the position that soldiers must give blind obedience. *See* Ziv Bohrer, *England and the Superior Orders Defence—Choosing the Middle Path*, 12 Oxford University Commonwealth Law Journal 273 (2012-13).

14 Ruvik Rosenthal, *Who Killed Fatma Sarsour: Background, Motives, and the Sequence of Events in the Case of Kafr Kassem in* Kafr Kassem: Myths and History 11, 45 (Ruvik Rosenthal, ed., 1st ed. 2000). Rosenthal quotes an article in *Maariv* newspaper from February 27, 1959, in which an IDF officer was reported to state that he had come to the courtroom to hear the verdict in the case of Colonel Shadmi because: "I came to hear if in the event of a future war, the commanders will need to go into battle with a personal lawyer for each of them."

15 Frederick Schauer, Playing by the Rules 15-37, 100-02 (1992).

16 Seaford Court Estates Ltd v. Asher [1949] 2 KB 481, 498-99 ("Whenever a statute comes up for consideration it must be remembered that it is not within human powers to foresee the manifold sets of facts which may arise, and, even if it were, it is not possible to provide for them in terms free from all ambiguity.") It is impossible to argue with the fact that certain norms of the laws of war suffer especially from problems of a lack of agreed interpretation. However, this does not mean that these norms can tolerate any interpretation. *See* Arthur D. Watts, *International Law and*

International Relations: U.K. Practice, European Journal of International Law 157, 164 (1991). In addition, it is important to note that there is a gradual process of clarification of the laws of war (or at least, of some of them). *See* Antonio Cassese, *The Statute of the International Criminal Court: Some Preliminary Reflections*, 10 European Journal of International Law 144, 156 (1999).

17 Paul H. Robinson, *Fair Notice and Fair Adjudication*, 154 University of Pennsylvania Law Review 335, 361 (2005-2006).

18 Larry Alexander and Emily Sherwin, The Rule of Rules 31-32 (2001).

19 Heidi Hurd, *Justifiably Punishing the Justified*, 90 Michigan Law Review 2203, 2238-39 (1992).

20 In the state context, sometimes, a clause in the law will even be annulled by the courts when it suffers from especially serious problems of ambiguity or over-inclusiveness. See a discussion on this in Israel High Court of Justice Case 6358/05 *Vanunu v. OC Home Front Command* (2006) (para. 20 of the verdict by Judge Procaccia).

21 Israel High Court of Justice Case 1397/03 *State of Israel v. Shimon Sheves*, para. 30 of the verdict by President Barak: "The level of [legal] certainty … must be higher in the penal realm. However, absolute certainty is not required; the maximum degree of certainty that can be achieved, considering the type of matter being resolved, should be required (…). We should not expect total certainty").

22 *See* Daniel Muñoz-Rojas and Jean-Jacques Frésard, The Roots Of Behavior In War: Understanding and Preventing IHL Violations 15 (2004).

23 *See* Frederick Schauer, *Rules and the Rule of Law,* 14 Harvard Journal of Law & Public Policy 645, 662-65 (1991).

24 *See* Re'em Segev, *Justification, Rationality and Mistake: Mistake of Law Is No Excuse? It Might Be a Justification!* 25 Law & Philosophy 31, 56-61, 67-74 (2006) (Segev argues that legal systems should do even more in the direction stated).

25 See David Luban, *That the Laws Be Faithfully Executed: The Perils of the Government Legal Advisor,* 38 Ohio Northern University Law Review 1043, 1044-45, 1055 (2011-2012).

26 Meir-Roth, *supra* note 10, 69.

27 For the history of the military "Staff," see *Encyclopedia Britannica* (11th ed., 1911), as presented in http://www.1911encyclopedia.org/Staff. For the role of the Staff, see Department of the Army, Staff Organization and Operations 1-1 (1997, FM 101-5); Boaz Zalmanovitz, *Who Needs a Chief of Staff?* 435 Maarachot 68, 68-70 (2011).

28 The example cited in the text is of course simplistic. In practice, in a modern military, the scope of discretion and the responsibility of Staff Officers is much greater than might be inferred from that example. See Morris Janowitz, The Professional Soldier 67 (1960). This fact only narrows the difference that exists in reality between the nature of the relationship between the commander and the artillery officer on the Staff and the nature of the relationship between the commander and the legal advisor.

29 *See* Luban, *supra* note 25, 1044-45. Needless to say, broader ethical and legal obligations are imposed on the State's lawyers than on those in private practice. See Watts, *supra* note 16, 164; Uri Shoham, *The Military Advocate General and*

the Attorney General: Between the Sadiel Affair and the Avivit Attia Petition to the High Court of Justice, 16(2) Mishpat VeTzava 203, 341, 361, 407-08 (2002).

30 Giora Eiland, *The Foundations of Israel's Response to Threats*, 2(1) Military and strategic affairs 57, 62 (2010).

31 *See* Antonio Cassese*, On the Current Trends toward Criminal Prosecution and Punishment of Breaches of International Humanitarian Law*, 9 European Journal of International Law 2 (1998).

32 *See* Yuval Shany, *The Entry into Force of the Rome Statute: What are the Implications for the State of Israel?*, 9 HaMishpat 51 (2004); International Criminal Court Office of the Prosecutor, *OTP Update on the Situation in Palestine* (April 3rd, 2012), http://www.icc-cpi.int/NR/rdonlyres/C6162BBF-FEB9-4FAF-AFA9-836106D2694A/284387/SituationinPalestine030412ENG.pdf; John V. Whitbeck, *Palestine and the ICC*, The Palestine Chronicle (April 6th, 2013), http://palestinechronicle.com/palestine-and-the-icc/#.UX9nJl_fodU.

33 *See* Orna Ben-Naftali and Keren Michaeli, *Universal Jurisdiction and the National Legal Discourse*, 9 HaMishpat 141 (2004).

34 For a review of some of these cases, see Diane Morrison and Justus Reid Weiner, *Curbing the Manipulation of Universal Jurisdiction*, Jerusalem Center for Public Affairs (2010), http://jcpa.org/text/universal-jurisdiction.pdf.

35 Naomi Levitsky, The Supremes: Inside the Supreme Court 176 (2006); Amihai Cohen, *The Impact of International Law on Israel in the Era of Global Jurisdiction*, 65 Parliament (2010) (a copy of the article can be found on the website of the Israel Democracy Institute, http://www.idi.org.il).

36 Elyakim Rubinstein, *On Security and Human Rights in the Era of the War on Terror*, 16(4) Mishpat VeTzava 765, 776-778 (2003).

37 *See* Avi Becker, *The Delegitimization of Israel: A New Secular Religion*, 24 Kivunim Hadashim 35, 41(2010) See also a more general discussion in Gad Barzilay, *The Ambivalent Language of Lawyers in Israel: Liberal Politics, Economic Liberalism, Silence, and Dissent*," 15(1) HaMishpat 193, 212 (2010).

38 *See* Cohen, *supra* note 35; Eiland, *supra* note 30, 62; Amir Oren, *The Goldstone Report on Operation Cast Lead: Fear is the Best Legal Advisor*, Haaretz, September 16th, 2009, http://www.haaretz.co.il/misc/1.1280927.

39 James Parkin, Judging Plans and Projects: Analysis and Public Participation in the Evaluation Process 42 (1993).

40 Robert Melson, *Churchill in Munich: The Paradox of Genocide Prevention,* 3(3) Genocide Studies & Prevention 297, 298 (2008). On other psychological biases that lead to greater public sympathy for a politician who has failed to prevent war than one who has prevented it, see Daniel Kahneman and Jonathan Renshon, *Why Hawks Win*, 158 Foreign Policy 34 (2007).

41 See the discussion of this incident in Ido Rosenzweig and Yuval Shany, *Update on Universal Jurisdiction: Spanish Supreme Court Affirms Decision to Close Inquiry into Targeted Killing of Salah Shehadeh*, 17 Terrorism and Democracy (April 5th, 2010), http://en.idi.org.il/analysis/terrorism-and-democracy/issue-no-17/update-on-universal-jurisdiction-spanish-supreme-court-affirms-decision-to-close-inquiry-into-targeted-killing-of-salah-shehadeh/; Ido Rosenzweig and Yuval Shany, *Update on Universal Jurisdiction: Spanish Court of Appeals Decides to Close the*

Inquiry into the Targeted Killing of Salah Shehadeh, 8 Terrorism and Democracy (July 17th, 2009), http://en.idi.org.il/analysis/terrorism-and-democracy/issue-no-8/update-on-universal-jurisdiction-spanish-court-of-appeals-decides-to-close-the-inquiry-into-the-targeted-killing-of-salah-shehadeh/. For a discussion of another case in which the attempt to prosecute Israelis abroad failed, see Ido Rosenzweig and Yuval Shany, *Universal Jurisdiction: Dutch Court Dismisses Appeal Petition on Torture Allegations against Ami Ayalon*, 11 Terrorism and Democracy (November 2009), http://en.idi.org.il/analysis/terrorism-and-democracy/issue-no-11/universal-jurisdiction-dutch-court-dismisses-appeal-petition-on-torture-allegations-against-ami-ayalon/.

Applying International Humanitarian Law to Cyber Warfare

Eitan Diamond

This article seeks to shed some light on the application of international humanitarian law (IHL), otherwise known as the law of armed conflict or the laws of war, to the phenomenon of cyber warfare.

For the purposes of this essay, the term "cyber warfare" describes cyber operations conducted in or amounting to an armed conflict. Such cyber operations, which involve the development and dispatch of computer code from one or more computers to target computers, can be aimed at either infiltrating a computer system to collect, export, destroy, change, or encrypt data, or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated system.[1]

Even while directed at computers rather than people, such operations could potentially cause a tremendous degree of human suffering. In times of armed conflict in particular, there are grounds for concern that cyber operations will be used to undermine the functioning of infrastructure needed for the provision of resources and services of crucial importance to the civilian population. Critical installations such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control all rely heavily on computer systems susceptible to infiltration and manipulation via cyber operations. The risk that civilians and civilian objects will come to harm as a result of cyber warfare is heightened by the high level of interconnectivity and interdependence between civilian and

Eitan Diamond is a legal advisor in the International Committee of the Red Cross (ICRC) Delegation in Israel and the Occupied Territories. The views expressed in this article are those of the author and do not necessarily reflect those of the ICRC.

military computer infrastructure, which can make it extremely difficult to differentiate between them.[2] Thus, an attack on a military computer system is very likely to damage civilian computer systems as well. These in turn may be vital for some civilian services such as water or electricity supply, or the transfer of assets.

In view of these potential risks, it is clear why there is a humanitarian need for the law to regulate and constrain cyber warfare. At the same time, despite some notable attempts to create greater clarity,[3] many questions remain open about how existing legal frameworks might be applied to this relatively new phenomenon about which much is still unknown.

This article will not provide comprehensive answers to all such questions. For one thing, it will not attempt to address questions relating to all of the bodies of law that may be applicable to cyber warfare, and will instead address only questions relating to the application of IHL. Furthermore, even while the analysis will be confined to the challenges that cyber warfare poses for IHL, a number of significant questions will remain unanswered. Rather than attempting to provide answers, which – for reasons that will be explained – is not currently possible, the article will endeavour to map out the most pressing questions and indicate what challenges must be overcome if IHL is to attain its goal of preserving human dignity and preventing unnecessary human suffering even in the wake of this novel form of warfare.

As a backdrop for the analysis, the article will first highlight the general difficulty of applying the long-established rules of IHL to hostilities involving new methods and means of warfare, a difficulty that is particularly evident in the case of cyber operations. The lack of transparency and the overall dearth of information surrounding cyber operations create further obstacles for the application of IHL. The article will then discuss problems that may arise in determining whether cyber operations have occurred within a situation of armed conflict. This is significant, because IHL only applies in an armed conflict. Once it has been determined that a situation of armed conflict exists, it is necessary to ascertain how the applicable rules of IHL are to be interpreted and applied to cyber operations. In this regard the article will consider in what circumstance cyber operations trigger the IHL rules on the conduct of hostilities, and how the principle of distinction, the principle of proportionality, and the duty to take precautions are to be implemented in the case of cyber warfare.

Adapting Old Laws to New Cyber Technologies

Legal norms are by nature general and forward looking. They establish rules of conduct that are to be applied in diverse and as yet unknown future situations. To accomplish this task the law must paint with a broad brush. It cannot possibly spell out specific rules for all sets of circumstances that may arise, and so instead, it applies rules across different general categories that it defines and distinguishes from one another. The transition from such general norms to concrete and ever-changing realities is not seamless and requires a regular process of adaptation.

In the realm of domestic law, this task is achieved in large part through acts of interpretation by national courts, which are constantly called upon to apply the law to specific incidents, and through legislative amendments, which can be enacted in response to changing sensibilities and new realities. In the realm of international law, the process of adaptation is far more cumbersome. For one thing, an international norm cannot be enacted by the legislature of a single state, but instead emerges only when multiple states express their consent to be bound by it.[4] Since states are driven by different and often contrasting interests and incentives, such consensus is difficult to achieve. Adapting international law through judicial interpretation is also complicated since relevant jurisprudence occurs haphazardly in instances from diverse jurisdictions, and it is therefore not always possible to extract a coherent and authoritative interpretation.

The process of adapting law to change is particularly challenging when it comes to IHL, as it regulates situations of armed conflict that naturally evoke contrasting positions between states. Indeed, states so rarely reach the necessary consensus on such matters that the key provisions of IHL are still found in treaties that are many decades old and in some cases date back more than a century.[5] But while the law evolves slowly, new means and methods of warfare develop continually and the battlefield is rapidly changing. Bridging the temporal and contextual gap between the moment of the law's formation and the moment of its application is thus becoming an ever growing and more urgent challenge.

Fortunately, and precisely because of the types of challenges just described, the IHL rules governing the conduct of hostilities, including such core principles as the principles of distinction and proportionality and the duty to employ precautionary measures, are broadly and flexibly defined and can therefore accommodate even far-reaching developments. These general

rules regulate all means and methods of warfare, including the use of all weapons, and are thus applicable to cyber warfare as well. However, in the case of cyber warfare, their capacity to accommodate change is tested to the extreme. The IHL framework governing the conduct of hostilities was designed to apply to methods and means of warfare involving the use of kinetic force in the physical world, and therefore makes an awkward fit for hostilities that consist of the manipulation of data in cyberspace. In fact, as we shall see, even some of the basic assumptions underlying IHL come into question, and categories and distinctions fundamental to IHL – such as "armed conflict," "attack," "civilian object," and "military objective" – are not easily retained when applied to cyber warfare.

Applying IHL to Technologies and Operations Veiled in Secrecy

The difficulty of adapting IHL to cyber warfare is compounded by the veil of secrecy enveloping cyber security operations. Law, after all, must be applied to facts. When the facts are not well known it is not possible to have a clear legal reading. More precisely, key information needed in order to make an informed evaluation of cyber operations compatibility with IHL is often lacking, including details about (a) the technology available, (b) the attacks conducted, (c) the identity of the parties conducting the attacks, and (d) the policies, guidelines, and rules that states apply in relation to cyber warfare, along with their reading of the applicable rules of IHL.

Information about the technological capabilities that exist or are under development is necessary to evaluate whether the methods and means of warfare facilitated by these technologies meet the requirements of IHL. In practice, however, states are rarely forthcoming about the offensive and defensive capabilities they already have or are developing for cyber warfare, and little is known about the types of cyber operations or cyber weapons available to other actors. States are equally unwilling to divulge details about cyber operations they have undertaken against others or about those that have been directed against them. Thus, it is hardly possible to review the ways in which belligerent parties engaged in armed conflict actually employ such operations in the conduct of hostilities. In other words, it is not properly known what attacks have been conducted using cyber technology, let alone what such attacks might have entailed. Likewise, since cyber operations are typically anonymous, it will in most cases be difficult, if not impossible, to identify the party responsible for the operation. Thus, it will often not be

possible to determine if the operation was conducted by a party to an armed conflict and, consequentially, if IHL even applies.

The secrecy surrounding state capabilities and practices in the field of cyber warfare also extends to the rules and regulations that states apply in relation to cyber operations. In light of this, and since states have for the most part refrained from disclosing directly what they consider to be the proper application of IHL to cyber warfare,[6] it is very difficult to discern their legal position on the matter.

Given that states are the authors of international law, the lack of transparency regarding both their practice and legal position in relation to cyber warfare undermines efforts to attain legal clarity in this area. Commentators are left to speculate what such warfare does or could entail, and to propose, without the benefit of supporting state practice or legal opinion, how it ought to be conducted.

Does Cyber Warfare Fall within the Confines of Armed Conflict?

Since IHL applies only in the context of armed conflict, what must first be ascertained when considering if a given cyber operation is subject to IHL is whether the operation in question was conducted in the context of and with a nexus to an armed conflict.

Seemingly the applicability of IHL would be relatively easy to establish in relation to cyber operations occurring against the backdrop of an existing armed conflict, but even then it is by no means self-evident and complicating factors are likely to come into play. In particular, it will not necessarily be possible to determine that the operations are in fact related to the armed conflict. Indeed, since the nature of cyber operations is such that the identity of the actor carrying them out may very well be unknown, there may be no grounds to assert that the operations were conducted by or on behalf of a party to an armed conflict. For such time as the connection to armed conflict remains in doubt, so too would the applicability of IHL.

Still more problematic would be cases in which cyber warfare does not occur alongside other forms of hostilities. In such situations the additional question arises whether cyber operations can themselves amount to armed conflict. In addressing this question, it is necessary to distinguish between the two different types of armed conflict that are regulated by IHL, i.e., international armed conflicts, occurring between states, and non-international

armed conflicts, in which at least one of the belligerent parties is a non-state actor.

An international armed conflict occurs whenever there is a resort to armed force between states.[7] Accordingly, cyber warfare would constitute an international armed conflict only if (a) the cyber operations involved are attributable to a state, and (b) they amounted to a resort to armed force against another state.

Again, the question of attribution is difficult in the context of cyber warfare. It has been suggested that this difficulty might be mitigated to some extent by adopting appropriate legal presumptions.[8] Thus, for example, a state would be presumed responsible for any cyber operation originating from its governmental infrastructure unless it could prove otherwise. However, there is no basis in existing international law for such a presumption. Moreover, given the ease with which different guises can be assumed in cyberspace and the difficulty of shielding computer infrastructure from manipulation, the presumption could be extremely artificial and might be said to place an unreasonable burden on states.[9]

Besides the factual difficulties in determining the source of a cyber operation, the attribution of a cyber operation to a state may also be complicated by questions concerning the scope of states' legal responsibility for cyber operations that were not conducted directly by them, but rather by private persons or groups. The potential attribution of acts of private agents to the state is not unique to cyber warfare. The general rule under international law in this regard is that the conduct of a person or group of persons is attributable to a state "if the person or group of persons is in fact acting on the instructions of or under the direction or control of that State in carrying out the conduct."[10] This has been interpreted variously to conclude that (a) the actions of private agents are attributable to a state only with respect to specific operations over which the state had effective control;[11] or that (b) it is sufficient for a state to have "overall control" over a group for the latter's actions to be attributed to it.[12] Either way, applying these tests to cyber warfare, where the relevant facts may be more difficult to establish, is likely to prove challenging and may be further complicated by the need to interpret the notion of "control" in relation to actions and actors operating in cyberspace.

Assessing whether cyber operations satisfy the second criterion for an international armed conflict, namely that they amount to the resort to armed

force against a state, presents another significant hurdle. The traditional concept of armed force is of hostilities involving means and methods of warfare entailing the use of kinetic force. Applying this concept to the act of developing and sending computer code is not a straightforward exercise. When can such acts be considered to amount to "armed force"? There is broad agreement among analysts that computer network attacks that lead to physical destruction parallel to the destruction produced by attacks employing kinetic force would amount to an armed attack.[13] However, cyber operations are capable of effecting other forms of harm. Rather than physically destroying a target system, they could be used to hamper its functioning. The harm thus caused would take direct effect not in the physical world but in cyberspace. Indeed, this type of cyber network attack might very well go undetected, while the indirect effects of such an attack – which could, for example, disrupt the supply of vital resources (such as water, electricity, or oil) or the provision of essential services – could be most harmful indeed. If IHL is to be interpreted in accordance with its underlying humanitarian purpose,[14] then presumably cyber operations producing such grave humanitarian consequences ought to be considered as within the ambit of armed force and thus subject to the protective provisions of IHL.

On the other hand, the classification of a situation as an armed conflict brings into play not only the restrictive provisions of IHL, but also its permissive aspects. IHL allows for – or at least does not prohibit – the intentional use of lethal force against certain categories of people (such as enemy combatants[15] and civilians directly participating in hostilities) and the intentional destruction of certain categories of property (military objectives), and also tolerates a degree of incidental harm to other categories of persons and objects ("collateral damage") that would all be prohibited by the law applicable outside of armed conflict. Those seeking to restrict the scope of force legally permissible might therefore have good reason to favor a more restrictive approach in interpreting when cyber warfare amounts to resort to armed force. In any event, in the absence of state practice or clarification of states' legal positions (*opinio juris*), it remains an open question whether, and if so, under what conditions, cyber warfare can be said to constitute resort to armed force even when not producing direct physical destruction.

A non-international armed conflict exists whenever there is protracted armed violence, meaning armed violence of a certain degree of intensity, between governmental authorities and organized armed groups or between

such groups within a state.[16] In other words, in order for a situation to be classified as a non-international armed conflict it must entail armed violence involving at least one non-state actor where (a) the parties involved satisfy a minimum level of organization and (b) the armed violence reaches a minimum level of intensity. However, applying these criteria to cyber warfare raises a number of difficulties.

For one thing, the nature of virtually organized groups of the type active in cyberspace – such as groups of hackers cooperating in joint cyber operations – is such that they will rarely, if ever, satisfy the requirement of a minimum level of organization as thus far understood. Under this requirement, the group should have a command structure with a level of hierarchy and discipline sufficient to enable it both to carry out sustained acts of warfare and to implement the basic rules of IHL.[17] It is difficult to see how groups whose members are linked only by virtual communication and who may never have met in person or even know each other's identity would fit this mold.[18] For this reason it seems that while the activities of such groups could certainly constitute criminal behavior, it would be incorrect to say that they also amount to an engagement in armed conflict. However, this conclusion might be met with some unease when it is observed that the cyber operations conducted by virtually organized groups could potentially result in levels of harm and destruction akin to that produced by armed conflict.

When cyber operations indeed bring about levels of physical destruction similar to those produced by kinetic operations, it would not seem contentious to say that they could meet the threshold of intensity required to bring a non-international armed conflict into play. However, as with the criterion of resort to armed force discussed above in relation to international armed conflict, it is by no means clear when and under what conditions the calamitous results produced by cyber operations through the manipulation of computer networks (rather than direct physical destruction) might also be deemed of such intensity as to have generated a non-international armed conflict. Here, again, there is no instructive state practice or *opinio juris*, and humanitarian considerations do not point conclusively in favor of a particular interpretive approach.

Applying IHL Rules on the Conduct of Hostilities to Cyber Warfare

If occurring in the context of armed conflict, cyber operations would be subject to IHL, including in particular the IHL rules governing the conduct of hostilities. It is clear, however, that the application of these rules to operations involving the deployment of computer code in cyberspace, as opposed to the use of kinetic force in the physical world, is no simple matter.

The first challenge in this regard would be to determine what types of cyber operations would be subject to the rules governing the conduct of hostilities. This question is pertinent because of cyber operations' capacity to severely disrupt the functioning of key infrastructure without causing physical destruction of the type produced by traditional methods and means of warfare. With respect to the types of cyber operations that do fall within the conduct of hostilities framework, it will then be necessary to consider how the relevant rules, and most fundamentally the principles of distinction, proportionality, and precaution, are to be adapted and applied to cyber warfare.

When are Cyber Operations Subject to the Rules on the Conduct of Hostilities?

The rules on the conduct of hostilities codified in the First Additional Protocol to the Geneva Conventions (Additional Protocol I) are broadly recognized as reflective of customary international law applicable both in international and non-international armed conflicts.[19] Most of the specific rules contained in this framework are formulated as restrictions on those military operations that constitute an "attack."[20] This has prompted many to conclude that the rules on the conduct of hostilities apply only to cyber operations constituting an attack as defined in IHL.[21] However, this position is difficult to reconcile with the fact that the provisions of Additional Protocol I establishing the principles of distinction, proportionality, and precaution all contain clauses relating to military operations in general.[22] If these clauses are not to be deemed superfluous, the core principles governing the conduct of hostilities should be understood to apply not only to attacks, but also to hostilities in broader terms, i.e., to other military operations carried out in the context of an armed conflict with the purpose of harming the adversary.

Still, it would seem that all of the specific rules on the conduct of hostilities focusing on attacks as distinct from other types of military operations do indeed apply only to those cyber operations amounting to an attack. Since

much, even if not all, of the body of rules governing the conduct of hostilities is thus confined to attacks, it is clearly important to ascertain what cyber operations would in fact amount to an attack.

Article 49 of Additional Protocol I, which reflects customary IHL, defines attacks as "acts of violence against the adversary, whether in offence or in defence." It is accepted that the violence relates to the consequences of the attack and not the means used to effect those consequences. Accordingly, the sending of computer code, though not itself an act of physical violence, could nonetheless constitute an attack if it produces a violent outcome.

This view is reflected in the Tallinn Manual when it defines "cyber attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[23] A pressing question that this definition does not resolve and remains subject to debate, however, is whether harmful outcomes produced by cyber operations might be deemed as constituting an attack even when they do not involve direct physical destruction, but instead cause other forms of damage to an object such as impaired performance. On the one hand, it would not make sense to maintain that cyber operations disrupting the functionality of critical infrastructure with deleterious consequences for potentially a great many people would not constitute an attack merely because they did not entail physical destruction. On the other hand, it would also be unreasonable to maintain that any interference with a computer system would amount to an attack that brings into play all of the rules governing the conduct of hostilities.

While the exact line of demarcation between cyber operations amounting to an attack and those that do not remains elusive, some considerations can help distinguish between them. For one thing, since the IHL concept of attack does not apply to non-physical means of psychological or economic warfare, such as the dissemination of propaganda or the establishment of an embargo,[24] cyber operations equivalent to such forms of "warfare" do not amount to an attack. Unlike attacks, which may never justifiably target civilians, IHL does not prohibit blockades and economic sanctions intentionally directed at the civilian population. Accordingly, cyber operations tantamount to economic sanctions cannot be said to constitute an attack.[25] Moreover, just as interferences with communications such as the jamming of radio or television broadcasts are not considered an attack under IHL and can therefore be directed at civilian communication systems as well, so

too not every disruption of computer based communication systems would constitute an attack. Of course, some types of interference with computer-based communications could have far reaching impact (e.g., disrupting the operation of financial institutions), and it therefore remains necessary to clarify exactly when, if ever, such interferences would constitute an attack. Indeed, while it is relatively straightforward to assert that cyber operations disrupting the functioning of objects in the physical world constitute an attack, the situation is far less clear when it comes to operations aimed merely at disrupting communication in cyberspace.

Applying the Principle of Distinction in Cyberspace

Under the principle of distinction, the parties to an armed conflict are obligated to distinguish at all times between the civilian population and combatants, and between civilian objects and military objectives, and may direct their operations only against military objectives.[26] Accordingly, cyber operations must only be directed at military objectives, namely "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."[27] Any object that does not fall within this definition is considered a civilian object and may not be the target of an attack.[28] Moreover, in case of doubt whether an object normally dedicated to civilian purposes is being used to make an effective contribution to military action, it must be presumed not to be so used and, consequently, may not be made the target of an attack.[29]

The main difficulty in applying these rules to cyber warfare lies in the fact that most cyber infrastructure is dual use, serving both civilian and military purposes. The currently prevailing position is that dual use objects are military objectives because of the military purpose they serve.[30] When applied to cyberspace, this position implies that almost all elements of international cyber infrastructure should be classified as military objectives and (subject to other IHL rules) could be susceptible to attack. Indeed, in this view, the cables, nodes, routers, and satellites on which so many civilian systems depend would all be deemed military objectives because they have the dual function of transmitting military information. With so many objects in the cyber realm thus considered military objectives, the principle of distinction – which is conceived as the foundational rule for shielding civilians from the dangers arising from hostilities – becomes largely devoid of protective

value. Whatever protection IHL might provide to civilian cyber infrastructure and to the civilian systems and services dependent on it would have to be derived from the principles of proportionality and precaution.

Even civilian cyber infrastructure that is not dual use and would therefore be protected from direct attack might nevertheless come to harm because of the interconnectedness of cyberspace. In order to avoid this outcome, and in accordance with the prohibition on indiscriminate attacks,[31] belligerent parties are prohibited from employing cyber weapons that are indiscriminate by nature, such as malware computer programs that replicate without control (viruses, worms) and whose harmful effects could not be limited as required by IHL. Furthermore, a belligerent intending to mount a cyber attack would have to first verify that in the given circumstances, the cyber weapon employed can be and is in fact directed at a military objective and that its effects can be limited as required by IHL.

The wide ranging list of military objectives in cyber warfare gives rise to questions concerning the geographical limits of the armed conflict. After all, cyber operations can utilize cyber infrastructure located anywhere in the world and could involve thousands or even millions of computers in diverse locations around the globe. If all such infrastructure were to be deemed a military objective, an armed conflict involving cyber warfare could be expanded to cover every corner of the earth. Every cyber war would be a potential cyber world war. In international armed conflicts the consequences would be checked to some degree by the laws of neutrality, which would limit the belligerent states' right to attack infrastructure located in the territory of a neutral state to those cases where the neutral state itself fails to terminate breaches of neutrality emanating from its territory; where such breaches constitute a serious and immediate threat to the attacked state's security; and when there is no other feasible and timely alternative response available.[32] In non-international armed conflicts, in which the law of neutrality is not applicable, questions about the geographical limitations of the battlefield are the subject of ongoing debate and become all the more vexing when the conflict involves cyber warfare.[33]

Applying the Principle of Proportionality in Cyberspace

Under the principle of proportionality, an attack is prohibited if it "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."[34] Here again a key question when applying the principle to cyber warfare will be to determine to what extent the term "damage" encompasses loss of functionality. In view of the severity of the consequences that may arise when the functionality of civilian infrastructure is disrupted, it seems only reasonable that such harm should figure in the proportionality calculus. On the other hand, and as already noted, it remains to be clarified exactly what types of disruptions to functionality fall within the relevant category of damage.

A further challenge in applying the principle of proportionality would be to determine whether the incidental damage to civilian objects that may be expected is excessive in relation to the military advantage anticipated. To be sure, the exercise of weighing expected harm to civilians or civilian objects against anticipated military advantage is always problematic, but in the case of cyber warfare the problems are exacerbated by the difficulty to assess with any accuracy what scope of incidental damage can be expected. This is so both because cyber operations are a relatively novel phenomenon and so little is known about their impact, and because the interconnected nature of cyberspace makes it particularly difficult to foresee all of the possible effects of such operations.

Applying the Principle of Precaution in Cyberspace

IHL requires belligerents to take precautions in attack,[35] as well as precautions against the effects of attack.[36]

Precautions in attack are mandated by a general rule, applicable to all military operations, whereby constant care must be taken to spare the civilian population and civilian objects,[37] and by additional rules establishing specific precautionary requirements. *Inter alia*, these rules require those who plan or decide upon an attack to do everything feasible to verify that targets are military objectives[38] and to take all feasible precautions in the choice of means and methods of warfare with a view to avoiding and in any event minimizing incidental harm to civilians.[39] Belligerents are further required to cancel or suspend an attack if it becomes apparent that it will entail a breach of the principle of proportionality.[40]

In light of these rules, a party to an armed conflict planning to implement a cyber attack would have to do everything feasible to gain the information necessary to verify that the projected target is a military objective and to

ascertain that the attack will not cause excessive harm. This may require employing technical experts to analyze the target network and the systems with which it is interconnected as best possible. When the expertise necessary to gain and to evaluate the required information properly is missing, the attack must be avoided altogether. In any event, attacks must be limited to those targets about which sufficient information is available.[41]

In certain circumstances, the duty to choose means and methods of warfare with a view to minimizing incidental harm to civilians could conceivably require belligerents to pursue their military objective via cyber attack rather than resorting to more destructive means involving kinetic force.

The duty to take precautions against the effects of attacks requires that to the maximum extent feasible, the parties to an armed conflict will endeavor to keep military objectives apart from civilians and civilian objects and will take other necessary precautions to protect civilians and civilian objects under their control against the dangers resulting from military operations.

In principle, belligerents may thus be required to do everything feasible to separate their military and civilian cyber infrastructure. In practice, however, military and civilian cyber infrastructures are so thoroughly interwoven that the endeavor to separate them is not likely to be deemed feasible. Perhaps more promisingly, and to the maximum extent feasible, belligerents would also need to take all necessary precautions to ensure that critical civilian infrastructure will be protected as much as possible from the effects of cyber attacks, e.g., by ensuring that necessary data is safely stored and effectively backed up and by providing for timely repair of civilian systems that come to harm.

Conclusion

Cyber warfare does not occur in a legal void. To be sure, cyber operations are governed by law, and when amounting to or occurring in the context of an armed conflict they are regulated by IHL. However, even while there is no question that IHL applies to cyber warfare, when considering *how* it is to be applied many questions emerge that have yet to be given a comprehensive and satisfactory answer.

Because of the shroud of secrecy surrounding cyber operations and because they involve methods and means of warfare so drastically different from those that IHL has evolved to regulate, it will often be difficult even to ascertain whether they occur within and in connection to an armed conflict.

Even when this is established and the applicability of the IHL rules on the conduct of hostilities is not in doubt, it is not entirely clear which cyber operations would be subject to these rules. Nor is there any clarity as to how the long established rules are to be interpreted when applied to this new form of warfare.

From a humanitarian perspective it is of the utmost importance that these questions be answered and that IHL be applied in such manner as to provide civilians and civilian infrastructure with effective protection from the harmful effects of cyber warfare. This will require careful interpretation of existing rules in light of the underlying humanitarian purpose of IHL and may also necessitate the development of some more stringent rules to ensure that humanitarian values will not be compromised.

Notes

1 For details on this definition see Cordula Droege, *Get off My Cloud: Cyber Warfare, International Humanitarian Law, and The Protection of Civilians* 886 International Review of The Red Cross 533, 538 (2012).

2 Due to internet interconnectivity, most military networks rely on civilian, mainly commercial, computer infrastructure. Conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems relying on global positioning system (GPS) satellites, which are also used by the military.

3 The most comprehensive of these efforts is the Tallinn Manual on the International Law Applicable to Cyber Warfare (hereinafter "Tallinn Manual"), which was drafted by a group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. See Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt, gen. ed., 2013), http://www.ccdcoe.org/249.html.

4 States express their consent to be bound by an international norm either by becoming party to an international treaty containing it, or via international custom which in turn emerges from the consistent practice of states combined with the view that such practice is mandated by law (*opinio juris*). A norm of customary international law is binding on all states apart from those which expressed a consistent objection to the applicability of the norm in question.

5 These treaties include, notably, the Hague Conventions of 1899 and 1907, The Four Geneva Conventions of 1949 and the 1977 Additional Protocols to the Geneva Conventions of 1949.

6 In something of an exception to this general tendency, some general aspects of the United States' positions on the application of IHL (and other areas of international law) to cyber warfare were discussed in a speech delivered on 18 September 2012 by US State Department Legal Advisor Harold Koh at a conference sponsored by United States Cyber Command (USCYBERCOM). In his speech, Mr. Koh did not provide a detailed account of the United States' position but did offer brief

answers to "fundamental questions" on the issue and identified several "unresolved questions" with which the United States would likely be forced to grapple in the future. *See* Harold Hongju Koh, *International Law in Cyberspace: Remarks of Harold Koh*, 54 Harvard International Law Journal (December 2012), http://www.harvardilj.org/2012/12/online_54_koh/.

7 This commonly accepted definition of international armed conflict was articulated by the International Tribunal for the former Yugoslavia (hereinafter "ICTY") in *Prosecutor v. Tadic*, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, Para. 70. International treaties do not contain a detailed definition of international armed conflict. That said, common Article 2 of the Four Geneva Conventions of 1949 does establish that the conventions apply to any armed conflict that may arise between two or more states. Article 1(4) of the First Additional Protocol to the Geneva Conventions extends the scope of application to other situations, but this applies only in relation to states party to the Additional Protocol and is thus not applicable to Israel.

8 *See* discussion in Droege, *supra* note 1, at 543.

9 Rule 7 of the Tallinn Manual (*supra* note 3) provides that "[t]he mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that state but is an indication that the state in question is associated with the operation."

10 *See*, International Law Commission, Draft Articles on the Responsibility of States for Internationally Wrongful Acts, *Yearbook of the International Law Commission*, 2001, Vol. II (Part Two) at Article 8.

11 This was the position taken by the International Court of Justice (ICJ). *See*, International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of 27 June 1986, paras. 115–116.

12 This position was articulated by the ICTY in relation to the attribution of the actions of organized armed groups to a state. *See*, ICTY, *Prosecutor v. Dusko Tadic*, IT-94-1, Appeals Chamber Judgment of 15 July 1999, para. 120. It should be noted, first, that the ICTY was relating only to the attribution of responsibility for the actions of an organised armed group and not private actors in general. Second, the ICTY itself clarified that more compelling indications of state control would apply in cases where the armed group is not acting from within the territory of the state in question. *See*, *Ibid.* at paras. 138-140.

13 *See*, Droege *supra* note 1, at 546; Michael N. Schmitt, *Classification of cyber conflict,* 17(2) Journal of Conflict and Security Law, 251 (Summer 2012); Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, International Committee of the Red Cross 3 (2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm; Heather Harrison Dinniss, Cyber Warfare and the Laws of War, 131 (2012); Nils Melzer, *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research, Resources Paper, 24 (2011), http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf.

14 A purposive interpretation of IHL has been regularly pursued by the ICTY. *See*, e.g., Prosecutor v. Delalic et al. (Celebici Case), Judgment, Case No. IT-96-21-T, T.

Ch. IIqtr, 16 Nov. 1998, para. 170. For a general and authoritative discussion about the purposive interpretation of law see Aharon Barak, Purposive Interpretation in Law (Sari Bashi trans, 2005).

15 The term combatant applies only to fighters on behalf of the rival parties to an international armed conflict who would be entitled to prisoner of war (hereinafter "POW") status if captured by the adverse party. Fighters in a non-international armed conflict are not entitled to POW status, but can be made the target of direct attack by the rival belligerent.

16 This definition was articulated in ICTY, *Prosecutor v. Tadic*, *supra* note 7, at para. 70.

17 *See* ICTY, *Prosecutor v. Boskoski*, IT-04-82-T, Trial Chamber Judgment of 10 July 2008, paras. 199–203. *See* also, ICTY, *Prosecutor v. Limaj*, IT-03-66-T, Trial Chamber Judgment of 30 November 2005, paras. 94–134; ICTY, *Prosecutor v. Haradinaj*, IT-04-84-T, Trial Chamber Judgment of 3 April 2008, para. 60.

18 *See* Tallinn Manual, *supra* note 3, Commentary on Rule 23, paras. 13-15.

19 *See*, International Committee of the Red Cross, Customary International Humanitarian Law, Vol. I, Rules (Jean-Marie Henckaerts and Louise Doswald-Beck eds., 2005).

20 Multiple references to attack are found, notably, in Articles 51, 52, and 54-58 of Additional Protocol I.

21 *See*, e.g., Michael N Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 Naval War College International Law Studies, 91 (2011). For alternative views see Melzer, *supra* note 13, at 28 (arguing that that the rules apply to all cyber operations constituting part of 'hostilities') and Dinniss, *supra* note 13, at 196-202 (arguing that the rules apply to all computer network attacks that constitute military operations by virtue of being associated with the use of physical force even while not themselves resulting in violent consequences).

22 The formulation of the principle of distinction in Article 48 of Additional Protocol I stipulates that the parties to an armed conflict "…shall direct their *operations* only against military objectives." The first paragraph of Article 51 thereto stipulates that civilians "shall enjoy general protection against the dangers arising from *military operations*" and Article 57, para. 1 thereto instructs that "in the conduct of *military operations*, constant care shall be taken to spare the civilian population, civilians and civilian objects" (emphasis added).

23 *See*, Tallinn Manual, *supra* note 3, rule 30.

24 *See*, Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949, 289 (1982).

25 *See*, Droege, *supra* note 1, at 559.

26 *See*, Article 48 of Additional Protocol I, which reflects customary IHL.

27 *See*, Article 52(2) of Additional Protocol I, which reflects customary IHL.

28 *See*, Article 52(1) of Additional Protocol I, which reflects customary IHL.

29 *See*, Article 52(3) of Additional Protocol I, which reflects customary IHL.

30 *See*, Tallinn Manual, *supra* note 3, Commentary on Rule 39, para. 1.

31 *See*, Article 51(4) of Additional Protocol I, which reflects customary IHL.

32 *See*, Tallinn Manual, *supra* note 3, Chapter 7, in particular the Commentary on Rule 94.
33 *See, Id.,* Commentary on Rule 21. *See* also, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report of the 31st International Conference of the Red Cross and Red Crescent, 21-22 (Geneva, 28 November - 1 December 2011; report prepared by the International Committee of the Red Cross, October 2011).
34 *See*, Article 51(5)(b) of Additional Protocol I, which reflects customary IHL.
35 *See*, Article 57 of Additional Protocol I, which reflects customary IHL.
36 *See*, Article 58 of Additional Protocol I, which reflects customary IHL.
37 *See*, Article 57(1) of Additional Protocol I.
38 *See*, Article 57(2)(a)(i) of Additional Protocol I.
39 *See*, Article 57(2)(a)(ii) of Additional Protocol I.
40 *See*, Article 57(2)(b) of Additional Protocol I.
41 *See*, Droege, *supra* note 1, at 574.

The "Dubai Clash" at WCIT-12: Freedom of Information, Access Rights, and Cyber Security

Deborah Housen-Couriel

> *It is clear that the world community is at a crossroads in its collective view of the internet and of the most optimal environment for the flourishing of the internet in this century.*
>
> US Ambassador Terry Kramer, speaking at a press conference at the conclusion of WCIT-12 in Dubai, December 2012

Critical decisions regarding the future of the internet, or internets, are upon us. In his seminal book published in 2008, entitled *The Future of the Internet: And How to Stop It*, Professor Jonathan Zittrain of Harvard Law School laid out the core dilemma behind these decisions.[1] On the one hand, the ubiquity of the world wide web, the richness of its resources, and the ease of access and transmission of information it provides for 2.7 billion people – which Zittrain calls the "generative internet" – have been determined by the web's original chaotic and largely unregulated design.[2] On the other hand, governments and inter-governmental organizations have become deeply challenged by the internet's freewheeling, "wild west" nature, and the facility with which it is leveraged for illicit activities, including costly cybercrime, due to the absence of multilateral, normative frameworks.[3] In the name of increasing cyber security concerns, and lacking effective global agreement on legal and policy parameters, governments have begun to regulate both content and access on their own. This pattern is at best counterproductive,

Adv. Deborah Housen-Couriel is a Research Fellow at Tel Aviv University's Yuval Ne'eman Workshop for Science, Technology and Security.

and at worst harmful and disruptive, given the global interoperability and interdependence of the internet.[4]

Zittrain opposed any overall tendency by regulators to stifle internet innovation and freedom of expression by its users, even in the name of cyber security. He called for a latter-day Manhattan Project to take on the challenge of moving the internet into its next global phase without a regulatory lockdown that would, in his view, sacrifice the innovative edge that characterized its genesis and early development.[5] Summarizing the importance of ensuring that state and non-state shareholders alike engage in this project, he wrote:

> Traditional cyberlaw frameworks tend to see the Net as an intriguing force for chaos…the name of the game is seen to be coming up with the right law or policy…to address the issues…. Stopping this future depends on some wisely developed and implemented locks, along with new technologies and a community ethos that secures the keys to those locks among *groups with shared norms and a sense of public purpose, rather than in the hands of a single gatekeeping entity,* whether public or private.[6] (emphasis added)

One of the catalysts for moving into this new stage of internet governance will be, he argues, "a collective watershed security moment," when governments and non-governmental actors will be forced to confront the vulnerability of the internet's infrastructure and operational flexibility.[7]

That critical moment in fact occurred in December 2012 in Dubai, at an inter-governmental conference held under the auspices of the UN's International Telecommunication Union (ITU). The conference, known as WCIT-12,[8] dealt with the ongoing revision of a relatively technical treaty establishing the principles for global telecommunication infrastructure, called International Telecommunication Regulations (ITRs).[9] Originally relating to telegraphy and telephony, the ITRs now also underpin the interconnection of systems utilizing telecommunication infrastructure for internet traffic. They address the development of new services, promotion of broad public access, system interoperability, mobile roaming, accounting rates, and priority for safety-of-life communications. The technical connectedness among global telecom systems that we experience as relatively seamless use of mobile phones and the web depends on ITR provisions.[10]

Despite its ostensibly technical nature, the WCIT-12 conference became a flashpoint of controversy around the future of internet governance months before it convened in Dubai. Underlying this controversy was the ongoing debate among states regarding the problematic relationship between internet governance and cyber security. Two recent reports of the US Council on Foreign Relations highlight this tension: [11]

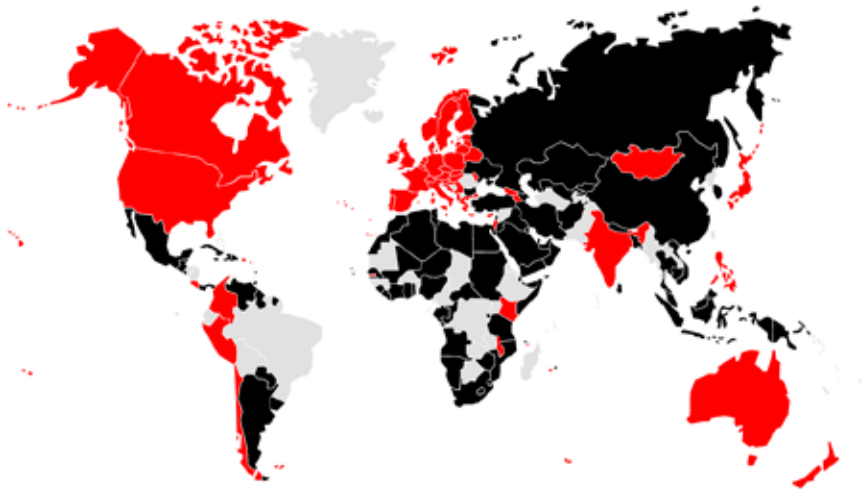
> Cyberspace is now an arena for strategic competition among states, and a growing number of actors – state and nonstate –use the Internet for conflict, espionage, and crime. Societies are becoming more vulnerable to widespread disruption as energy, transportation, communication, and other critical infrastructure are connected through computer networks. At the same time, the open, global Internet is at risk. Nations are reasserting sovereignty and territorializing cyberspace. The justifications are many – national security, economic interest, cultural sensitivity – but the outcome of blocking, filtering, and regulating is the same: a fragmented Internet and a decline in global free expression.[12]

While there is currently no accepted definition of "cyber security" in international law, many states, including Israel, emphasize the elements included in the ITU approach, which encompasses the totality of state and organizational behaviors that are designed to protect cyberspace and its users from harm to computer systems, data, and personnel.[13] The differences center on domestic law and policy considerations of what constitutes "harm." Although most would agree that threats to cyber security include cyber crime, cyber espionage, and cyber attacks, in the absence of coordinated, mutually-agreed international legal norms, at present each state determines the legality of cyber activity independently, exclusively in accordance with its domestic law.[14]

The WCIT-12 galvanized and polarized these differences of approach: on the one hand, that of the Western democracies and their allies, led by the US and the EU and including Israel; and on the other, that of regimes more restrictive of the freedoms of expression and access, led by China, Russia, and some Arab states. The former held that the status quo of a light-handed and multi-stakeholder approach regarding internet governance should be maintained, including non-state actors that have so far played a key part in

internet evolution. The latter approach advocated heavier regulation, with a greater role for state intervention in both internet traffic and content.

Figure 1 maps the voting patterns of ITU member states. The non-signatories, which amounted to 38 percent of conference participants, included the US, the EU, Canada, Japan, Australia, and Israel.[15]



■ – Signatories
■ – Non-signatories
■ – Countries not included in the ITU list

Figure 1. Voting Patterns among ITU Member States

Source: M. Masnick, *Who Signed the ITU WCIT Treaty…And Who Didn't*, Techdirt, December 14th, 2012

The end result was a sharp division between those countries that signed the ITR's 2012 revisions and those that refused to do so, remaining bound by the 1988 version of the ITRs. In rejecting the revisions, these countries dissented from what they perceived as a concerted project on the part of non-Western countries to inaugurate an interventionist and anti-democratic regulatory model of internet governance. The US State Department framed the clash in terms that echo Professor Zittrain's:

> We believe these provisions reflect an attempt by some governments to regulate the Internet and its content, potentially paving the way for abuse of power, censorship and repression…. We stand on one of our most cherished of principles, free

> expression, in not signing this treaty and seeking more positive outcomes in the future that support the open and innovative Internet. We believe an open Internet also is important for commercial growth in all parts of the world.[16]

The actual effect of the Dubai amendments to the ITRs on the future of internet operability and governance has yet to be seen.[17] Yet the perception by the US, Europe, and allied states that the China-Russia-India-Africa bloc was intent on preempting the future of the internet in ways hostile to democratic values polarized positions and led to the conference's conclusion in a legal and policy stalemate between countries supporting two different versions of the ITRs: the Melbourne 1988 version and the amended Dubai 2012 version. The clash at Dubai was Zittrain's "collective watershed security moment." It signaled to global decision-makers the high cost of what states believe to be at stake regarding the future of internet governance.

What follows is a review of the international legal and policy debate in the ITU that led up to WCIT-12, followed by an analysis of the legal issues of freedom of information on the internet and access to digitized information. The article then examines the Dubai Clash's ramifications for cyber security, and draws some conclusions regarding the steep normative, economic, and security costs of non-resolution of the present global debate around internet governance.

The International Debate around Internet Governance at the ITU

The revision of the ITRs prior to Dubai dates from 1988, when the internet had yet to become the economic, social, educational, political, and security phenomenon that it is today. The 1988 ITRs focused on then-relevant aspects of international telecommunications, such as interconnection routing and fees.[18] While the emergence of the web has changed international telecommunications in dramatic ways, these changes have taken place largely without intergovernmental regulation by bodies such as the ITU. On the contrary: development has moved ahead by involving a mix of non-governmental stakeholders focusing on the operational priorities through standards, communications protocols, and domain name management.[19] Organizations and extra-governmental groups such as ICANN,[20] the Internet Society,[21] and IETF[22] (MACHBA and the IIA in Israel)[23] have taken the lead

on rapid and overall effective resolution of these issues, technical in nature yet crucial to ensuring the open nature of web access. Perhaps predictably at the early stages, US-based bodies were dominant, largely supported by the EU[24] and other Western democracies, including Israel.

However, with the dramatic expansion of the internet over the two decades (*see* figure 2),[25] many states in the early twenty-first century began to express dissatisfaction with the multi-stakeholder governance model and the perception of US dominance. China and other developing countries first proposed an international treaty on internet governance in the months prior to the 2003 ITU World Summit on the Information Society (WSIS) held in Tunisia.[26] Disagreements among ITU member states advocating this new regime and those interested in maintaining the status quo (roughly the division later seen at WCIT-12) resulted in the matter being referred to the UN Secretary-General. He proceeded to establish a Working Group on Internet Governance (WGIG) in 2004, which in turn recommended the creation of an Internet Governance Forum as a non-binding intergovernmental forum for discussion on internet-related issues and internet governance.

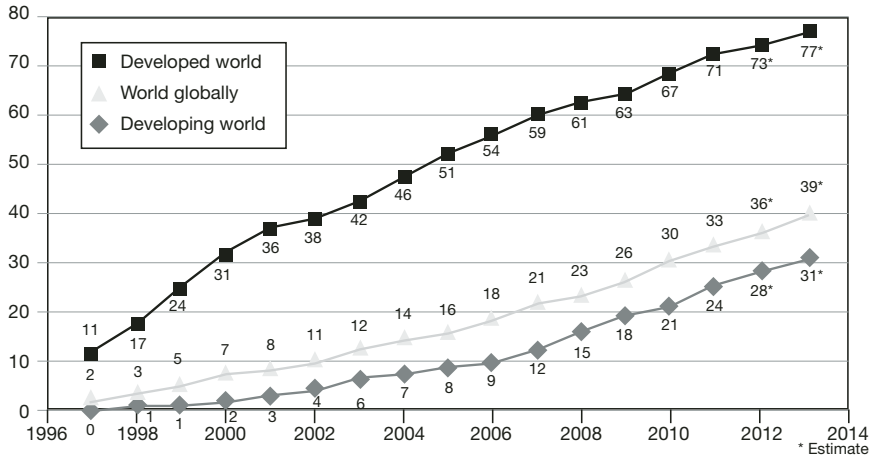


Figure 2. Internet Use

Source: ITU, *Internet Users per 100 Inhabitants 2006-2014* (May 2013)

Article 4 of the Tunis Declaration reached at the conclusion of the 2003 WSIS conference reflected a consensus regarding freedom of expression over the internet.[27] The article promotes freedom of trans-border expression and access to data embodied in Articles 19 and 20 of the Universal Declaration on Human Rights (reviewed in Section III below), and is important as a

substantive basis for internet governance discussions within the UN system. Indeed, it had ramifications at WCIT-12 as well, having been incorporated into the binding legal norms of the ITU.[28]

In light of the UN organizational initiatives and the dramatically-altered international telecommunication environment, the ITU decided in 2006 to convene WCIT-12. The stated goal was to adapt the ITRs to contemporary telecommunication realities, including vastly expanded global internet traffic. The road from the 2003 WSIS to the WCIT-12 is charted in figure 3.

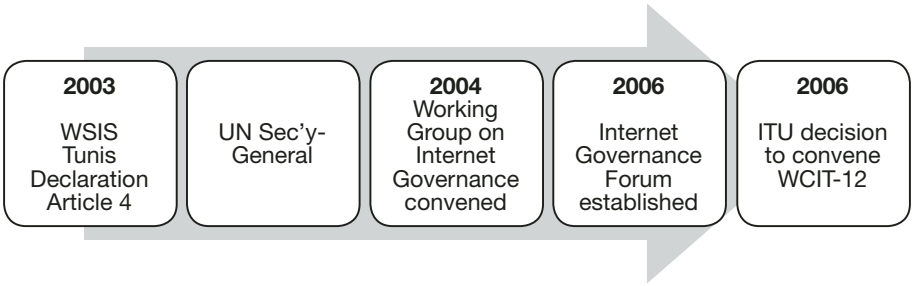


Figure 3. Selected Points of Engagement of the ITU and UN on Internet Governance

Prior to the conference, ITU Secretary-General Hamadoun Touré stated publicly that WCIT-12 would seek consensus around the technical issues with which the ITRs have traditionally dealt. Touré wanted to avoid earlier controversies at the WSIS and the WGIG around the governance conundrum, and to keep off the table the issues of freedom of speech on the internet and electronic access that had become so much more politically divisive since the 2003 Tunis Declaration. In particular, tensions were running high around the role played by the internet in the Arab Spring uprisings and other social unrest around the globe.[29] Yet delegates had already understood the inevitability of a clash at WCIT-12 between the opposing approaches that had come to the fore since Tunis, as controversial proposals were submitted in the months leading up to the conference.[30]

Freedom of Information on the Internet and Access to Digitized Information

Substantive Norms under General International Law

Domestic law reflects the internal balance that governments strike between the issues of freedom of information and access to data and other constraints

such as national security, privacy, and intellectual property rights. When communications cross state borders, international law considerations also become relevant, in particular, the right to receive and transmit information across national borders. This freedom is recognized in Article 19 of the Universal Declaration of Human Rights:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers.*[31] (emphasis added)

The evolution of the legal norm embodied in Article 19, the article of the same number in the 1966 International Covenant on Civil and Political Rights, along with similar provisions in several regional human rights treaties,[32] has an interesting history rooted in the nineteenth century concepts of democracy and freedom of expression in domestic legal systems.[33] While acknowledging that freedom of information emerged as a legal concept on the international level only in the second half of the twentieth century, Malancuk has noted that:

> From the very beginning, individual liberal constitutions have attached particular importance to freedom of opinion and expression, freedom of the press, and freedom of information of the individual in the sense of the right to receive, impart and seek information and ideas regardless of frontiers.[34]

The scope of freedom of information across national borders – and the enforcement of this provision – has waxed and waned in accordance with both technological developments and the state practice that reflects them. Debate remains among scholars regarding whether Article 19 embodies a customary norm of international law,[35] although the question of derivation of this right from international treaty law or customary law may, in the event, be largely moot, given the widespread accession of states to treaties containing an "Article 19" provision and the body of domestic and international jurisprudence surrounding it.[36] According to Mayer-Schonberger and Foster, "While speech has never enjoyed – and never will enjoy – absolute protection, the principle of freedom of speech has become part of a minimum standard of freedoms for the great majority of nations.[37]

Metzl has also argued convincingly that there is a "strong presumption" in international law supporting the international right to communicate, although it may have limitations in extreme circumstances such as the Rwanda radio broadcasts inciting to engage in genocide of the Tutsis in the early 1990s. He argues that these broadcast may have legitimately been jammed by other states, and that there may even be a duty to jam broadcasts that violate *jus cogens*, or in circumstances where the jamming can mitigate a humanitarian crisis.[38] This conclusion is supported by UN Charter Article 41, which permits the Security Council to call upon members to interrupt "postal, telegraphic, radio and other means of communication" as a response to a threat to peace, danger to peace or aggression.[39]

Extending the analysis above into the context of internet communication, freedom of information is codified at the international level as a technology-neutral right, although there are specific limitations on its scope due to illegal content, such as incitement of racism, child pornography, and the like.[40] In particular, freedom of information in cyberspace, as with other types of trans-border communication, may be limited by the international community for *jus cogens* considerations, such as the prevention of incitement to genocide.[41]

ITU Treaty Law

The ITU regime also provides a strong normative backbone for ensuring open and uninterrupted international communications. Trans-border freedom of information and access are supported by several principles of the ITU constitution that govern the global use of telecommunication infrastructures and resources.[42] The first is embodied in Article 33, prescribing the non-discriminatory use of communications infrastructure:

> Member States recognize the right of the public to correspond by means of the international service of public correspondence. The services, the charges and the safeguards shall be the same for all users in each category of correspondence without any priority or preference.[43]

This "public right" may be limited by the authority of states under Articles 34 and 35, which permit states to suspend ingoing and outgoing communications with respect to their own national territory, conditional upon public notification of stoppage or suspension.[44] This authority, stemming from a state's capacity

as a sovereign to control the flow of information domestically, does not extend beyond its borders.

Under Article 38, states are required to ensure optimal technical conditions for uninterrupted international telecommunications, and to refrain in particular from disrupting operations in other states. These constitutional principles are incorporated into Article 1 of the ITRs as follows:

> These Regulations establish general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the underlying international telecommunication transport means used to provide such services.[45]

Article 3 states that any user "has the right to send traffic," subject to domestic law. And under Article 4, "International telecommunication services," member States "shall promote the development of international telecommunication services and shall foster their availability to the public."[46]

In summary, trans-border freedom of expression, information, and access to data, as codified in Article 19 of the Universal Declaration of Human Rights and the ITU constitution, are broadly recognized principles of international law. In addition, ITU treaty law prescribes a free flow of information across borders at both the technical and substantive levels. Differences in interpretation and enforcement of these principles by countries relate to the types of content that are covered by them. They leave open the controversial issue of content regulation in trans-border communication, which was the basis for the clash of approaches at WCIT-12.

The Dubai Clash and Cyber Security

Internet Governance and Cyber Security

The breadth and depth of public interest in the Dubai conference marked a significant departure from ITR conferences of the past.[47] In the months leading up to WCIT-12 the unprecedented media attention included high profile op-eds in the *New York Times* and the *International Herald Tribune*,[48] a public protest by Google on its "Take Action" website,[49] a global petition to "Protect Global Internet Freedom,"[50] and a Wikileaks-style website publishing conference documents.[51] This activity was prompted by several conference proposals submitted by member states, perceived by the US, Europe, and their allies as threats to cyber security by their calling into

question the multi-stakeholder status quo and enhancing state sovereignty and discretion over internet infrastructure.[52] For instance, Russia proposed the addition of an ITR article providing an alternative to the current ICANN domain name scheme:

> Member States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of the basic Internet infrastructure.[53]

Other controversial proposals by China and the Arab bloc dealt with altering the financing model for internet communications (to a "sending party pays" model), adjusting network security, broadening the jurisdictional scope of the ITRs to include private operating agencies such as internet service providers, and blocking spam.[54]

The controversy around spam provides an example that is especially relevant to the freedom of speech and access issues around which much of the WCIT-12 debate pivoted. The new ITR Article 5B prohibiting spam states:

> Member States should endeavor to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services.[55]

Inclusion of the new article raises two questions: the first regarding the potentially *ultra vires* expansion of the scope of the ITRs to an issue that arises exclusively in the context of internet communications, rather than telecommunications as a whole. The second relates to the US-Europe perception that the blocking of spam by governments (and the decision of what constitutes spam) marks a slippery slope to internet content regulation.[56] While the domestic law of member states defines illicit content in accordance with each country's legal system irrespective of the ITRs, Article 5B is perceived by Western countries as providing superfluous and detrimental international legal cover for unwarranted content regulation.[57] The potential for abuse of power by states claiming to implement cyber security measures vis-à-vis spammers but in fact wanting to crack down on dissidents was understood by the US and its allies as a threat to freedom of communication

and digital access. A recent report by the Council on Foreign Relations summarized this normative tension at WCIT-12:

> Confronted with this challenge, the global community faces a dilemma. The neutrality of the Internet has proven to be a formidable ally of democracy, but the cost of protecting users' freedom is skyrocketing. Critical services, such as e-commerce or e-health, might never develop if users are not able to operate in a more secure environment. Moreover, some governments simply do not like ideas to circulate freely.[58]

Thus, while the Dubai ICT revisions may not constitute radical de facto changes in the present model of internet governance, the perception of Western democracies that basic values were undermined by their inclusion in international treaty law brought about the current stalemate.

Israel's Position at WCIT-12

The Israeli position at WCIT-12 regarding internet governance and cyber security remained squarely in the camp of the Western democracies. Its "Proposals for the Work of the Conference" took a position against any reform of the ITRs affecting the internet: [59]

> It is our strong belief that the existing global, transparent, multistakeholder, bottom-up model of Internet governance is effective and inclusive, and must remain in effect.
> Recognizing the immense contribution of the Internet to economic growth and to human welfare, as well as to the promotion of free speech and human rights, Israel shares the concern of many, that the development of this invaluable asset may only be hindered if it is brought under governmental or intergovernmental regulation.[60]

In addition to opposing future ITR provisions furthering global internet governance in any form, the Israeli proposal opposed the conference's adoption of any specific business or commercial model, mandatory telecom standards, any departure from technological neutrality, jurisdiction over spam, and the determination of any architectural preference pertaining to the internet.[61] The position regarding cyber security encompasses an especially

clear expression of Israeli governmental policy regarding its minimalist view of the scope of the ITRs, and refers to the Article 19 rights reviewed above:

> Cybersecurity is outside the purview of the ITU […]. We believe that any text in the ITRs related to security should be narrowly focused on international telecommunication networks, should not involve content or information security, should avoid topics related to law enforcement or national security, and should be fully consistent with Member State commitments under the UN Declaration on Human Rights.

Israel voted with the US-EU bloc at the conclusion of WCIT-12.[62]

Trends and Conclusions

In purely legal terms, the result of the Dubai Clash at WCIT-12 presents the anomaly of an international treaty that as of January 1, 2015 will be in force in two different versions for two groups of ITU member states. It is an open question whether this anomaly will prove to have significant impact on the ongoing functioning of the internet and the future of internet governance.

In any event, this situation constitutes serious evidence of the "Zittrain moment" that will determine the future structure of cyberspace. Will blocs of countries decide to cede from the open, unrestricted access of the present world wide web into their own virtual private networks (VPNs) with restricted content? Will a "grey internet" develop, providing access from these VPNs to illicit content for a price? Are we on the way to content tiering, with information of a higher quality available at steeper rates for those who can pay, or only data paid for by the wealthy being widely accessible, as hinted at in the current hearings on net neutrality in the US Court of Appeals for the District of Columbia?[63] As one observer wrote at the end of WCIT-12:

> The real story here is a world in which there are two competing visions for the future of the internet—one driven by countries who believe the internet should be more open and free—and one driven by the opposite. Whether or not the [ITRs are] ever meaningful or effective, these two visions of the internet are unlikely to go away any time soon.[64]

The global dilemma regarding the internet's future may not in fact have a successful resolution. At its heart are issues of state sovereignty over the

types of information that governments believe their citizens should by right be able to transmit and receive, in a global context of ever-increasing cyber security concerns. The requisite balance of information and access rights with security and law enforcement concerns has yet to be achieved within many countries, much less globally.[65] Perhaps the legal and policy vacuum exposed by the Dubai conference might only be effectively addressed, and potential damage mitigated, by a highly pragmatic and forward-looking initiative of major internet stakeholders, anchored in the steep normative, economic, and security costs of ongoing non-resolution. Specifically, in the absence of clarification of the normative parameters of internet governance for freedom of information and access, global cyber security will continue to be characterized by normative uncertainty and the absence of state and organizational responsibility for illicit behavior on the internet. The upcoming ITU Plenipotentiary Conference of all member states in 2014 in Busan, Korea will provide an important opportunity to make progress beyond the Dubai clash.

Notes

1 J. Zittrain, The Future of the Internet and How to Stop It (2008).

2 In Q2 2012, the site *Internet World Stats* showed 2,405,518,376 users (www.internetworldstats.com/stats).

3 See, for instance, Center for Strategic and International Studies, The Economic Impact of Cybercrime and Cyber Espionage (July 2013); observations on the US-China consultations on illegal uses of the internet (*Admit Nothing and Deny Everything*, The Economist, June 8th, 2013); and "Digital Wildfires" in World Economic Forum, Annual Report (2013).

4 *See* European Union, European Internet Security Strategy (April 2013): "Even if sovereignty considerations have become increasingly important, there is evidence that the participation to international cooperation or policy frameworks is positively related to the cyber security performance of a country; additionally, cyber-threats are not confined by administrative borders as network and information systems are globally interconnected." Lest we think that only non-Western, non-democratic governments engage in the regulation of internet access, it is worth noting the recent FCC hearings in Washington D.C. on access regulation. *See* E. Wyatt, *Verizon-F.C.C. Court Fight Takes On Regulating Net*, The New York Times, September 8th, 2013.

5 Zittrain and others have since focused on particular examples of this tension. In his 2011 book, Access Contested (J. Zittrain, R. Deibert, J. Palfrey and R. Rohozinsky, eds., 2011), he examines "the interplay of national security, social and ethnic identity, and resistance" in the context of internet regulation by Asian governments.

6 Zittrain, *supra* note 1, 5.
7 *Ibid*., 51.
8 Formally, the conference is named the *World Conference on International Telecommunications*.
9 WCIT convenes periodically as an intergovernmental conference under the auspices of the International Telecommunication Union (ITU), the UN specialized agency responsible for international communications infrastructures and development. *See generally,* A. Noll, *The ITU in the 21st Century*, 5 Singapore Journal of International and Comparative Law 63 (2001). See also the ITU website for the Final Acts of WCIT-12, December 14th, 2012, http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.
10 WCIT-12 Final Acts *, ibid*., at Article 1.3, "Purpose and Scope of the Regulations." A comprehensive explanation of the challenges of interoperability can be found in OECD, Communications Outlook 137-176 (2013), http://dx.doi.org/10.1787/comms_outlook-2013-en.
11 "The question becomes more urgent every day: Should the Internet remain an end-to-end, neutral environment, or should we sacrifice Internet freedom on the altar of enhanced security?" A. Renda, *Cybersecurity and Internet Governance*, Council on Foreign Relations, May 13th, 2013, http://www.cfr.org/cybersecurity/cybersecurity-internet-governance/p30621.
12 Defending an Open, Global, Secure, and Resilient Internet 67 (J. Negroponte and S. Palmisano, eds., 2013).
13 The operative definition was drafted by Study Group 17 of the ITU Telecommunication Sector: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation, Confidentiality." (ITU-T X.1205, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx). For Israel's definition, see *Government Decision No. 3611* of August 7, 2011. http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx.
14 The Council of Europe's Convention on Cybercrime is the one exception. Israel is presently in the process of accession (Convention on Cybercrime, 23 November, 2001, 185 CETS).
15 190 ITU Member States were party to the 1988 ITRs. For various procedural reasons, only 144 delegations had voting rights at WCIT-12. 89 states signed the revised ITRs (in black) and 55 did not (in red). In terms of population, the signatories represent 3.8 billion people, and the non-signatories 2.6 billion; *see* M. Masnick, *Who Signed the ITU WCIT Treaty…And Who Didn't*, Techdirt, December 14th, 2012.

16 Cited in W. Rash, *WCIT Treaty Talks End in Dubai With Walkout of U.S., Allies*, EWeek, December 15th, 2012, http://www.eweek.com/cloud/wcit-treaty-talks-end-iin-dubai-with-walkout-of-us-allies-2#sthash.mRAJCe98.dpuf.

17 Although the jury is still out on the final result of ITU member state ratification processes, which need to conclude by January 1, 2015 when the revised ITRs enter into force, some observers are skeptical that the amended ITRrs will have significant impact on internet operation. See M. Mueller, *ITU Phobia: Why WCIT was derailed*, Internet Governance Project, December 18th, 2012.

18 *See* International Telecommunication Regulations, Melbourne (1988), http://www.itu.int/pub/T-REG-ACT-1988.

19 D. Fidler, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, 17 ASIL Insights, February 7th, 2013.

20 ICANN is the Internet Corporation for Assigned Names and Numbers, famously incorporated in California as a non-profit public benefit corporation. For an example of challenge to ICANN's accountability, see D. Lindsay, *ICM Registry v. ICANN: Introductory Note*, 49 International Legal Materials 956, 956-1002 (2010).

21 The Internet Society is a Geneva-based non-profit (www.internetsociety.org). *See generally* the Internet Society 2012 Annual Report.

22 The Internet Engineering Task Force, *see* www.ietf.org.

23 MACHBA, or the Inter-University Computation Center (IUCC), is a non-profit organization established in 1984 by eight Israeli universities and is supported by the Council for Higher Education; the Israel Internet Association was established in 1994.

24 *See* European Parliament Resolution on the forthcoming World Conference on International Telecommunications (WCIT-2012) of the International Telecommunications Union, and the possible expansion of the scope of international telecommunication regulations (2012/2881(RSP), 20/11/2012); and C. Franzen, *European Parliament Adopts Resolution Vowing to Fight ITU Internet Regulation*, TPM IdeaLab, November 23rd, 2012.

25 In addition, according to Cisco's VNI Forecast, global IP traffic volume has grown eightfold over the period 2006-11.

26 *See, The Future of Internet Governance*, 101 Proceedings of the Annual Meeting of the American Society of International Law 201, 201-213 (March 28th-31st, 2007).

27 "We recognize that freedom of expression and the free flow of information, ideas, and knowledge, are essential for the Information Society and beneficial to development." (WSIS-05/TUNIS/DOC/7-E, 18, Article 4, November 2005).

28 The ITU Constitution and Convention set out substantive norms such as the public's right to trans-border communication (Constitution, Article 33) and states' responsibility for the maintenance of international infrastructures (Constitution, Article 38), www.itu.int/aboutitu/Basic_Text_ITU-e.pdf.

29 For a review of some of the tensions between Arab governments and their citizens regarding the use of the internet in mid-2012, see T. Pavel, *Continuing as Usual*, Makor Rishon 8, April 27th, 2012.

30 In an attempt to perhaps soften the divide, the head of the United States' delegation welcomed the increasingly non-Western character of the World Wide Web in a

December 13 interview, at the conclusion of the conference. *See* J. Crook, *United States Rejects International Telecommunications Union Conference Outcome, Fearing Interference with Internet Freedom,* in J. Crook, *Contemporary Practice of the United States Relating to International Law*, 107(2) American Journal of International Law 431 (2013).

31 UNGA 217 A (III) 1949. Article 29 potentially tempers the scope of Article 19 and other rights set forth in the Declaration by prescribing "respect for the rights and freedoms of others" and the requirement of "meeting the just requirements of morality, public order and the general welfare."

32 *See* Article 10 of the European Convention on Human Rights, 4 November 1950, E.T.S. No. 5; Article 9 of the African Charter on Human and Peoples' Rights, 26 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982); and Article 13 of the American Convention on Human Rights, 22 November 1969, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123.

33 See P. Malancuk, *Information and Communication, Freedom of*, in 9 Encyclopedia of International Law 148, (R. Bernhardt et al. eds., 1986).

34 *Ibid.*

35 Malancuk does not agree that an international custom has been established (*ibid*., 168).

36 *See, e.g.*, Autronic AG v. Switzerland, 22 May 1990, ECHR, Application No. 12726/87; Khursid et al v. Sweden, 16 December 2008, ECHR, Application no. 23883/06; and *Satellite jamming and freedom of expression*, statement of Article 19 organization regarding the jamming of LuaLua TV in Bahrain, 21 November 2011, http://www.bahrainrights.org/en/node/4855.

37 *See* V. Mayer-Schonberger and T. Foster, *A Regulatory Web: Free Speech and the Global Information Infrastructure*, in Borders in Cyberspace 243 (B. Kahin and C. Nesson eds., 1999).

38 Mayer-Schonberger and Foster also advocate a *jus cogens* approach *(ibid.). See also* Prosecutor v. Ferdinand Nahimana et al*,* Case No. ICTR -99-52-T (3 December 2003).

39 The article states: 'The Security Council may ... call upon the Members of the United Nations to apply such measures [as] complete or partial interruption of ...postal, telegraphic, radio, and other means of communication....' , Article 41, Charter of the United Nations, 26 June, 1945, 1 UNTS 14.

40 See the Additional Protocol to the Convention on Cybercrime (28 January 2003, CETS 189) concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems: Council of Europe, 2003. Some jurists have proposed that a *jus cogens* approach to prohibited content on the internet may lead the way to resolution of the current impasse.

41 Prosecutor v. Ferdinand Nahimana et al, *supra* note 39.

42 For discussion of the customary elements of the ITU regime, see P. Malancuk, *Telecommunications*, *International Regulation*, in 9 Encyclopedia of Public International Law 367 (R. Bernhardt et al., eds., 1986).

43 ITU Constitution, *supra* note 29, at Article 33.

44 They are respectively entitled 'Stoppage of Telecommunications' and 'Suspension of Services', ITU Constitution, *ibid.,* note 29.

45 Article 1, Purpose and scope of the Regulations, *supra* note 9.
46 *Ibid.*
47 WCIT convenes periodically as an intergovernmental conference under the auspices of the International Telecommunication Union (ITU), the UN specialized agency responsible for international communications infrastructures and development. On the ITU in general, see A. Noll, *The ITU in the 21st Century*, 5 Singapore Journal of International and Comparative Law 63 (2001).
48 V. Cerf, *Keep the Internet Open*, The New York Times, May 24th, 2012; and *Global Internet Diplomacy*, The International Herald Tribune, December 12th, 2012.
49 *Google attacks UN's internet treaty conference*, BBC News, November 21st, 2012.
50 The petition stated: "Internet governance decisions should be made in a transparent manner with genuine stakeholder participation from civil society, governments and the private sector. We call on the ITU and its member states to embrace transparency and reject any proposals that might expand ITU authority to areas of internet governance that threaten the exercise of human rights online."
51 The site is WCITleaks.org. Although the conference materials were not confidential, access was limited by the need for registration and a password.
52 *Supra* note 12.
53 Russian Federation, *Proposals for the Work of the Conference*, Document 27, WCIT-12, 17 November 2012, Article 31B.
54 For a full review of the relevant provisions, see Fidler, *supra* note 19. He focuses on the revised Preamble, the addition to Article 1, the revision of Article 1.1, new Articles 5A and 5B, and Resolution 3.
55 WCIT Final Acts, *supra* note 9.
56 Fidler, *supra* note 19.
57 *Ibid.*
58 A. Renda, *supra* note 11.
59 Israel (State of), *Proposals for the Work of the Conference*, Document 28, World Conference on International Telecommunications, 19 November 2012.
60 *Ibid.* Despite the final paragraph quoted here, Israel does in fact regulate the internet, as do the US, the EU and other countries that opposed the adoption of the WCIT-12 Final Acts. The divisive issue is international, not domestic, regulation of the web.
61 *Ibid.*, at I and II.
62 See also the Ministry of Communication's recent notice regarding the Telecom Network Neutrality Bill, which passed its first Knesset reading on October 28, 2013, http://www.moc.gov.il/sip_storage/FILES/5/3355.pdf.
63 See the current US hearings around internet tiering, E. Wyatt, *Judges Hear Arguments on Rules for Internet*, The New York Times, September 10th, 2013, at B1.
64 *Supra* note 15.
65 Melissa Hathaway has recently lamented the plethora of international bodies now engaged with these issues, in her words an "operational collision" of competing interests that are stifling any progress that might be made. (M. Hathaway, *Change the Conversation, Change the Venue and Change Our Future*, Harvard Kennedy School Belfer Center, May 13th, 2013, http://www.technologyandpolicy.org/2013/05/14/change-the-conversation-change-the-venue-and-change-our-future/#.UnuDkXC9klk).

Protecting Offshore Drilling Platforms against Terrorist Attacks: The Legal Perspective

Assaf Harel

The discovery of natural gas in the eastern basin of the Mediterranean Sea is good news for Israel. The gas is expected to satisfy Israel's energy needs for many years, and export to other states is expected to yield significant tax revenues. It is therefore generally said that the infrastructure for drilling natural gas and transporting it to Israel's shores, mainly drilling platforms, constitutes a strategic asset for Israel.

Joining the opportunities created by the discovery of gas deposits at sea and the possibilities generated by their extraction are significant security risks to the drilling platforms. These platforms are located mid-sea, far from Israel's coasts (some over 100 kilometers), and are liable to become a target for terrorist attacks. Beyond the loss of human life (the platforms are manned by dozens of workers), such an attack may have serious consequences for the state. In economic terms, for example, rebuilding a damaged platform can cost hundreds of millions of dollars.[1] An interruption in gas pumping until the infrastructure is rebuilt also incurs a heavy economic loss. Moreover, an attack of this sort may likewise have harsh strategic consequences: it is capable of having a severe impact on the supply of energy to Israel, given the reliance on natural gas for energy production that is expected to increase with time.

Major Assaf Harel is a senior legal advisor in the Israel Defense Forces' Military Advocate General's Corps. The opinions in this article are those of the author and do not necessarily reflect the opinions of the IDF, the Israeli Ministry of Defense, or the State of Israel. This article is partially based on a comprehensive study published by the author – Assaf Harel, *Preventing Terrorist Attacks on Offshore Platforms: Do States Have Sufficient Legal Tools?*, 4 Harvard National Security Journal 131 (2012).

The challenges Israel faces in protecting the platforms are not only a function of the platforms' distance from Israel's shores. They also result from the fact that the platforms are located in a region where Israel's authority under international law is limited – mostly restricted to the right to exploit natural resources. This is not the same sovereignty that Israel enjoys over its territorial waters. For example, as a general rule, navigation and overflight cannot be restricted, ships passing through the area cannot be required to identify themselves, and so forth. This situation poses a significant challenge to Israel's security forces, particularly in scenarios in which there is a general threat to the platforms but no previous intelligence exists concerning the involvement of a specific vessel in hostile activity.

There is an extensive variety of threats to the platforms, among them, shore-to-sea missiles, unmanned aerial vehicles, and undersea sabotage operations.[2] In addition to the drilling platforms themselves, there are also threats to the accompanying infrastructure, such as undersea pipes, auxiliary vessels, and more.[3] The analysis that follows focuses on the threat to drilling platforms from hostile vessels, but the principles that it outlines are relevant to dealing with a broad range of threats.

This article assesses the authority under international law for protecting the drilling platforms against terrorist attacks. It first reviews the relevant legal framework and defines the basic terms required for a legal analysis of the question of authority. It then analyzes the legal tools available to Israel for handling definite threats as well as for coping with general threats that are not based on concrete intelligence information. Finally, the article proposes solutions under the existing legal framework. The article deals with the threat under international law, and does not analyze aspects of internal Israeli law that may arise, for instance, regarding the division of responsibility between the government and the private companies operating the platforms, for the security of the platforms.

The Legal Framework

The authority to deal with threats to offshore drilling platforms is derived from three branches of international law: the law of the sea, the law of self-defense, and the law of naval warfare.

The Law of the Sea

The law of the sea broadly regulates the legal rights and duties of states at sea. These laws, which are partly based on old practices, are anchored today in customary international law[4] and in a number of international treaties, the most important of which is the 1982 United Nations Convention on the Law of the Sea (UNCLOS).[5] Israel is not a party to UNCLOS, but it is widely accepted that many of the rules set forth in the convention are customary rules binding on all states.[6]

The law of the sea establishes two basic principles relevant to the subject at hand. The first is flag state jurisdiction. Under this principle, a vessel is considered subject to the sovereignty of the state in which it is registered (the flag state). The flag state has exclusive jurisdiction over vessels flying its flag, except in specific cases explicitly addressed in UNCLOS. Therefore, in general, only the flag state is authorized to exercise sovereign authority over its vessels. The second principle is freedom of navigation. Under this principle, vessels of all states enjoy complete freedom of movement on the high seas. A breach of freedom of navigation is only allowed under one of the exceptions recognized under international law. Violating freedom of navigation without the express authority of international law and without the consent of the flag state would generally be considered a violation of the flag state's sovereignty.

In many cases, freedom of navigation may conflict with a state's security needs. For example, due to such needs a state may wish to interdict a vessel on the high seas, or to restrict navigation in areas where its strategic assets – such as drilling platforms – are located. Beyond the legal duty to respect freedom of navigation, the principle is extremely important even from a utilitarian perspective. Erosion of this principle is liable to have grave strategic and economic consequences, especially for states such as Israel whose navigation routes are near states with hostile interests.

Based on these general principles, the law of the sea grants various rights to states, depending on the geographic area involved. Several maritime zones are relevant to this discussion.

The *territorial sea* of a state extends 12 nautical miles from its shores. A state has broad sovereign authority in its territorial sea, including the right to impose restrictions on navigation for reasons of security and safety. Nevertheless, a state is obligated to allow "innocent passage" of foreign

vessels through its territorial sea, meaning passage that "is not prejudicial to the peace, good order or security of the coastal state."[7]

The *exclusive economic zone* (EEZ) of a state is the area adjacent to its territorial sea, extending to 200 miles from its shore. States with adjacent exclusive economic zones are required to delineate the borders of these areas through an agreement. In its EEZ, a state has the exclusive right to exploit the natural resources of the seabed, subsoil and waters, as well as the exclusive right to conduct marine scientific research. Under this right, the coastal state has the exclusive authority to establish and allow the establishment of drilling platforms for the production of oil and gas.

The sovereignty of the coastal state in its EEZ, however, is confined to the exploitation of natural resources and the conduct of marine scientific research. Thus, for example, vessels and aircraft from all states enjoy freedom of navigation and overflight in an EEZ. Article 56 of UNCLOS states that the coastal state and other states shall have "due regard" for the rights of one another. When navigating in the EEZ of another state, a vessel is subject to the sovereignty of its flag state, except for select aspects involving the exclusive rights of the coastal state in its EEZ, such as the exercise of enforcement jurisdiction over fishing. Israel has never explicitly declared an EEZ, but in July 2011 it deposited coordinates with the UN for the delimitation of the northern border of its EEZ, following an agreement between Israel and Cyprus on the delimitation of the EEZ in the area.[8]

Another maritime zone is the *continental shelf*. This area extends to the edge of the continental margin,[9] or 200 nautical miles from the shore (whichever is greater). As with the EEZ (which in most cases overlaps this area), within its continental shelf, the coastal state enjoys exclusive authority to exploit the natural resources of the seabed and subsoil. Vessels and aircraft also enjoy freedom of navigation and overflight in this region. In contrast with the EEZ, however, the rights within the continental shelf do not apply to fishing. The discussion below on the authority to protect platforms in the EEZ is also valid for the continental shelf.

The *high seas* are a zone comprising all the maritime areas that are neither within an EEZ nor within the territorial sea of any state. In this region, all states enjoy freedom of navigation and freedom of overflight. Vessels on the high seas are subject to the exclusive jurisdiction of the flag state.

The Law of Self-Defense

The right to self-defense, enshrined in Article 51 of the UN Charter, allows a state to use force in response to an armed attack against it. This authority constitutes an exception to the general ban on the use of force between states, set forth in Article 2(4) of the UN Charter. Although the doctrine of self-defense traditionally dealt with force in response to an attack launched by a state, state practice over the past decades shows that the right of self-defense can also be used to justify a response to an armed attack launched by non-state actors, including terrorist organizations. Furthermore, although some assert that the authors of Article 51 intended to regulate the response of a state to an attack against it after the attack has already taken place, international law today seems to also recognize the right of a state to use force in order to prevent an anticipated attack against it.

The lawful use of force under the right of self-defense must satisfy three criteria: necessity, proportionality, and imminence. According to the necessity criterion, the use of means other than force to thwart an attack must be attempted, insofar as such measures are possible under the circumstances. Under proportionality,[10] the force used should be limited to what is necessary under the circumstances to thwart the attack or prevent additional attacks. Finally, imminence applies to threats that have not yet been carried out. Under this criterion, force may be used only to foil an attack expected in the near future.[11]

The Law of Naval Warfare

The law of naval warfare regulates the rights and duties of states conducting naval operations in the context of an armed conflict. These laws developed mainly in customary international law and are not part of any official binding international treaty. Many of the customary rules in this area, together with innovations and current trends, are gathered in the 1994 San Remo Manual on International Law Applicable to Armed Conflicts at Sea.[12] It should be noted that while the law of naval warfare was developed largely in the context of international armed conflicts (i.e., between states), it nevertheless can be relied on as a source of authority for actions carried out by a state in an armed conflict with a non-state actor such as a terrorist group.[13]

A state that is engaged in an armed conflict is authorized to impose certain restrictions on navigation that cannot be legally imposed during peacetime, and to use force against vessels that violate these rules. Since October 2000,

Israel has been engaged in an armed conflict against Palestinian terrorist organizations, first and foremost Hamas,[14] and has taken measures under the framework of the law of naval warfare in the context of this conflict.[15] It seems fair to determine that Israel is also engaged in an ongoing armed conflict with Hizbollah.[16]

Confronting Concrete Threats

Israel has extensive authority to deal with a scenario in which it identifies a specific vessel that is planning an attack against its drilling platforms. Such identification is likely to be based on prior intelligence or detection of a vessel's hostile intent and the means of executing it (for example, identification of weaponry on a ship behaving in a threatening manner in the proximity of the platforms). In such situations, under the law of the sea, Israel can contact the vessel's flag state and ask the latter state to exercise its authority over the vessel in order to thwart the attack. However, the legal solution to such threats, which ordinarily necessitate a quick response, lies mainly in the law of self-defense and the law of naval warfare.

According to the law of self-defense, Israel is entitled to use force against a vessel posing a definite threat to its platforms. In order to take action against it, Israel must determine that there is an intention to use the vessel for an attack on the platforms in the near future. In addition, Israel must employ means other than force to prevent the attack, insofar as such measures are possible in the circumstances at hand. One example of such a measure is an appeal to the flag state or the state from whose port[17] the vessel is bound to set sail, asking that state to exert its authority to foil the attack (for example, by preventing the vessel from leaving the port). If force is eventually used against the vessel, it must conform to the principle of proportionality. For example, the threat would preferably be removed by seizing the threatening vessel, rather than attacking it, provided that this does not pose a significant risk to the forces.

The law of naval warfare is likely to provide Israel with even more extensive authority with respect to a vessel belonging to a party with which Israel is in armed conflict (for example, Hamas or Hizbollah). Under the law of naval warfare, a vessel bearing military characteristics and belonging to such a party will usually constitute a military objective.[18] Israel is therefore entitled to attack such a vessel in order to remove the threat.

As a rule, the use of force against a vessel, whether under self-defense law or under the law of naval warfare, should take place outside the territorial waters of neutral states (i.e., states not party to the conflict) in order to avoid a breach of their sovereignty. Additionally, a precondition for attacking a ship is the existence of reliable information about its involvement in hostile actions. Israel must also take steps to reduce the expected collateral damage to civilians or civilian objects caused by the attack, and refrain from attacking when the anticipated collateral damage is excessive in comparison with the military advantage expected from the attack.

Thus it appears that dealing with vessels when well-established information exists concerning their intention to attack drilling platforms does not involve significant legal challenges. Israel possesses relatively broad authority to take action to remove such threats, based on the law of self-defense or the law of naval warfare. General threats, however, pose a far greater challenge.

The Principal Challenge: Defense against the General Threat

The routine protection of platforms from general threats that cannot be tied to a concrete vessel creates a substantial challenge, in part due to the restrictions imposed on the authority of the coastal state in its EEZ.

Creating Safety Zones around the Platforms under the Law of the Sea

The law of the sea grants a state the authority to establish "safety zones" around its drilling platforms located in the EEZ, and to employ "appropriate measures" to ensure the safety of the platform and the ships navigating in the area. The difficulty in relying on these safety zones for protection of the platforms against terrorist attacks lies in the breadth of the zones: as a rule, under Article 60(5) of UNCLOS, the width of such a safety zone cannot exceed 500 meters. This restriction greatly curtails the possibility of effectively dealing with terrorist threats against the platforms.

Both the authority to declare safety zones around platforms and the restrictions on their width were first set out in the 1958 Convention on the Continental Shelf.[19] Research into the process that led to the formulation of this treaty indicates that the choice of a 500-meter limit was quite arbitrary: this restriction was derived from the prevailing national standards at the time for the protection of land-based oil drilling facilities against fires.[20] In other words, the drafters of the treaty were not thinking about the security risks involved in the operation of platforms in an area traversed by vessels

of varying speed and size, let alone the danger to drilling platforms posed by maritime terrorism – a threat that developed several decades after the treaty was formulated.

The question of the width of the safety zones surrounding the platforms was discussed during the negotiations on UNCLOS in the 1970s. Some states asserted that 500 meters was inadequate for dealing with the modern security risks facing the drilling platforms – mainly the fear that large, fast ships would collide with the platforms. These states proposed that rather than stipulate a maximum radius of 500 meters, the treaty should grant the coastal state discretion in determining the breadth of the safety zones, subject to reasonableness. However, concern that granting discretion in this matter would open the door to exploitation and in practice lead to the imposition of broad restrictions on freedom of navigation in EEZs led to the adoption of the 500-meter limit in UNCLOS as well.[21] Nevertheless, in order to meet the concerns raised about the ability to prevent accidents using 500-meter safety zones, the treaty left the door open to setting larger safety zones, provided it was recommended[22] by the International Maritime Organization (IMO).[23]

Since UNCLOS entered into force, a number of states have asked the IMO to approve safety zones wider than 500 meters. A key example is the submission by Brazil in 2007. As part of its request, Brazil demonstrated that routine loading and unloading of oil from drilling platforms (during which a tanker is connected to a platform) requires an operating space of 1,400 meters. According to Brazil, a safety zone with a width of 1-2 nautical miles could help significantly reduce concern about vessels colliding with the platforms.[24] This request, however, like similar requests submitted to the IMO, was rejected by the organization under the general argument that the organization was not convinced of the need to establish broader safety zones.[25]

It appears that this decision was based on the same concern that prevented the expansion of the safety zones during the UNCLOS negotiations – fear of a loophole that would lead to the imposition of severe restrictions on freedom of navigation in EEZs. The IMO discussions on this issue dealt solely with the safety question. A request to the IMO to enlarge the safety zones for security reasons, such as prevention of terrorism, would likely encounter even more difficulties, given the political considerations that are, as a general rule, involved in deciding international issues of this type.

It is clear that safety zones of only 500 meters do not provide the solution needed for the protection of drilling platforms against terrorist attacks, such as a collision with a boat mounted with explosives. To illustrate this problem, it should be borne in mind that a vessel traveling at 25 knots (about 46 kilometers per hour) will cross such a safety zone within 40 seconds, leaving security personnel on the platform an extremely brief window of time, to say the least, within which to remove the threat. Furthermore, the weaponry currently possessed by terrorist organizations, such as anti-tank missiles,[26] makes it possible to attack a platform from a distance of over 500 meters without even penetrating the safety zone.

The law of the sea, therefore, does not provide an effective solution to the problem of terrorist threats to the platforms. With this in mind, the authority to restrict navigation in the proximity of platforms under the law of self-defense and the law of naval warfare must be considered.

Restrictions on Navigation in the Proximity of Platforms under the Law of Self Defense and the Law of Armed Conflict

General

When a vessel nearing a drilling platform is identified and there is definite information that its operators intend to attack the platform in the near future, proportionate force may be used to remove the threat. In reality, however, the security forces will not always have prior information of a vessel's hostile intent. In order to prevent such attacks, it is therefore important to identify the threat as early as possible.

As will be demonstrated below, the law of self-defense and the law of naval warfare may allow the imposition of restrictions on navigation more than 500 meters away from the platforms in order to increase the response time and improve the ability to counter threats to the platforms. Measures of this type, however, can only be taken for short periods of time, and only in relatively extreme circumstances of hostilities or in the face of an imminent threat. In exercising authority of this type, operations in the territorial waters of neutral states should be avoided, and the effect of this activity on the freedom of navigation of foreign vessels should be reduced to the minimum. The fact that the exercise of this authority is liable to arouse international criticism on the grounds of excessive interference with the freedom of

navigation, even if exercised in compliance with the rules, should also be taken into account.

Warning of an expected attack on platforms

Self-defense law confers the authority to temporarily restrict navigation beyond the 500-meter range in a scenario where there is an established warning of an imminent attack against the platforms. These measures are aimed at making it possible to identify a hostile vessel at a relatively early stage, so that the attack can be thwarted.[27] Such restrictions may, for example, take the form of a general ban on navigation within a range of a few miles from the platforms, making entry into the area conditional on compliance with a security check, and so on. Nevertheless, use of this authority requires satisfaction of the criteria applicable to actions in self-defense (discussed above).

First, the threat at hand must be imminent. Such restrictions can therefore only be imposed temporarily. Second, the restrictions imposed in the proximity of the platforms and the means used to enforce them must fulfill the principle of necessity. For example, if it is possible to settle for making entry into the relevant area conditional on a security check, instead of preventing entry altogether, this should be preferred. Furthermore, before using force against a vessel suspected of violating the restrictions, security forces should exhaust the non-forceful means available to them, such as effective advance warning and warning shots into the air.

Third, the measures taken must be reasonably related to the threat they are designed to meet. For example, a state should limit the area in which restrictions are imposed to the essential minimum. Similarly, force used against a specific vessel in order to impose the restrictions must be gradual and proportional in relation to the threat posed by the vessel. Finally, advance notice of restrictions of this type should be given to all the parties liable to be affected by them, including the states in the region, port authorities, and vessels traveling in the area.[28]

Another way of coping with a general warning regarding an expected attack on the platforms is through the authority to conduct a "visit and search" on suspicious vessels – an authority originating in the law of naval warfare. Israel may exercise this authority against a vessel when, for example, there are reasonable grounds for suspecting that it is operated by a party to an armed conflict with Israel (such as Hamas or Hizbollah). When such a

vessel is spotted it may be stopped for the purpose of conducting a search onboard. This authority may be exercised at a considerable distance from the platforms, provided this occurs outside the territorial waters of neutral states.[29] If a suspicious vessel resists the implementation of this authority, reasonable force may be used in order to enforce compliance.

In essence this means that the more limited the measures that a state takes, in time and space, and the better founded and more imminent the threat they are designed to meet, the better the chances of proving that the imposition of restrictions and the degree of force used to enforce them are legal. In this context, the difficulty of subsequently justifying the use of force against a vessel in breach of the restrictions, if it turns out that it was not involved in hostile acts, should be taken into account. In such scenarios, the state would generally be required to prove to the international community that it had indeed perceived a real and imminent threat, and that the means employed met the requirements of necessity and proportionality. Proving such a claim is likely to be difficult given the complications involved in revealing the intelligence on which such warnings are typically based.

Restricting navigation in areas in which naval operations are taking place

The law of naval warfare provides a state with the power to impose additional restrictions on navigation in the proximity of drilling platforms. One option is to declare an "exclusion zone" – an area of the sea in which a party to an armed conflict is authorized to prevent the entry of vessels due to military necessity. Whether an authority to declare exclusion zones exists nowadays is a controversial matter among international legal scholars.[30] Nevertheless, the San Remo Manual recognizes the legality of this measure "as an exceptional measure."[31] According to the Manual, a party to an armed conflict that declares an exclusion zone is authorized to take enforcement actions against vessels that act in breach of the restrictions on navigation in the zone.[32] A prominent example of the use of this authority is the UK's declaration of a 200 nautical mile exclusion zone around the Falkland Islands during the conflict between the UK and Argentina in 1982. The international community's response to this measure was rather mild.[33]

The declaration of an exclusion zone is subject to a number of conditions. First, the size of the zone, its location, duration, and the means of enforcement must be in reasonable proportion to the military necessity for which the zone is declared. Proportionate force may be used in order to enforce the

restrictions, yet unauthorized access in itself would not constitute grounds for attacking a vessel. Second, neutral states should be notified of the zone's commencement, duration, location, its dimensions, and the means used to enforce it. Third, safe access should be provided to the ports of neutral states. In addition, due regard must be given to the rights of these states, in particular freedom of navigation.

In any event, the legality of exclusion zones in international law is a controversial matter. Therefore, it appears that only circumstances of active and significant hostilities would justify the use of such authority.

Aside from declaring exclusion zones, a state is also entitled to impose restrictions on navigation in a zone in which naval operations are taking place, i.e., an area of hostilities or one in which the belligerent forces are actually operating.[34] Insofar as a vessel is in breach of these restrictions, proportionate force may be used to detain it, providing that the restrictions were not set arbitrarily. For example, to the extent that the Israel Defense Forces must carry out naval operations in the proximity of the platforms, restrictions may be imposed on navigation around them. In this context, operational activity designed to protect the drilling platforms against attack when hostilities are taking place may in itself justify the imposition of restrictions on navigation under this authority.[35]

Restrictions under the law of self-defense and the law of naval warfare: The bottom line

The law of naval warfare and the law of self-defense are likely to provide additional legal tools for protecting offshore platforms against terrorist attacks – but these tools are limited and are mainly practical for dealing with scenarios in which warning of an attack has been received or when actual hostilities affecting the vicinity of the platforms is ongoing or underway. These sources of authority do not provide a genuine solution for the routine task of guarding the platforms in the absence of such warning or of hostilities in the vicinity.

Possible Solutions

Israel is not the only state facing the challenge of protecting drilling platforms against terrorist attacks. A complete legal solution to this threat will require international cooperation in amending UNCLOS to enable the establishment of safety zones greater than 500 meters, or at least the formulation of IMO

recommendations that will permit the extension the safety zones. Since such solutions are not expected to be achieved in the foreseeable future, states such as Israel will have to find practical solutions for protecting their platforms, considering their limited ability, under international law, to interfere with navigation in areas beyond a 500-meter radius from the platforms.

In addition to technological means for prior identification of threats, "soft" tactics may be employed to assess the potential risk posed by vessels navigating in the vicinity of the platforms. One example is requesting information from vessels coming within a certain distance of the platforms.[36] As part of this questioning, which may be conducted via radio from ships, aircraft, or the platforms themselves, the vessel would be asked to provide information that will make it possible to determine the potential level of threat that it poses. For example, this information may include the vessel's port of origin and destination, ports it has recently visited, its planned course, the identity of its crew members, and so forth.[37] The information provided during the questioning may be verified using information available from other sources, such as automatic systems installed on a vessel (for example, AIS and LRIT).[38] In addition, the information may be verified by contacting the vessel's flag state or the port and destination states, insofar as time allows. Based on the information obtained from the vessel or its willingness to cooperate with the questioning, the level of potential threat may be estimated, allowing security forces to determine whether the vessel's activity requires special attention (e.g., tracking or a higher alert on the platform).

Similarly, a state may establish "warning zones" of several nautical miles around its platforms and issue a recommendation to vessels to refrain from entering those zones.[39] A vessel that nevertheless enters a warning zone will be questioned along the lines described above.

A vessel's refusal to comply with such warnings or its unwillingness to cooperate with questioning may not by itself constitute grounds for restricting its freedom of navigation. Assuming, however, that operators of civilian vessels would usually have no reason to refuse to cooperate with questioning, this method is likely to make it easier for a state to identify potential threats in advance.

The use of questioning methods and the establishment of warning zones may contribute to the ability to identify threats in the vicinity of offshore platforms. Nevertheless, without cooperation between states on the issue, the effectiveness of such means is liable to erode with time. A mechanism

for international cooperation in this context – for example, an international treaty obligating ships to provide the coastal state with information when approaching its drilling platforms – could upgrade the effectiveness of these means. Additionally, guidelines for rapid cooperation between the coastal state and the flag state when dealing with noncompliant vessels should be established in the framework of such a treaty. Such rapid cooperation may, for example, provide the coastal state with the flag state's consent to stop and search the noncompliant vessel. Promoting mechanisms of this type is liable to prove a difficult task, yet far easier than obtaining international agreement on the extension of safety zones around drilling platforms.

Conclusion

Protecting offshore drilling platforms poses a significant challenge to Israel. Dealing with this challenge is influenced to a large extent by the legal limitations on coastal state authority in the EEZ, where the platforms are located.

When a state possesses well-founded information about a vessel's intent to attack a drilling platform, it enjoys relatively broad authority to take action to remove the threat under the law of self-defense or the law of naval warfare. However, dealing with general threats that are not based on specific intelligence information poses a far greater challenge. While the law of the sea gives a state the authority to restrict entry to safety zones surrounding the platforms, the maximum breadth of those zones is limited to 500 meters from the platform, a distance that does not allow security forces ample response time to remove threats.

The law of self-defense and the law of naval warfare may allow the imposition of restrictions on navigation beyond the 500-meter range for the purpose of increasing the response time and improving the ability to thwart threats to the platforms. The tools provided by these laws, however, are limited and are mainly suitable for addressing scenarios in which there is a warning about an imminent attack, or when actual hostilities are taking place in the vicinity of the platforms. These sources of authority do not provide a genuine solution to the routine task of securing the platforms in the absence of warning or naval operations in the area.

Israel is not the only state to encounter the challenge of protecting drilling platforms against terrorist attacks. A comprehensive legal solution to this threat will require international cooperation in amending UNCLOS to

enable the establishment of safety zones wider than 500 meters, or at least the formulation of IMO recommendations that broaden safety zones. Since such solutions are not expected to be achieved in the foreseeable future, states like Israel will have to find practical solutions for protecting their platforms considering their limited ability, under the law, to interfere with navigation in areas beyond a 500-meter range of the platforms.

The use of "soft" defensive tactics, such as questioning vessels in the proximity of the platforms and establishing "warning zones," may contribute to the ability to spot threats in advance. Nevertheless, without cooperation between states, the effectiveness of these means is liable to erode with time. A mechanism for international cooperation could significantly improve the effectiveness of these methods. While promoting mechanisms of this type is liable to prove a difficult task, it will certainly be easier than attempting to obtain international agreement on the enlargement of safety zones surrounding offshore drilling platforms.

Notes

1 Amiram Barkat, *The State Will Pay Compensation for Drilling Platforms Damaged in Hostile Operations*, Globes, February 25th, 2013, http://www.globes.co.il/news/article.aspx?did=1000825022.

2 Lecture by Brigadier General (res.) Noam Feig at the *Natural Gas Discoveries: Strategic Implications* conference held by the Institute for National Security Studies (INSS) on November 23, 2010. A summary of the conference appears on the INSS website, http://www.inss.org.il/index.aspx?id=4480&eventid=2967; Gili Cohen & Itai Trilnick, *Navy Demands NIS 3billion to protect Mediterranean Drilling Platforms*," Haaretz, July 9th, 2012.

3 Lecture by Brigadier General (res.) Noam Feig, *supra* note 2.

4 International law consists of two kinds of rules – treaty and customary: a treaty rule is one that is legally binding on a particular state as a party to an international treaty that establishes the rule, while a customary rule is binding on all states. A state is therefore obligated to observe a customary rule, even if the rule is not stated in any of the treaties that it is party to.

5 United Nations Convention on the Law of the Sea (UNCLOS), Dec. 10, 1982.

6 As of the time of writing, 166 states have signed UNCLOS. States that have not signed include the US, Turkey, Iran, Syria, Thailand, and North Korea. From among Israel's neighboring states, parties to the convention include Cyprus, Lebanon, Egypt, Jordan and Saudi Arabia.

7 UNCLOS, Articles 17-19.

8 List of Geographical Coordinates for the Delimitation of the Northern Limit of the Territorial Sea and Exclusive Economic Zone of the State of Israel, July 12th, 2011, http://www.un.org/depts/los/LEGISLATIONANDTREATIES/PDFFILES/isr_eez_northernlimit2011.pdf; Agreement between the Government of the State of Israel

and the Government of the Republic of Cyprus on the Delimitation of the Exclusive Economic Zone, signed in Nicosia on December 17, 2010, http://www.un.org/depts/los/LEGISLATIONANDTREATIES/PDFFILES/TREATIES/cyp_isr_eez_2010.pdf. Note that following the depositing of these documents, the government of Lebanon filed a complaint to the UN Secretary-General claiming that the border submitted by Israel encroached into Lebanon's EEZ and illegally annexed approximately 860,000 square kilometers. The Lebanese Foreign Minister's letter of September 3, 2011 can be found at http://www.un.org/depts/los/LEGISLATIONANDTREATIES/PDFFILES/communications/lbn_re_isr_listofcoordinates_e.pdf.

9 The continental shelf is a geological term that refers to the seabed of the moderate incline starting at the coastline and ending at the point at which the angle of the incline changes sharply.

10 A distinction should be made between proportionality under the law of self-defense, which involves a balance between the gravity of the threat and the degree of force necessary to thwart it, and proportionality under the law of armed conflict, which involves a balance between the military advantage anticipated from a given attack and the anticipated collateral damage to civilians and civilian objects resulting from it. The term "proportionality" used in this article refers to the first type.

11 On this subject, note that according to the U.S. Department of the Navy, Commander's Handbook on the Law of Naval Operations (hereinafter, US Navy Handbook), "'imminent' does not necessarily mean immediate or instantaneous," *see* US Navy Handbook, section 4.4.3.1 (2007).

12 San Remo Manual on International Law Applicable to Armed Conflicts at Sea 73 (Louise Doswald-Beck ed., 1995). The manual was written by an international group of experts in the years 1988-1994. It should be noted that although the manual represents to a great extent the customary international law regarding naval warfare, some of its rules reflect *lex ferenda*, which does not bind states legally.

13 Assaf Harel, *Preventing Terrorist Attacks on Offshore Platforms: Do States Have Sufficient Legal Toos?*, 4 Harvard National Security Journal 131, 164-165 (2012).

14 This position was supported by a series of Supreme Court rulings. For example, see Israel High Court of Justice Case 769/02 *Public Committee against Torture in Israel v. the Government of Israel*.

15 For example, the law of naval warfare is the normative source regulating the Israeli naval blockade on the Gaza Strip; *see* The Turkel Commission, Public Commission to Examine the Maritime Incident of May 31, 2010; Report Part I, 42-45 (2011), Secretary-General's Panel of Inquiry, *Report on the 31 May Flotilla Incident* (September 2011), 41-42.

16 Given, among other things, that the 2006 war did not end in a ceasefire, and that Hizbollah continues its terrorist attacks against Israel (for example, Hizbollah is strongly suspected of having organized the attack on Israeli tourists in Burgas, Bulgaria on July 18th, 2012).

17 A state's port is an area completely under its sovereignty. As a rule, a vessel anchoring in the port of a state is therefore subject to the laws of that state (other than government ships, which enjoy immunity in certain respects). Accordingly, insofar as local law allows, the port state can prevent a vessel involved in terrorism from leaving the port.

18 Under the law of armed conflict, a "military objective" is an object that by its nature, location, purpose, or use makes an effective contribution to the enemy's military action, and whose destruction, capture or neutralization, under the circumstances, offers a military advantage to the attacking side. *See* Article 52(2) of the 1977 Additional Protocol I to the Geneva Conventions.

19 Convention on the Continental Shelf, April 29th, 1958. Under the treaty, the rights of states to exploit the natural resources of the seabed were acknowledged for the first time. The provisions of this treaty were included under Part VI of UNCLOS.

20 Geir Ulfstein, *The Conflict Between Petroleum Production, Navigation and Fisheries in International Law*, 19 Ocean Development and International Law. 229, 244 (1988); Harel, *supra* note 13, at 144-145.

21 Note that there is a decades-long conflict between states seeking to apply broad sovereign rights in the EEZ, extending beyond the resource-related rights specified in UNCLOS (such as China, Peru, and Ecuador) and states opposed to such measures (headed by the US) in the name of preserving freedom of navigation. *See* J. Ashley Roach & Robert W. Smith, United States Responses to Excessive Maritime Claims, 166-171 (2nd edition, 1996).

22 UNCLOS, Article 60(5).

23 The IMO is a UN agency whose main task is developing international regulations in the fields of international shipping, maritime safety, preventing sea pollution, and maritime security. The organization, composed of representatives of its member states, fosters progress on these issues by convening international conferences, and through discussions in the committees operating in its framework.

24 Proposal for the Establishment of an Area to be Avoided and Modifications to the Breadth of the Safety Zones Around Oil Rigs Located off the Brazilian Coast – Campos Basin, at 9, IMO Doc. NAV (February 26, 2006 53/3).

25 IMO Maritime Safety Committee, Subcommittee on Safety of Navigation, Report on its 56th Session, paragraph 4.6, IMO (Doc. NAV 56/20, August 31, 2010).

26 For example, it was previously reported that both Hamas and Hizbollah possessed the Kornet anti-tank missile, which according to Jane's Defense Weekly has a range of five kilometers; *see* Roni Sofer, *Chief of Staff: Kornet Missile Penetrates Tank in Gaza for First Time*, Ynet, December 21st, 2010, http://ynet.co.il/articles/0,7340,L-4002468,00.html. It was also reported that the two terrorist organizations also had RPG-29 anti-tank missiles, which according to Jane's Defense Weekly have a range of 500 meters; *see* Roee Nahmias, *Hamas Has Same Power as Hezbollah Before the War*, Ynet, December 13th, 2009, http:// www.ynet.co.il/articles/0,7340,L-3827244,00.html; Jane's Infantry Weapons 410 (Terry J. Gander & Charles Q. Cutshaw eds., 27th ed. 2001-02).

27 This approach was implemented by the US Navy. *See* U.S. Naval War College, Maritime Operational Zones 1-5-6 (2006).

28 For example, such notice may be given through a Notice to Mariners system used to distribute notices to all vessels navigating in a certain area, to port authorities, and to the public at large.

29 Article 146(c) of the San Remo Manual, *supra* note 11.

30 See Christopher Michaelsen, *Maritime Exclusion Zones in Times of Armed Conflict at Sea: Legal Controversies Still Unresolved*, 8 Journal of Conflict and Security Law, 363.
31 San Remo Manual, *supra* note 11, 181-182.
32 *Ibid.*
33 Condemnations were made mostly by Argentina and the Soviet Union; *see* Michaelsen, *supra* note 29, 372-374.
34 San Remo Manual (*supra* note 11), para. 180.
35 In 2004, Coalition forces, led by the US, imposed restrictions on navigation at a radius of up to three kilometers around two oil terminals off the Iraqi shore, following a terrorist attack aimed at the terminals. *See* US Navy Handbook, *supra* note 10, at C1-C2.
36 International law permits a warship or military aircraft to request the identification details of a vessel navigating in an EEZ. For example, according to the US Navy Handbook, a warship or military aircraft is authorized to approach a vessel in international waters in order to verify its nationality (*supra* note 10, 3-4).
37 Australia adopted this practice of questioning vessels in its EEZ as part of a program that it had implemented in 2004 for the purpose of protecting its drilling platforms and ports against the threat of a terrorist attack. See Natalie Klein, *The Right of Visit and the 2005 Protocol on the Suppression of Unlawful Acts Against the Safety of Marine Navigation*, 35 Denver Journal of International Law & Policy 287, 314 (2007).
38 The AIS (Automatic Identification System) is a VHF-based system that provides information about the location of ships. The LRIT (Long Range Identification and Tracking) system provides states with information about the identity, location, and navigational courses of ships within a range of 1,000 nautical miles of their shores. The IMO rules impose a duty to install systems of this type on ships of various categories, particularly passenger ships and large ships.
39 Following the terrorist attack on the US Marines headquarters in Beirut in 1983, the US Navy declared warning zones around its vessels navigating in the Middle East. A notice issued in this regard advised vessels and aircraft to identify themselves and provide information about their intentions before approaching US forces. Additionally, vessels and aircraft were advised to maintain a distance of five nautical miles from US vessels, and it was stated that vessels failing to keep such a distance could mistakenly be perceived as a threat, leading to the exercise of protective measures. The US Navy has used such warning zones on a number of other occasions since then; *see* Operational Zones, *supra* note 25, at 2-3, 2-4, and 3-2.

The State Secrets Privilege: From Evidentiary Privilege to Executive Immunity in the United States

Galit Raguan

In recent years, a number of controversial programs initiated by the United States administration under the auspices of its post-9/11 "war on terrorism" have come to light. These include the program to transfer detainees taken into custody by American forces to third countries, where the detainees were exposed to brutal and invasive forms of interrogation.[1] Attempts to question the legality of such executive steps in the courts have encountered several hurdles, which in practice have prevented further legal proceedings and adjudication. One of the more prominent of these hurdles is the state secrets privilege recognized in the United States legal system.

Originally, the privilege was designed to enable the administration not to disclose certain evidence during civil legal procedures if the disclosure was likely to harm national security. Even under the privilege's original formulation by the Supreme Court in the 1950s, almost complete deference was given to the interests of the government. Moreover, federal courts have interpreted the privilege very broadly in recent years, determining that the government is not required to invoke the privilege with regard to any particular piece of evidence. Instead, in several cases the courts have accepted the government's request to dismiss lawsuits at the outset without

---

Galit Raguan holds a Doctor of the Science of Law and is an Attorney at the Department of Special International Affairs at the Israeli Ministry of Justice. This essay is based on an earlier article: Galit Raguan, *Masquerading Justiciability: The Misapplication of State Secrets Privilege in Mohamed v. Jeppesen – Reflections from a Comparative Perspective*, 40 Georgia. Journal of International & Comparative Law 423 (2012). This essay expresses solely the author's personal opinion.

any substantive adjudication because of the risk that, should the court allow the proceedings to continue, secret evidence might be revealed.

The application of the state secrets privilege in such a broad manner raises serious questions relating to fundamental principles of the American legal tradition. In practice, this barrier to the adjudication of legal disputes, which is seemingly procedural in nature, provides the government with immunity from judicial review of the administration's policy on security matters. As a result, not only are the interests of individual plaintiffs harmed, but the ability to determine in the courts whether or not the actions of the administration conform to its legal obligations is undermined. This essay contends that a narrower application of the state secrets privilege is called for, one that allows for the balancing of the privilege against other interests, including justice and the search for the truth. In this context, the experience of the State of Israel – another state facing difficult legal challenges with respect to national security – may be instructive, and could perhaps assist in tailoring a more balanced mechanism in the United States for the protection of state secrets.

The State Secrets Privilege

The state secrets privilege is an evidentiary, judge-made doctrine (i.e., developed by the federal courts rather than set in legislation) most commonly attributed to the 1953 Supreme Court ruling in *United States v. Reynolds*.[2] In that case, the widows of three civilians working for an Air Force contractor sued the federal government for the deaths of their spouses in the crash of a military aircraft. During the discovery stage, the Air Force refused to reveal various materials pertaining to the investigation of the event, claiming that this was necessary to safeguard national security and military secrets. The case ultimately reached the Supreme Court, which determined that the government's claim should be recognized and that non-disclosure of certain information is to be allowed if disclosure is likely to harm national security.[3]

Under *Reynolds*, when a court examines the government's claim to privilege, the court must also weigh the plaintiff's need for information. The more significant the plaintiff's need, the more thoroughly the court must investigate the claim to privilege. Nevertheless, in the event that the court accepts the government's claim, the privilege is absolute.[4] The state secrets doctrine applies to civil proceedings, i.e., both in non-criminal lawsuits against the state (including constitutional and administrative matters) and

in suits involving two private parties, where the government sees fit to intervene and raise the state secrets privilege claim.[5]

Thus, Supreme Court precedent recognizes the possibility that the government can be exempt from disclosing particular information, should its exposure harm national security, and in *Reynolds* the exposure of certain materials (the investigative report of the plane crash and affidavits submitted by crew members who survived the crash) was indeed prevented. By contrast, in legal proceedings that have taken place in recent years in the United States, the government has sought dismissal of lawsuits – some against private parties rather than against the government itself – on the basis of the claim that hearing the suit at all is impossible given the concern that sensitive information might be revealed. The federal courts' willingness to accept this claim, as was the case in *Jeppesen* (discussed below), is too broad an expansion of the state secrets privilege that in practice protects the government from judicial review and exacts a heavy toll on those who have allegedly been harmed by the government.

Mohamed v. Jeppesen Dataplan, Inc.

In 2006, President Bush revealed that detainees taken into custody by the United States had been transferred to third countries for interrogation as part of the Extraordinary Rendition Program.[6] Had these detainees been held in official United States detention facilities, such as Guantanamo Bay, Cuba, or on American soil, they would have been subject to various forms of legal protection, oversight by certain bodies, and access to federal court. By contrast, detention in secret facilities in countries such as Morocco, Afghanistan, and Egypt apparently facilitated the subjection of detention conditions and interrogation methods that do not meet international or American standards.[7]

The plaintiffs in *Jeppesen*,[8] citizens of different countries, were apprehended in various locations around the world. According to the plaintiffs, they were moved to interrogation facilities outside the United States, where they were detained under harsh conditions, beaten, threatened with death, and subjected to various interrogation methods constituting physical and mental abuse, and even torture.[9] Based on openly published information, the plaintiffs concluded that they were subject to the United States' Extraordinary Rendition Program. They sued Jeppesen Dataplan, Inc., a Boeing subsidiary that was alleged in the complaint to have carried out the flights aboard which the plaintiffs were

moved to those third countries. The plaintiffs claimed that the defendant knew or should have known that they would be subjected to torture, and therefore bore responsibility for what had happened to them. In order to establish their claim the plaintiffs submitted hundreds of public documents, including the findings of an investigation by the Council of Europe and the European Parliament, as well as foreign governments and agencies, from which it was possible to learn about various aspects of the program.

Following earlier rulings by the district and appellate courts,[10] the case was eventually brought before an expanded panel of the appellate court. A majority opinion of five judges, joined by a judge issuing a separate concurring opinion, determined that even though the existence of the program in and of itself was not a state secret, the landmark *Reynolds* ruling compelled the court to dismiss the suit outright because there was no practical possibility of litigating the case and examining the liability of Jeppesen without creating an unjustified risk that state secrets might be exposed. The decision to dismiss the lawsuit was given despite the fact that the majority was ready to assume that neither the plaintiffs nor the defendant would need classified evidence to prove their case.[11]

Had the court determined that the defendant could not present a proper defense without needing classified evidence, the dismissal of the lawsuit would have been understandable. Fundamental principles of justice require that people be given the opportunity to defend themselves against legal proceedings and use exculpatory evidence. But the majority in this case was willing to recognize that the parties apparently did not need classified information to establish their case. The concern was that sensitive information would inadvertently come to light in the course of the proceedings. According to the majority opinion, this concern justified the dismissal of the suit.

A minority opinion of five additional judges felt that it was inappropriate to invoke the state secrets privilege at the beginning of the proceedings as a reason for dismissal because the state secrets privilege is fundamentally evidentiary in nature and was designed to allow non-disclosure of specific evidence. The minority opinion reasoned that it was therefore improper to exempt the government (or any third party) entirely from presenting its defense since allowing this effectively renders the state secrets privilege a doctrine of immunity. The minority judges dug through the many documents submitted by the plaintiffs and pointed to the unclassified documents that seemingly supported the plaintiffs' claims, thereby attempting to show

that it was improper to dismiss the suit at this preliminary stage without allowing the plaintiffs to attempt to substantiate their case on unclassified information, especially in light of the serious implications for the plaintiffs of preventing their access to the courts.[12]

From an Evidentiary Privilege to Executive Immunity

From the discussion above it would appear that the main disagreement between the majority and minority opinions in *Jeppesen* was over *when* to invoke the state secrets privilege. While the majority felt it could be raised at the outset, as a reason to dismiss the suit and avoid having to present a defense, the minority felt that the defendant first had to present its defense and invoke the state secrets privilege only with regard to certain evidence that, according to the government, could not be revealed. However, all the judges on the *Jeppesen* panel were in agreement that the case involved state secrets that could not be revealed during the proceedings. If so, why is the *Jeppesen* ruling so troubling?

One might argue that the approach of the majority is the more efficient one. If the plaintiffs are expected to inevitably hit a brick wall at a later stage of the proceedings – e.g., at a point when they will need classified evidence that they will be unable to attain – why waste time and resources on holding the proceedings to begin with? Isn't it preferable to dismiss the suit outright? The simple answer is no, for several crucial reasons.

First, it is impossible to know with certainty that the plaintiffs would need classified information to establish their claims (and similarly, that the defendant would need classified information to establish its defense). It may very well be that the case could have been heard without resorting to any classified evidence; indeed, this was the starting point of the majority opinion. The decision to dismiss the suit outright was designed to preempt the unintentional disclosure of classified information during the legal proceedings, which can be complex and involve a plethora of information. This is a conservative approach, which to a large degree questions the government's and the court's ability to conduct themselves responsibly and professionally when handling sensitive information. As a result, the plaintiffs' right to have their dispute heard by the courts is dealt a fatal blow. The plaintiffs themselves – not the government – are forced to pay the price of protecting state secrets.

Beyond the harm to the individual plaintiffs' interests, which one might argue is justified when balanced against the harm to the government should

it fail to maintain its secrets, the judiciary's ability to examine the legality of the Executive's actions is also severely impaired. Revealing details about the Extraordinary Rendition Program, as used by the Bush administration, would most likely have had political and diplomatic ramifications. At the same time, however, there are important legal questions at the very core of the program as well, such as: was the United States entitled to transfer people it had detained to foreign countries for interrogation, and if so, under what conditions? Did the interrogation methods to which the detainees were subjected amount to improper treatment or even torture? If so, was it the United States' active obligation to ensure that such methods would not be used before it rendered the detainees to these foreign countries? To the extent that the government promotes a policy that is not in keeping with the country's legal obligations and profoundly harms individuals' basic rights and liberty, there is tremendous importance to bringing the practice to a halt and to a judicial declaration that such a practice cannot continue in a democratic society.[13]

There are other advantages inherent in allowing judicial proceedings to proceed, to the extent possible, instead of a clumsy and unduly broad application of the state secrets privilege. By their nature, legal proceedings air other important details about the government's practices, contributing to lively public debate and a reexamination of policy by government bodies, which could lead to improvements and reforms. Furthermore, holding proceedings could create opportunities for reaching a settlement between the parties. Aside from the advantages outlined above, there is a glaring disadvantage to the approach that allows the outright dismissal of a case on the basis of a general claim that it is impossible to hold a hearing without endangering state secrets: namely, that the government does not assume any risk under such a legal approach. Essentially, there is no cost to advancing the argument as a threshold claim because the government always retains the right to invoke its privilege later on in the proceedings with regard to particular pieces of evidence. Therefore, the approach fails to provide any incentive to the government to limit the use of the doctrine as much as possible; in fact, it does just the opposite.

Despite the considerations justifying a narrower approach to the state secrets privilege – one that allows the state to invoke the privilege only vis-à-vis specific evidence rather than a threshold claim for dismissal of the legal proceeding as a whole – one must recognize that there may still

be many cases in which legal challenges will fail because of the inability to reveal information that includes or touches upon state secrets. This is partly as a direct result of the *Reynolds* ruling that holds that when the court is convinced that certain items of evidence do indeed involve state secrets, absolute privilege is extended even if such items of evidence are crucial to one of the parties. Therefore, it is not enough to adopt a narrower approach to the state secrets privilege than the one advocated by the government (and affirmed by the *Jeppesen* majority), although adopting such a stance is desirable given the current state of affairs. In addition, what is needed is a reexamination of the *Reynolds* ruling itself and a reconsideration of the balance that perhaps ought to be struck in American courts between the protection extended to state secrets and other important interests.

An Alternative Model to the State Secrets Privilege: A Glance at the Israeli Experience

In practice, the *Jeppesen* ruling forces the plaintiffs themselves to bear the cost of protecting national security in the sense that it prefers to block the possibility of holding legal proceedings at all rather than run the theoretical risk that sensitive information might be revealed during the proceeding. But there is another difficulty in the application of the state secrets privilege in the United States as formulated in the *Reynolds* ruling, which concluded that when the court is convinced that certain information amounts to state secrets, the protection extended to that information is absolute and the court does not have discretion over whether to allow its disclosure. The courts' discretion is thus limited only to determining whether certain materials should enjoy the state secrets privilege. Once the courts are convinced that the doctrine applies, the information cannot be disclosed. Thus, the Supreme Court of the United States grants an obvious advantage to the government's interests.

This all-or-nothing model, providing absolute protection to the government's interest in not revealing the information, is not the only model possible or even the only model in existence. In Israeli legislation a different model was adopted that enables a balance between the interests of the state and considerations of justice. In the Israeli context, the legal framework that enables the protection of state secrets is found in the Evidence Ordinance [New Version] 1971, which regulates, *inter alia*, the handling of classified evidence.[14]

Section 44 of the Evidence Ordinance states that the Prime Minister and Minister of Defense or Minister of Foreign Affairs may issue a "certificate of privilege" with respect to evidence whose disclosure is likely to impair national security or Israel's foreign relations. In such a case, that evidence cannot be used in legal proceedings. Section 45 creates a similar arrangement for evidence whose disclosure has been determined likely to damage an important public interest by any other government minister. Nonetheless, these sections also state that the courts may order that the secret evidence be disclosed if it is convinced that "the need to disclose it for the purpose of doing justice outweighs the interest of non-disclosure."[15] To make sure that no sensitive information is revealed during the hearing of the request to remove the privilege, section 46 of the Evidence Ordinance states that the hearing of such a petition can be held behind closed doors and that the court is permitted to hear the state's explanations *ex parte*. These paragraphs of the Evidence Ordinance apply to both civil and criminal proceedings. In Israel, as in the United States, a private party may request that the state issue a certificate of privilege in proceedings involving two private parties.[16]

Thus, the Evidence Ordinance establishes a mechanism that allows the courts to balance the need to prevent the disclosure of material whose exposure could harm state interests and the need of a plaintiff, a defendant – or the accused in the case of a criminal proceeding – for information in order to establish their claims. One may well ask how the court can compel the exposure of evidence when doing so would damage a critical national interest; does this not represent an unreasonable risk to national security, foreign relations, and other interests? This question may be answered in several ways.

First, the courts are routinely required to balance national interests, including those affecting national security, against other interests, such as the right to liberty, the right to privacy, freedom of expression, and so forth.[17] This is not unique to courts in Israel. American courts, which generally tend to take a more conservative approach when it comes to judicial review of matters seen as political in nature,[18] are also often required to balance national security needs with other individual rights.[19] There is therefore no justification that in the evidentiary field in particular absolute preference will be given to the interests of the state over other interests.

Second, the Israeli courts use various tools to reduce the possible harm to state interests when sensitive materials are involved. At times, for example,

with the consent of the opposing side, sensitive information is presented to the court *ex parte*.[20] While the party that cannot see or hear the evidence firsthand is still disadvantaged, if that party believes that the evidence can support its case, one may assume that it will prefer to allow the court access to that information, even if in an *ex parte* setting, rather than have the evidence excluded from the proceedings altogether. Other examples of means designed to prevent the inadvertent disclosure of sensitive materials include: keeping the evidence in a secured environment at the courthouse;[21] submitting rulings to the state before their publication;[22] releasing a summary or acquiring the state's consent that only the plaintiffs and their representatives with appropriate security clearance be able to review the sensitive information.[23] It should be noted that special arrangements for the handling of sensitive information in federal criminal proceedings also exist in the American context.[24]

Third, the state always has the option to prevent the harm likely to be caused as a result of the disclosure of the information. In civil proceedings, this could mean reaching a settlement, whether in the form of awarding damages or by stopping the harmful practice.[25] Such steps essentially represent the internalization by the state, and not (just) the individual, of the inability to disclose state secrets. Furthermore, the state is required to take such steps only if the court finds that considerations of justice compel the disclosure of privileged evidence. The courts still have the discretion to determine that, despite its critical nature, certain evidence will remain secret, even when in practice this decision means that the proceeding will have to end.

Thus, it is hard to argue that the Israeli arrangement and its application by the courts deal Israel's national security a fatal blow. Rather, they allow for a balance between the state's interests and considerations of justice in a manner that is missing from the American practice of recent years. Further support for this position may be found in the fact that since the enactment of sections 44-46 of the Evidence Ordinance, this Israeli legislative arrangement has not been altered.

Looking Ahead

Since the Obama administration entered the White House in 2009, and contrary to certain expectations,[26] the administration has continued to make relatively aggressive and extensive use of the state secrets privilege.[27] Specifically, the government continues to claim that attempts to challenge the administration's national security policy should be dismissed outright on the basis of this

doctrine.[28] In 2009, the Attorney General issued a memorandum designed to ensure that the doctrine be used judiciously,[29] though neither the memo nor its application have relieved critics' concerns.[30]

In this context, the initiative to regulate via legislation use of the state secrets privilege, first proposed in Congress in 2008, bears mentioning.[31] The bill is designed to set in place a "safe, fair and responsible" mechanism for the invocation of the state secrets privilege,[32] and seeks to confront most of the difficulties arising from the privilege's current use.[33] However, it has failed to make it past congressional committee since its proposal. In the meantime, the state secrets privilege, as well as a number of other procedural barriers developed by the courts, prevents the possibility of debating and clarifying essential legal issues relating to national security matters.[34] These issues will often have a significant impact on the fundamental rights of American citizens and others who come under American jurisdiction or control.

The United States is not the only country in the world facing challenges pertaining to the protection of sensitive information while conducting legal proceedings.[35] As discussed in detail above, Israel has a mechanism, established through legislation, that the courts use with some frequency. While the legal systems in Israel and the United States are not identical and it is not necessarily appropriate for the United States to import the Israeli approach, Israel's experience shows that even when confronting serious security challenges, the possibility for the state to deal with secret evidence differently exists. Consequently, Israel's experience may well be helpful in formulating a more balanced mechanism for invoking the state secrets privilege in the United States.

Notes

1 Another central issue was that of the Bush administration's warrantless wiretap program; *see* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, The New York Times, December 16th, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all. In June 2013, an extensive Obama administration program to collect records of phone calls made in the United States was also exposed; *see* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, June 6th, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order. See also Barton Gellman and Laura Poitres, *British intelligence mining data from nine U.S. Internet companies in broad secret program*, The Washington Post, June 7th, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-

11e2-8845-d970ccb04497_story.html. The program has given rise to public furor and extensive debate in the media and among commentators.

2 United States v. Reynolds, 345 U.S. 1 (1953).

3 It should be noted that some view the doctrine's source in an older decision, Totten v. United States, 92 U.S. 105 (1875). In *Totten*, which dealt with a damage suit resulting from espionage services supposedly given to the administration of President Abraham Lincoln, the Supreme Court determined that the lawsuit could not go forward, as it was based on a covert agreement between the plaintiff and government to provide confidential services. At times, courts present both rulings as the two sources of the same doctrine; *see* Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc). Other commentators argue that the *Reynolds* ruling (*supra* note 2*)* alone is the source for the state secrets privilege, whereas *Totten* relates only to specific cases wherein the foundation for the lawsuit is a secret agreement with the government; *see*, e.g., Christina E. Wells, *State Secrets and Executive Accountability*, 26 Constitutional Commentary 625, 639 (2010); Sudha Setty, *Litigating Secrets: Comparative Perspectives on the State Secrets Privilege*, 75 Brooklyn Law Review 201, 233 (2009); Carrie Newton Lyons, *The State Secrets Privilege: Expanding Its Scope Through Government Misuse*, 11 Lewis & Clark Law Review 99, 120-121 (2007). However, this distinction is not essential for our purposes; under both approaches, *Reynolds* is a binding legal precedent and key to the doctrine.

4 *See Reynolds*, *supra* note 2, 11.

5 As for criminal proceedings, there is specific legislation that deals with the handling of sensitive evidence; *see* Classified Information Procedures Act (CIPA), 19 U.S.C. app. 3 §§ 1-16 (1980). CIPA creates procedural steps for disclosing classified information connected to national security and its use in criminal proceedings in federal courts. These steps include protective orders, specific rules on revealing documents, *ex parte* hearings, and more.

6 Lucien J. Dhooge, *The State Secrets Privilege and Corporate Complicity in Extraordinary Rendition*, 37 Georgia Journal of International & Comparative Law 469, 474 (2009). The program preceded the Bush administration and referred to the transfer of suspects to third countries for arrest or trial, but after 9/11 its features and purpose were changed by the Bush administration in essential ways (*ibid.*, 472). Another similar move was transferring detainees to secret interrogation places called "black sites" belonging to the CIA outside of the United States; *see* Open Society Justice Initiative, Globalizing Torture: CIA Secret Detention and Extraordinary Rendition (2013), http://media.tcm.ie/media/documents/o/openSocietyJusticeInitiativeGlobalizingTortureReport.pdf. Many commentators writing on the topic fail to maintain the distinction between the two programs.

7 As an aside, it should be noted that a legal opinion prepared by the White House Office of Legal Counsel on transferring suspected terrorists to third countries for interrogation determined, for a host of reasons, that there was no legal hindrance to doing so. The legal rationale underlying the opinion has not yet been examined by the courts because the legality of the Extraordinary Rendition Program itself has yet to be examined by any American court; *see* Memorandum from Jay S. Bybee, Office of Legal Counsel, for William J. Haynes, II, Re: The President's power as

Commander in Chief to transfer captured terrorists to the control and custody of foreign nations (Mar. 13, 2002), http://www.justice.gov/opa/documents/memorandumpresidentpower03132002.pdf.

8 See Jeppesen, *supra* note 3. The ruling is one of the most prominent ones handed down in recent years in the context of the state secrets privilege. Even though this was a ruling in a federal court of appeals, rather than the Supreme Court, it is a critical one for several reasons. It was a ruling of the 9th Circuit Court of Appeals, considered the most important of the appellate courts, partly because its local authority extends also to California. In addition, the *Jeppesen* ruling was given by an expanded panel of judges. Following the ruling, writ for certiorari (request for leave to appeal) was filed with the Supreme Court, and was rejected. Therefore, currently, the ruling is the leading source for the application of the doctrine. Other appellate courts have applied the state secrets privilege in a similar manner in cases relating to national security; *see*, e.g., El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007).

9 *See Jeppesen*, *supra* note 3, 1074-1075.

10 *Mohamed v. Jeppesen Dataplan, Inc*., 539 F. Supp. 2d 1128 (N.D. Cal 2008); *Jeppesen*, *supra* note 3.

11 *Ibid*., 1087, 1099.

12 *Ibid.*, 1098, 1101.

13 It should be noted that there are other ways of examining the legality of the government's actions besides judicial proceedings. For example, Congress can initiate an investigation or through legislation create a mechanism that would grant compensation to anyone harmed by government activity; in this context, *see Jeppesen*, *supra* note 3, 1091. One could also try to use international mechanisms, though their effectiveness vis-à-vis the United States is liable to be limited.

14 *See The Laws of the State of Israel*, New Version 18, p. 421.

15 Paragraphs 44 and 45 of the Evidence Ordinance.

16 Yaakov Kedmi, *On Evidence*, Part 2, 874 (2003).

17 See, e.g., Israel High Court of Justice Case 2056/04, *Beit Surik et al v. State of Israel* (2004), which determined that the state had to reexamine the proposed route of the security fence despite the security interests it served, given the severe harm it was causing the area's Palestinian residents; Israel High Court of Justice Case 3239/02, *Mirab v. Commander of IDF in Judea and Samaria* (2003), which determined that the extension of detention of Palestinian detainees without being brought before a judge during intensive fighting did not meet binding legal standards and was therefore null and void; Israel High Court of Justice Case 680/88, *Shnitzer v. Chief Military Censor*, ruling 42(4)617, which determined that the decision of the Chief Military Censor to suppress the publication of an article about the Mossad was unreasonable.

18 In the United States, the political question doctrine formulated in the ruling of Baker v. Carr, 369 U.S. 186 (1962) is recognized. In accordance with the doctrine, courts avoid adjudicating cases when political questions come up and there are no judicial standards for reaching a decision; when it is impossible to decide issues the case arouses without making a policy determination; or when a ruling would involve an expression of disrespect towards one of the other branches of government; *ibid.*,

217. See, e.g., El-Shifa Pharm. Indus. Co. v. U.S., 607 F.3d 836 (D.C. Cir. 2010); Schneider v. Kissinger, 412 F. 3d 190 (D.C. Cir. 2005); Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010). In Israel, the application of the doctrine, manifested in the question of justiciability, is much narrower; *see* Aharon Barak, *Foreword: A Judge on Judging: The Role of a Supreme Court in a Democracy*, 116 Harvard Law Review 16, 98-106 (2002).

19 See, e.g., Hamdi v. Rumsfeld, 542 U.S. 507, 529-533 (2004), which determined that the mechanism for detaining those defined by the administration as illegal combatants does not meet the requirements of due process and that individuals detained under such circumstances were entitled to receive information about the factual basis for their detention and a fair opportunity to rebut the state's factual assertions before a neutral decision maker. The Supreme Court determined that the risk that under current conditions individuals would be detained without justification was unreasonably high and that the probability was low that the procedure the Court was demanding be implemented would have the severe ramifications claimed by the government; *ibid*., 532-534.

20 See, e.g., Various Civil Requests 6763/06, Hiyat v. Israel Airports Authority (2006).

21 *Ibid.*

22 *Ibid.*

23 See, e.g., Civilian Appellate Authority, 7114/05, State of Israel v. Hizi (2007).

24 See *supra* note 5.

25 In the case of evidence needed for the defense in a criminal case, this could under certain circumstances mean the withdrawal of the indictment; see, e.g., Appellate Authority 2489/09 Braude v. State of Israel (2009). Although this is a relatively extreme outcome, the move is designed to serve a purpose no less worthy than enforcing the law – namely, ensuring due process and the defendant's rights, in particular the ability to prove one's innocence. Some commentators have suggested that if the American courts rule against the government should it refuse to disclose secret evidence, this would provide incentive for private bodies to initiated unjustified litigation against the government and exploit the government's inability to disclose relevant evidence to establish its defense; see, e.g., Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 George Washington Law Review 1249, 1313 (2007). In practice, given the procedural obstacles facing potential plaintiffs, such as the standing requirement and the high costs of litigation, it is highly doubtful that this path would prove attractive to many potential plaintiffs. Moreover, it is possible to create mechanisms that would minimize this risk, such as one that would allow the courts to review sensitive evidence *ex parte* with both parties' consent so that it can determine whether the evidence supports the plaintiff's claims or not.

26 See, e.g., Center for Constitutional Rights, 100 Days: End the Abuse of State Secrets Privilege, http://ccrjustice.org/learn-more/faqs/100-days%3A-end-abuse-state-secrets-privilege.

27 Setty, *supra* note 3, 257-258.

28 See, e.g., Yassir Fazaga et al, v. Federal Bureau of Investigation, 884 F. Supp. 2d 1022 (C.D. Cal. 2012), which dismissed a suit challenging the collection of

information about Muslim residents on the basis of their religious affiliation alone by using covert government agents.

29 Memorandum from Eric Holder, Attorney Gen., U.S., to Heads of Exec. Dep'ts & Agencies, U.S. (Sept. 23, 2009), http://legaltimes.typepad.com/files/ag-memo-re-state-secrets-dated-09-22-09.pdf.

30 See Sudha Setty, *Formalism and State Secrets* in Secrecy, National Security and the Vindication of Constitutional Law, (David Cole et al. eds., 2013) (forthcoming); Wells, *supra* note 3, 644-645.

31 State Secrets Protection Act, S. 2533, 110th Cong. (2008).

32 *Ibid*.

33 For example, it allows courts to use various means to protect sensitive information and sets forth how the court should examine state secrets claim, the burden of proof on the government, and more. As for when to invoke the privilege, the bill states that the claim of state secrets will be considered by the court only after the conclusion of discovery of non-sensitive evidence and an opportunity is granted to the sides to make their arguments. As a general rule, it would be impossible to invoke the state secrets privilege at the beginning of proceedings, as was done in *Jeppesen* (*supra* note 3). The bill also states that after the court has been persuaded that certain items of evidence are non-disclosable, it retains the discretion to "weigh the equities and take appropriate orders in the interest of justice."

34 See, e.g., Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010), which dismissed a suit brought by a father to prevent the targeted killing of his son after the court determined that the father had not proven his legal standing or, in other words, had failed to show that he was an interested party from a legal perspective such that he would be able to bring suit. The targeted strike was carried out a few months later. See also Clapper v. Amnesty International U.S.A., 133 S. Ct. 1138 (2013), in which the Supreme Court dismissed an attempt to challenge the legality of the government's wiretapping program also on the basis of the inability of the organization bringing suit to prove standing because it failed to show that it was itself placed under government electronic surveillance. In both cases, state secrets claims were invoked by the government as reasons for its refusal to disclose information relevant to the suits.

35 Also see Benjamin Wittes, *Hugo Rosemont on Secret Evidence and Civil Justice in Britain*, Lawfare Blog, April 5th, 2012, http://www.lawfareblog.com/2012/04/hugo-rosemont-on-secret-evidence-and-civil-justice-in-britain.

INSS Memoranda, 2013 – Present

No. 138, July 2014, Pnina Sharvit Baruch and Anat Kurz, eds., *Law and National Security: Selected Issues*.

No. 137, May 2014, Emily B. Landau and Azriel Bermant, eds., *The Nuclear Nonproliferation Regime at a Crossroads*.

No. 136, May 2014, Emily B. Landau and Anat Kurz, eds., *Arms Control and National Security: New Horizons* [Hebrew].

No. 135, April 2014, Emily B. Landau and Anat Kurz, eds., *Arms Control and National Security: New Horizons*.

No. 134, March 2014, Yoram Schweitzer and Aviv Oreg, *Al-Qaeda's Odyssey to the Global Jihad*.

No. 133, March 2014, Pnina Sharvit Baruch and Anat Kurz, eds., *Law and National Security: Selected Issues* [Hebrew].

No. 132, January 2014, Yoram Schweitzer and Aviv Oreg, *Al-Qaeda's Odyssey to the Global Jihad* [Hebrew].

No. 131, December 2013, Amos Yadlin and Avner Golov, *Regime Stability in the Middle East: An Analytical Model to Assess the Possibility of Regime Change*.

No. 130, December 2013, Yehuda Ben Meir and Olena Bagno-Moldavsky, *The Voice of the People: Israeli Public Opinion on National Security 2012* [Hebrew].

No. 129, July 2013, Zvi Magen and Vitaly Naumkin, eds., *Russia and Israel in the Changing Middle East*.

No. 128, June 2013, Ruth Gavison and Meir Elran, eds., *Unauthorized Immigration as a Challenge to Israel* [Hebrew].

No. 127, May 2013, Zvi Magen, *Russia in the Middle East: Policy Challenges*.

No. 126, April 2013, Yehuda Ben Meir and Olena Bagno-Moldavsky, *The Voice of the People: Israeli Public Opinion on National Security 2012*.

No. 125, March 2013, Amos Yadlin and Avner Golov, *Regime Stability in the Middle East: An Analytical Model to Assess the Possibility of Governmental Change* [Hebrew].