

JOURNAL OF LAW AND CYBER WARFARE

- I. Counterterrorism Measures via Internet Intermediaries: A First Amendment & National Security Dilemma.....1
Mohamed H. Aziz
- II. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks.....23
Elizabeth Mavropoulou
- III. Legal Implications of Vulnerability Disclosure in International Conflict.....93
Thomas Cross
- IV. Virtual Crimes, Actual Threats: Deterring National Security Offenses Committed Through Cyberspace.....108
Asaf Wiener

Editor-in-Chief

Daniel B. Garrie, *Partner, Law & Forensics*

Senior Associate Editors

Michael Mann
Samantha Tucker
Radhika Tiwari
Tarique Collins

Junior Associate Editors

Jennifer Chan
Barry Dynkin
Anthony Ford
Geoffrey Kalender
Zachary Levy
Mary Beth Winningham

Editorial Board

Christopher Burgess <i>Founder & CEO, Prevendra</i>	Robert Clark <i>Cyber Attorney, Army Cyber Institute</i>
Jean-Claude Knebel <i>Consul General of Luxembourg to New York</i>	Robert Bair <i>Lieutenant Commander, United States Navy</i>
Jack Dever <i>Director, Business Intelligence Unit, General Electric</i>	Deborah Housen-Couriel <i>Special Counsel, Zeichner Ellman & Krause</i>
Dr. Larry Ponemon <i>Chairman, Ponemon Institute</i>	William Spernow <i>Chief of Security, Virus Inspector</i>
Jeremy Kroll <i>CEO, K2 Intelligence</i>	Eric Jensen <i>Law Professor, BYU</i>
John Dever <i>General Counsel of Defense Firm</i>	Uma Chandrashekhar <i>Global Information Security and Privacy Leader at Edwards Life Sciences</i>
Major Reserve, US Army	Vincent Scott <i>GBS-ITS Cybersecurity, Proctor & Gamble Company</i>
Dr. Joseph Weiss <i>Managing Partner, Applied Control Solutions</i>	Rhea Siers <i>Senior Associate at the GWU Cyber Security Initiative</i>
Shane Reeves <i>Associate Law Professor, US Military Academy, West Point</i>	Richard Borden <i>Chief Privacy Lawyer, Department of Trust and Clearing Corproartion</i>
Mitchell Silber <i>Executive Managing Director, K2 Intelligence</i>	Professor Michael Schmitt <i>Director, Stockton Study of International Law at the US Naval War College</i>
Noah Bledstein <i>IT Data Privacy Leader at GE Healthcare</i>	
Retired Major U.S. Airforce	

Virtual Crimes, Actual Threats: Deterring National Security Offenses Committed Through Cyberspace Asaf Wiener*

ABSTRACT

With the pervasive use of online communication media, we witness the increasing abuse of such media by terrorists and their supporters. These groups and individuals take advantage of online communication to promote and execute physical acts of terror. Due to the characteristics of online activity (mostly anonymity and monitoring limitations), such cyber-crimes pose serious policy challenges because it is difficult to isolate and punish these perpetrators through traditional legal measures. This paper explores possible responses to those challenges. It begins with the Israeli judicial experience regarding cyber-terrorism. An Examination of recent Israeli

* Ph.D. candidate and research fellow, Zvi Meitar Center for Advanced Legal Studies, Buchman Faculty of Law, Tel-Aviv University. The Author would like to thank Professor Michael D. Birnhack, Maya Ben-Meir, Omer Netzer and Jana Rabinovich for their constructive comments. A previous draft of this paper was presented at: INAUGURAL VOX-POL CONFERENCE: 'VIOLENT ONLINE POLITICAL EXTREMISM: SETTING A RESEARCH AGENDA', London, August 2014.

case law indicates that courts impose punishments for crimes committed in the virtual world that are comparable to more traditional criminal activity in the physical realm. Some courts even go a step further, and have debated whether virtual criminal activity should merit harsher punishments than physical crime in the interest of deterrence, considering that virtual crime is more difficult to detect and prosecute than traditional crime. Expanding upon this debate, this paper examines the instrumental capacity of criminal law, and criminal deterrence-by-punishment policy, in addressing the unique challenges of cyber national security offenses. The following analysis of the general challenges of deterrence by-punishment and cyber-terrorism is not unique to the Israeli legal system. An examination of these issues suggests that increased punishment severity is limited in its ability to serve as an effective deterrence mechanism given the cyber aspects of those crimes and the unique criminological aspects of terror-related activity. This paper, therefore, includes policy guidelines for future legal responses to cyber national security offenses, including recommendations for joint legislative actions and a focused legal response to supporters of those criminal acts.

I. PREFACE

*"Today's terrorism is not only characterized by its global, world-encompassing nature, but also by a great deal of sophistication... Terrorist groups engage in systematic operations that involve the development of extensive infrastructures that accommodate training, intelligence-gathering and tactical operations, all of which include the use of advanced technologies, for the sole purpose of engaging in terrorist attacks designed to inflict heavy tolls... The courts must consider any act of aiding and abetting terrorism with great severity..."*¹

CrimA 3827/07 Doe v. State of Israel (27.3.2007), para. 9.

Criminal law plays a pivotal role in regulating social conduct, and it therefore naturally provides a significant tool for nations to use in their efforts to fight terrorism. This paper focuses on sentencing, and it seeks to examine the ability of criminal law to regulate social conduct in the realm of cyber-terror. The paper explores the various policy considerations regarding legal responses to the emerging phenomenon of cyber national security offences (NSOs), by introducing and assessing current legal responses in Israel.

The term cyber national security offenses (NSOs) refers to a group of offenses involving collaboration with enemy forces to bring about some manner of harm to a nation. These offenses include acts such as espionage or disclosing classified information.² These offences receive special

¹ All quotes of Israeli verdicts were translated to English for the purpose of this paper and do not constitute official translation.

² See *infra* Part II.

attention because they constitute tangible versions of their cybercrime counterparts; namely, offenses *by* computers, as opposed to offenses *against* computers. As discussed below, NSOs in cyberspace (cyber-NSO) raise no unique difficulties regarding formulating legal prohibitions (the criminalization aspect). But, there is an ongoing trend whereby current court verdicts punish cyber-NSOs in a harsher manner than sentences punishing non-cyber-NSOs. The examination of the Israeli legal system contained here should serve only as the starting point for a more general discussion of the desirable legal responses to cyber-NSOs, both as terror-related offenses and cyber-crimes.

This paper's analysis will be arranged as follows: *Part II* addresses the foundational principals for applying existing criminal law to cyber-crime, and explores the current and evolving judicial policy of punishing cyber-crimes (such as online gambling and online sex offenses) more harshly than their conventional, real-world counterparts. *Part III* touches on the unique characteristics of national security offenses, and on the sentencing policy of Israeli courts regarding NSOs. *Part IV* details the emerging judicial policy regarding cyber-NSOs, as surmised from the Israeli Supreme Court preliminary sentences issued between 2012 and 2014. Finally, *Part V* assesses the current deterrence-by-punishment approach regarding cyber-NSOs and considers possible adjustments, which may allow the legal system to better deal with the unique challenges that arise in the context of cyber-NSOs.

II. CRIMINAL LAW AND CYBER CRIME

Criminal law regulates social conduct by

removing undesirable acts from the realm of the conventional. It does so by combining two interconnected measures: first, prescribing prohibitions that establish a set of binding norms, and second, prescribing a system of sanctions inflicted on violators. The appearance of criminal activity in the online sphere, including terror-related crimes, mandates the legal system's adaptation to this new arena of crime. This adaptation must accommodate both of the aforementioned modes of operation: criminal prohibitions that have a tangible basis in the real world must now be suited to include online activity,³ and the criminal justice system must determine the severity of sanctions to deter criminal conduct in the virtual world.

Israeli law, like other legal systems, distinguishes between offenses *against* computers and offenses *committed through* computers. The

³ The adaptation of existing criminal prohibitions to the world of cyberspace is, naturally, a special case of the challenges facing the legal system in its efforts to formulate a legal response to a new social reality. The advent of cyberspace resulted, naturally, in a plethora of legal challenges, discussed in the broader context of *law & technology*. See generally LAWRENCE LESSIG, CODE VERSION 2.0 (2006) (pointing to four regulating factors in the context of cyberspace: network architecture, societal regulations, market forces, and law). For an introduction to the legal debate on whether specific laws ought to be devised so as to govern the online instances of tangible acts which are now being regulated under existing legislation, see generally Frank Easterbrook, *Cyberspace and the Law of Horse*, 1996 U. CHI. LEGAL F., 207 (1996). In terms of criminal law, the advent of cybercrime may bring about a variety of new challenges, such as enforcement obstacles (for example, cybercrime monitoring difficulties, extra-territorial offenses), the use of electronic evidence, causality gaps with regard to consequential offenses, and the psychological-criminological consequences of cybercrime. See *infra* Part V.

phrase “offenses committed through computers,” refers to the “migration” of traditional crimes to the virtual world, while “offenses against computers” (or “Netcrime”) refers to crimes in which a computer system is the target of the crime.⁴ The facilitation or commission of terrorist acts may be committed through computers or against computers. One example of the former is a cyber-attack against computer systems designed to damage and disrupt military or civilian systems, such as transportation systems.⁵ And examples of the latter kind of offense include terrorist recruitment through online social networks, fundraising through online money transfers, and online propaganda dissemination.

Within the Israeli justice system (operating within a common law tradition), the lion's share of the struggle with legal challenges, unique to cyber-crime, is allocated to the court system. In Israel, courts have taken an active role in reconstructing the penalization of cyber-crime offenses, including cyber-NSOs, to facilitate the government's efforts to fight such offenses.⁶ The Israeli Supreme Court has concluded that criminal activity conducted in cyberspace presents significant challenges, which may justify the stricter punishment of such offenses. This view is exemplified in a landmark Supreme Court case, in which the Court discussed important sentencing considerations when punishing online

⁴ See, e.g., Donald R. Mason, *Sentencing Policy and Procedure as Applied to Cyber-Crimes*, 76 Miss. L.J. 903, 905 (2007).

⁵ See, e.g., Computers Act, 5758-1998, __ LSI __ (1998) (Isr.) (enumerating, *inter alia*, the following offenses: damage or disruption to computers or computer-stored materials, unlawful access to computer-stored materials, false output, etc).

⁶ On this ground, the principal research method employed in this paper relies mostly on existing case law and an analysis of the findings derived therefrom.

gambling offenses:

Online offenses augment the number of potential victims, as such crimes can be automatically repeated thousands of times without any further effort invested by the perpetrator. This aspect of cybercrime renders it more dangerous to victims and more lucrative for the perpetrator. Such offenses further differ from others in that the ability to enforce laws against them is markedly inferior, as the nature of cyberspace allows perpetrators to conceal their actions and remain anonymous, thus significantly curtailing the capacity of law enforcement agencies to detect the offenses and identify their perpetrators...⁷

In this landmark ruling, which established the judicial policy underlying the punishment of online gambling offenses, the Court determined that the online nature of the acts warrants more severe punishment for two principal reasons: (1) cyber-crimes result in more potential victims making them more dangerous for the victims and more beneficial to perpetrators; and (2) it is much harder to prosecute cyber-crimes as compared to traditional crimes because of the added difficulties in monitoring and identifying offenses and their perpetrators.

In another ruling, which concerned the blocking of online gambling websites, the Court determined that the adverse effects of online gambling are immeasurably more significant than those of gambling events taking place in the real world. This is so because of the increased

⁷ CrimA 6889/11 State of Israel v. Oved (14.2.2012), para. 5 [hereinafter Oved Appeal].

accessibility and availability afforded by cyberspace and the ability to disguise the identities of those occupying it.⁸ Later in that ruling, the Court stated the following: “The efforts of law enforcement agencies to apprehend perpetrators do not end in cyberspace. The internet shall not be considered a safe haven. It is not the platform used for online gambling that is key to our discussion, but rather the actual act of illegal gambling.”⁹

This approach is also characteristic of the Supreme Court's policy on online sex offenses. The Supreme Court rejected the argument that the “technologically-produced distance” between the appellant and their victims justifies mitigation, and has espoused the view that such offenses should be punished with relative severity:

Even though the acts of the appellant and the suffering of his victims took place in cyberspace, the actual harm and emotional suffering inflicted on those young victims is undeniably real. Moreover, *on the internet, the potential to cause harm is especially grave, given the ease with which duplication and dissemination are achieved The mere fact that an offense is committed online does not suffice in alleviating the severity with which protected values are compromised. On the contrary, the legal system should be poised to deal with new threats to the person, dignity and well-being of victims, and must be able to provide the aforementioned with*

⁸ Administrative Petition Appeal 3782/12 Police Chief of Tel Aviv-Jaffa District v. Israel Internet Association (24.3.2013).

⁹ *Id.* at para. 41.

*adequate solutions.*¹⁰

This discriminating approach indicates that the Supreme Court has already qualitatively distinguished between committing a tangible offense and committing the same offense using online measures, and has ascribed greater severity to the latter.¹¹ This approach was set and affirmed in cases of online gambling and online sex offenses, but it has yet to be fully applied in the field of cyber NSOs. The aggravating aspects of online activity, mentioned above, concerning online sex crimes or gambling (i.e., enforcement limitation or increasing the number of potential victims) can be used as a basis for discussion, but it should be further examined whether these aggravators are equally relevant considerations when attempting to punish and deter cyber-NSOs.

III. NATIONAL SECURITY OFFENSES IN THE ISRAELI LEGAL SYSTEM

A. National Security Offenses in Israeli Criminal Law

The criminal offenses most relevant to our discussion are chiefly addressed in *Chapter G* of the Israeli Penal Code and the Prevention of Terror

¹⁰ CrimA 6703/13 Cohen v. State of Israel (16.1.2014), para. 13 (emphasis added). It is interesting to note the many similarities between this approach and that previously described with respect to online gambling offenses.

¹¹ The notion that the shift of offense-commission from the physical world to the cyber sphere should result in a different sentencing policy is not unique to Israel. See Mason, *supra* note 4, at 907.

Ordinance.¹²

In Israel, as in other western democracies, NSOs, principal among them being the offense of treason, are some of the most severe of all criminal offenses.¹³ These offenses are committed not against a person or organization, but rather against the nation or society at large, and most entail long prison sentences (and symbolically, those are the first offenses defined under by the Israeli Penal Law). Another manifestation of the unusual severity with which NSOs are regarded in Israel can be found in the strict legal procedures that apply to citizens suspected of committing security offenses. These procedures differ from general criminal procedure. For example, those suspected of security offenses are at times prevented access to their attorneys, and the legal system allows for more protracted periods of incarceration before a judicial hearing.¹⁴

Importantly, the Israeli Criminal Code does not differentiate between crimes committed in the real

¹² See also Defense (Emergency) Regulations (ex-penal legislation, used mostly regarding non-Israeli citizens in the West Bank and Gaza. Those regulations establish military tribunals to try civilians, extensive powers of search and seizure, curfew, administrative detention, publications preventions, and house demolitions); Cheryl V. Reicin, *Preventive Detention, Curfews, Demolition of Houses, and Deportations: An Analysis of Measures Employed by Israel in the Administered Territories*, 8 CARDOZO L. REV. 515 (1986-1987).

¹³ For comparative anti-terror legislation, see CLIVE WALKER, BLACKSTONE'S GUIDE TO THE ANTI-TERRORISM LEGISLATION 50-66 (2002) (UK); STEPHEN DYCUS ET. AL., NATIONAL SECURITY LAW 561-86 (3th ed., 2002) (US); ERLING JOHANNES HUSABO, FIGHTING TERRORISM THROUGH MULTILEVEL CRIMINAL LEGISLATION (2009) (EU).

¹⁴ Articles 1 & 7, Chapter 7, the Penal Code, 1977; Criminal Procedure Act (suspect of national security offenses) 2006.

world and those same crimes committed through cyberspace. The law, in a sense, is technologically neutral. Therefore, the same rules and penalties apply to physical NSOs as to cyber-NSOs. At first blush, it would appear that this technological neutrality constitutes a desirable approach because it poses fewer obstacles to criminalization. But, this paper suggests that the technological neutrality serves to undermine the instrumental purpose of criminal law – regulating social conduct – as it pertains to cyber-NSOs and other online offenses).

B. Sentencing Policy regarding traditional NSOs

Generally speaking, criminal punishment may advance several goals and policy considerations. The relative consideration and importance that any goal receives in the delineation of a punishment scheme is a matter of social agenda. The most important goals of punishment are:

Retribution / Proportionality: This suggests that the punishment should be commensurate with the crime.

Deterrence: This is forward-looking and is designed to reduce the incentive for future offenses when compared to the benefits obtained by the perpetrator because of the offense. Deterrence influences behavior on two levels: general deterrence and specific deterrence. General deterrence is the impact of the threat of the criminal sanction on the public, and results from the risk of detection and punishment when criminal laws are violated. Specific deterrence is the impact of the actual criminal sanctions on the agents who are aware of and influenced by them, and results from either

personal apprehension of the potential negative consequences of a criminal act, or from actual prior experiences with detection, prosecution, and punishment.

Incapacitation / Prevention: Similar to deterrence, prevention is designed to reduce the frequency of future offenses. This usually involves the perpetrator's incarceration and isolation from society, in a manner preventing him or her from further breaking the law.

Rehabilitation: This goal focuses on the treatment of congenital and environmental causes which result in criminal behavior. While punishment is typically viewed as backward-looking-- that is, a person is made to suffer for wrongful acts that occurred in the past-- many penal systems encourage offenders to change personally to avoid recidivism upon release back into society.

A fundamental principle of criminal punishment is that some combination of these considerations should guide the effort to formulate a suitable punishment for each offense - regarding both the legislators who enact laws that dictate the punishment of each crime, and to criminal prosecution, which culminates in the sentencing of criminals. In 2012, the Knesset (the chief Israeli Legislative body) enacted a significant amendment (No. 113) to the Israeli Penal Code. The purpose of this amendment, *inter alia*, was "To determine the guiding considerations and principles of sentencing, the weight that ought to be given to them and the interrelationship between them."¹⁵ Prior to this amendment, courts possessed significant discretion

¹⁵ Penal Code (113 Amendment), 2012 [hereinafter: Amendment 113].

when considering the relative weights of the different sentencing factors, and the Supreme Court was the guiding institution in that matter. Amendment 113 specifically stipulates that the guiding principle of sentencing is proportionality, and therefore the principle of general deterrence must be subordinated.

As to NSOs, the Israeli Supreme Court has formulated a consistent policy - deterrence should be preferable to other sentencing-related considerations regarding security offenses. This trend has resulted in a long series of sentences issued by the Supreme Court in the last few decades (prior to Amendment 113). The Supreme Court often regards itself as committed to the struggle against security threats, and does so by way of utilizing deterring sentences. For example, in a sentence issued in 2003, the Court stated:

The times in which we live are fraught with bloodshed, and all, and primarily those who swear allegiance to the State of Israel, are obligated to take whatever measures necessary for mitigating the effects of terrorism. That goal is shared by the courts, which must seek to deter the masses.¹⁶

In another case, the Court similarly extrapolated

¹⁶ CrimA 2131/03 Saadi v. State of Israel (22.12.2003). In this case, the Appellant was convicted of Contact with a Foreign Agent, which involved the disclosure of information to a terrorist organization member prior to the commencement of a suicide-bombing mission on Israeli soil. The Supreme Court denied the appeal filed by the Appellant, which contended the sentence's leniency, and sustained the prison sentence decreed by the District Court – 6 years of active imprisonment. In its sentence, the Court further added that the original punishment was "so moderate as to undermine the principle of deterrence."

on the importance of deterring acts of terror:

[A]s tremendous efforts are being invested in the defending of the civilian population against those who wish to do it harm, it is of paramount importance to ensure the deterring effect of sentencing, so that no act conducive to or facilitating the operations of terrorist organization is committed.¹⁷

These sentiments reflect the principles of the court's current policy that the dangerous nature of NSOs, and the social interests which the laws punishing them are designed to protect, demand severe sentencing (and a lower weight on rehabilitation considerations). The enactment of Amendment 113, has not changed this well-established policy.

The intermediate conclusion is that we can observe the legislature (in the Penal Code prescriptions) and courts presenting a united front characterizing NSOs as severe crimes requiring severe sentencing policies (although the new Amendment 133 gives more declarative weight to proportionality of general deterrence). An examination of existing legislation and case law

¹⁷ Crim. App. 10680/04 State of Israel v. N. Knaana (10.11.2005). In this case, the Appellant was convicted of Contact with a Foreign Agent, which involved the delivery of various materials such as maps and instructions for the assembly of explosives to and from various members of the Fatah organization. The District Court sentenced the Appellant to 30 months of active imprisonment, and against this sentence, appeals were filed by both the convicted felon and the State. The Supreme Court sustained the State's appeal, and determined that the convicted be sentenced to 54 months in prison.

indicates that the perception of these offenses as extremely severe (justifying strict punishment) is not the product of an independent judicial policy of the court, but is founded on criminal legislation. However, as illustrated by the extracts presented above, when determining a defendant's sentence, the court considers itself committed to an active role in the state and the justice system's struggle against terrorist threats even if that entails a fundamental change in the way penal considerations are perceived. In the next part, I seek to identify and present the Supreme Court's sentencing policy in cases of cyber-NSOs, which reflects both existing policies against security offenses and the struggle against the legal challenges that activities in cyberspace pose.

IV. PENAL POLICY ON CYBER NATIONAL SECURITY OFFENSES

This section addresses penological considerations of NSOs committed in cyberspace. It briefly presents the current tendencies of the Israeli Supreme Court in the last few years, as reflected in several exemplary cases. It also proposes an analysis and assessment of the aforementioned judicial policy, namely: can more severe punishment in cases of cyber-NSO (compared to offline-NSOs) adequately address unique challenges posed by cyber-NSOs, both as cyber-crime and as ideological-crimes?

The Israeli court first addressed the online aspect of NSOs as a consideration affecting the court's sentence in the 2009 case *Shamir v State of*

Israel (“Shamir Criminal Appeal”).¹⁸ The defendant, a reservist IDF officer in possession of classified materials approached certain hostile organizations and hostile nations and offered to provide them the materials. The defendant communicated with these organizations and nations by email (sent to the Iranian Ministry of Foreign Affairs and to certain Hamas members in Gaza). After the defendant delivered some of the information, he was caught and charged with two NSOs: Contact with a Foreign Agent and Possession of Information with the Intent of Jeopardizing National Security. The defendant pleaded guilty and was convicted by the District Court, which sentenced him to five years of imprisonment.

When sentencing the defendant, the district court expounded upon the considerations that guided it in crafting Shamir’s punishment. First, the court stated the judicial policy in favor of strict punishment for security offense cases given the added severity ascribed to such offenses. Later, the court specifically considered the ‘virtual aspect’ of the act as a *mitigating* factor in determining the defendant’s sentence, alongside other considerations. The Court highlighted “the other aspect characteristic of the nature of communications engaged in by the Defendant with hostile operatives, *which were virtual in nature* and which failed to attain their goals”.¹⁹ However, the court failed to explain exactly why the virtual aspect of this crime made it somehow less serious and deserving of punishment.

The Defendant appealed the sentence on the basis of his allegedly impaired mental state at the

¹⁸ CrimA 1803/08 Shamir v. State of Israel (9.3.2009).

¹⁹ CrimC (Tel Aviv District Court) 1126/07 State of Israel v. Shamir (17.1.2008), para. 9 (emphasis added).

time of his crimes, and on his assertion that he was otherwise a “law abiding citizen.” Ruling on his appeal, the Supreme Court initially reaffirmed the policy dictating that NSOs warrant severe punishment, primarily for the purpose of deterrence. The Court affirmed the defendant’s sentence explaining that the sentence was appropriate given the serious nature of the defendant’s crimes. Later, the Court asserted that even if it entails the increased severity of the then-prevailing penal policy, the new policy (of deterrence by severer punishment) should prevail: “It is indeed merited to achieve the purpose of deterrence by way of sentencing”.²⁰ Later, the Supreme Court denied the remaining claims raised by the Defendant without addressing the virtual aspect of the offense, which the District Court had considered a mitigating factor.²¹

Shortly after *Shamir* was decided, cyber terror-related crimes were again raised in *State of Israel v Doe* (“*Doe I*”).²² There, the Defendant, an Israeli resident and citizen, initiated communications in 2009, via email, with Hezbollah (using contact information found on their website), and offered to translate certain articles. Later, Hezbollah provided the defendant with an encryption program (a “splitter”), and asked him to send encrypted data to the organization per certain instructions he received. The Defendant's handler instructed him to gather

²⁰ Shamir Criminal Appeal, *supra* note 18, at para. 7.

²¹ At the beginning of the Supreme Court's sentence, the various considerations enumerated by the District Court were reviewed, including “a certain examination of the type of relations formed by the Appellant, which were virtual in nature”. Shamir Criminal Appeal, *id.*, at para. 4. However, the Court declined to address this consideration in its opinion.

²² CrimA 3417/10 State of Israel v. Doe (31.1.2011).

intelligence on Israeli military and civil infrastructures, and information regarding various individuals. The Defendant did as he was asked, and sent to his handler (using the splitter in his possession) multiple messages containing large amounts of information. Eventually the Defendant was caught by law enforcement agencies and charged with seven counts of Delivery of Information to the Enemy. The Defendant pleaded guilty. At sentencing the Defendant sought leniency, arguing, among other things, that he was a law abiding citizen with moderate rather than extremist views, and that he fell victim to solicitations by Hezbollah. When determining his sentence, the court considered the potential damage of the Defendant's communications with a terrorist organization without focusing on the online nature of the communications. Eventually, the defendant was sentenced to three years of imprisonment.

Both the state and the defendant appealed the sentence to the Supreme Court. The state sought a harsher punishment, while the defendant sought a reduced sentence, arguing that the information he had relayed to Hezbollah was inconsequential.

The Supreme Court ruled in favor of the state. The Court reviewed the underlying rationales of sentencing: rehabilitation, retribution, prevention and deterrence, and stressed the conventional judicial policy regarding NSOs-- namely, that their principal penal consideration is that of deterrence. As the Court explained:

Indeed, these offenses are usually carried out as a result of ideological motives, and from that follows the special consideration given to the deterring value of the

punishment, which will later be taken into account by the accused and by other potential perpetrators, before they set about the business of committing a national security offense.²³

As previously mentioned, this is not a novel judicial policy, and is conventional as to NSOs. However, the Court further added that in the instant case there existed another aspect of deterrence pertaining to the online nature of the offense:

Two elements of severity can be ascribed to the Appellant's conduct. First, the Appellant is an Israeli resident in possession of an Israeli citizenship. . . . *Second, the engagement in communications with hostile forces has become relatively simple with the advent of the World Wide Web*, thus making it easier for those who seek to harm their country. Such elements, which, lamentably, appear in more and more cases as time goes on, require that a clear and forthright message be conveyed to the public, namely, that to aid and abet the work of elements hostile to the State of Israel *shall result in a heavy price borne by the perpetrators of such crimes*.²⁴

The Court accordingly increased the punishment and sentenced the defendant to four and a half years of imprisonment.

The Court's determination that the ease of the defendant's communication with hostile agents was an aggravating factor suggests that the court ascribed

²³ *Doe I* case, *Id.* at para. 5.

²⁴ *Id.* at para. 6 (emphasis added).

significant value to the difficulties the online sphere poses to law enforcement and national security. In *Doe 1*, the online aspect of the crime contributed to the relative ease with which the defendant could communicate the sensitive information to Hezbollah. The interrelation between the Court's emphasis on deterrence and its observations regarding the relative ease of committing cyber-NSOs suggests that the Court adopted a policy of considering online elements of NSOs as aggravating factors when meting out sentences. Subsequent Israeli cases have relied on *Doe 1* for this proposition.²⁵

The third case discussed in this paper is *Doe 2*,²⁶ which was concluded in early 2014. The two main defendants were brothers, both of them Israeli citizens and residents. They corresponded with two Hamas activists via Facebook. In their correspondence, which continued for two years, the defendants expressed their willingness to assist Hamas in recruiting members and supplying weapons. The defendants even organized meetings at several locations. After they were caught, the two brothers were charged with Contact with a Foreign Agent and for Attempted Assistance to Enemy in War, and they both pleaded guilty to all charges. At sentencing, the brothers argued that the 'virtual nature' of the crimes of which they were convicted "meant that their crime was to be considered as the

²⁵ Cf. 7430/10 Doe v. State of Israel (2012) (the Supreme Court cited *Doe 1* when it stated: "it is impossible to ignore that the Internet era has led to significant ease, technically, in committing criminal offenses, such as conspiracy... this case exemplify the need for deterring-punishment on the negative and criminal side effects of the Internet's technological advancements", when sentencing cyber-NSOs);

²⁶ CrimA 2791/13 Doe v. State of Israel (3.2.2014) ("Doe 2").

least severe form of security offenses.” But the State argued that “the insufferable ease with which security offenses are committed via the internet” necessitated a harsher sentence to deter others from taking similar actions.

The District Court agreed with the state predicated its decision on the Supreme Court’s ruling in the *Doe I* case:

[T]he internet enables online and prompt telecommunications has turned the virtual realm into a convenient medium that makes it possible to commit multiple crimes. New varieties of crime which were previously common throughout the globe, for convenience purposes, have been superimposed onto the online world, as is the case for our present discussion... the internet and various social networks provide a convenient, readily-available and even common platform for committing various crimes, and in this regard I see no reason to distinguish between “real” and “virtual” spaces. *In this day and age, all that is virtual is also real, and it behooves one to reject the notion that cybercrime is tantamount to youthful frivolity, to crimes carried out carelessly, or to acts pursued for the purpose of surmounting social challenges. Cybercrime is equal to any other form of criminal activity. The high frequency of cybercrime necessitates that a clear and forthright message be conveyed to the public, namely, that to aid and abet the work of elements hostile to the State of Israel shall result in a heavy price borne by*

*the perpetrators of such crimes.*²⁷

The District Court's ruling suggests that the harsher treatment of online NSOs in *Doe 1* has become widely accepted amongst the Israeli judiciary. Note that the court did not just equate 'real' and 'virtual' crime, but also stated that the frequency of cyber-crime (derived from the large-scale communication opportunities of the Internet) should be answered with a *severe* punishment. Ultimately, the appellants were sentenced to 6 and 6.5 years in prison (each appellant's sentence was based on his particular involvement in the crimes committed).

The Defendants appealed their sentences to the Supreme Court. Their appeal challenged the severity of their sentences. The majority of the defendants' arguments concerned the virtual nature of the offenses. They argued that they did not comprehend the seriousness and gravity of their crimes because they were committed while staring at a computer screen. The Court explicitly rejected this argument, and determined that:

These offenses do not merit leniency strictly on the grounds that they were allegedly committed in cyberspace. Cybercrimes can result in all the offenses and injuries that exist in the real world. In any event, *in this case* one should not ascribe special meaning to the medium via which communications were effected... It is not the means by which the acts were carried out, be they virtual or otherwise, that matters in our present case, but rather the

²⁷ CrimC (Nazareth District Court) 11230-01-12 State of Israel v. As'ad (6.3.2013) (emphasis added).

nature of the acts themselves. In this context, when the offense involved conspiring with hostile agents, the medium used to attain that purpose is entirely irrelevant, and serves to neither aggravate nor mitigate the severity of the crime.²⁸

After having rejected the defendants' claim that the online nature of their actions should constitute a mitigating factor, the Court upheld the trial court's finding that, at least in the instant case, the online nature of the crimes could properly be considered an aggravating factor for sentencing purposes:

Without stipulating a general rule at present, *it may even be held that the ease with which messages are conveyed through the employment of various technological means and the difficulty, with which such crimes are monitored and scrutinized, should compel the court to severely punish perpetrators caught in the act of committing such crimes.*²⁹

Although the Court did not announce a policy of considering online aspects of NSOs to be aggravating factors at sentencing, it clearly approves of such findings in individualized cases. The general takeaway of *Doe 2* seems to be that online aspects of NSOs are not mitigating factors, and may properly be considered aggravating factors on a case-by-case basis. Cyber NSOs, according to the Court, warrant at least as much punishment as traditional NSOs, and

²⁸ *Doe 2 Case*, *supra* note 26, at para. 19 (emphasis added).

²⁹ *Id.* at para. 21 (emphasis added).

probably more. However, is punishing cyber NSOs more severely really the best approach? In the final part of this paper, I examine the social utility and overall efficacy of attempting to deter cyber-NSOs by punishing them more severely than NSOs committed solely in the kinetic world.

V. DISCUSSIONS: CYBER-NSOS AND DETERRENCE-BY-PUNISHMENT POLICY

As to cyber-NSOs, the judicial policy favoring more severe criminal punishment whenever the offense involves online activity is warranted and proper. Increased punishment addresses the challenges presented by cyber crime: ease of commission, on the one hand, and enforcement limitations (anonymity and monitoring impracticalities), on the other. As discussed, the suggested judicial response seems focused on deterring cyber-NSOs.³⁰ In this section, I will present possible criticisms regarding the institutional and instrumental aspects of this approach, respond to those criticisms, and suggest possible guidelines for continuing and enhancing this legal response.

A. *The Institutional Criticism*

Some would argue that the policy of punishing cyber-NSOs more harshly than traditional NSOs, is not the kind of policy determination courts

³⁰ As mentioned previously in Part III, deterrence is the premier consideration in the general domain of NSOs, but it also the prominent one in the specific cases of cyber-NSOs, as shown in Part IV.

should make. As an institution, is preventing NSOs a task that the court system should take up, or should it confine itself to merely enforcing the criminal law when cases are brought to trial? Seemingly, the Supreme Court's approach tips the balance regarding conventional considerations that affect criminal sentencing, and shifts the focus of criminal sentencing to deterrence at the expense of other purposes.³¹ Therefore, perhaps this issue, which has direct implications on basic rights, should be formally addressed by way of legislation, rather than exclusively by the judicial branch.³²

This criticism carries little weight. First, as a balance between uniform and equalitarian punishment and the need to solve the specific aspects of a tangible criminal act, the current policy provides the judicial system with broad yet strictly-defined discretion. The policy clearly defines the factors that courts should consider when sentencing for cyber-NSOs, yet still affords significant leeway for individualized determinations. Second, the general

³¹ In Kantian terms, this policy is contrary to the categorical imperative, as it considers the objects of punishment to be a "means" to a social end. In terms of Israeli constitutional law, one may wonder whether such offensive means commensurate with the principle of proportionality: a rational link between the offending means (stricter sentencing) and the attainment of the purpose which they seek to achieve (deterrence or social conduct with regard to online security offenses); the fact that the aforementioned means are used to achieve the purpose while compromising individual liberties to the least degree practicable; sufficient proportionality when considering the adverse effects on individual liberties as opposed to the benefits afforded by the emphasis placed on the purpose in question.

³² In addition, in practical terms, it is conventionally held that legislative bodies possess greater resources and professional capabilities when compared to the court in their endeavors to set public policy.

judicial policy on security offenses – which is exceedingly severe – is not the product of an independent decision made by courts. Rather, it is founded on legislation.³³ Third, the formulation of this judicial policy notifies the legislature of an important gap in sentencing policy. The legislature may either implicitly approve of the court's actions, or it may legislate a different solution.³⁴

B. Instrumental Criticism: the 'null hypothesis' of severer criminal punishment

Assuming that the courts may properly take an active role in dealing with the limitations of enforcement, the judicial policy that underlies the justification for strict punishment on grounds of deterrence should be assessed. This paper does not focus on the normative question of whether it is morally permissible to employ stricter punishment for general deterrence purposes.³⁵ Instead, it focuses

³³ Furthermore, the more general policy of favoring deterrence when it comes to security offenses as a rule was determined and ratified over a long period by the courts, as described above in Part II.

³⁴ The appearance of judicial statements in court rulings that are explicitly directed at the legislature has been the object of a comprehensive empirical study, which sought to examine the judicial guidelines incorporated in various rulings of the Israeli Supreme Court. The insight gleaned from that study is that, as a rule, such guidelines do not notably affect actual legislation. See Liav Orgad & Shai N. Lavie, *Judicial Guidance: Comments on Legislative Amendments in Supreme Court Rulings*, 34 TEL-AVIV U. L. REV. 437 (2011) (Hebrew).

³⁵ For the broad debate regarding the morality of general deterrence consideration, See, e.g., ANDREW VON HIRSH, PAST OR FUTURE CRIMES: DESERVEDNESS AND DANGEROUSNESS IN THE SENTENCING OF CRIMINALS (1985). The argument that

on the specific instrumental considerations regarding cyber-NSOs – namely, the efficacy of that policy regarding achieving deterrence. Naturally, if this policy cannot achieve its deterrence goals, then it must be reconsidered, regardless of the normative debate.

As a starting point, one may refer to scholarly works dealing with the concept of deterrence-by-punishment, and the effects of penal severity on actual social conduct. The traditional assumption underlying the connection between strict sentencing and deterrence is that it is possible to deter criminals by undermining the "advisability" of the offense. Cast in a legal economic framework: if a certain act is more costly (in terms of the penal sanction imposed) when compared to the benefits afforded by the agent (the perpetrator) then a rational person would seek to avoid such an act.³⁶

This traditional assumption has been challenged by legal scholars, social scientists, and criminologists. In general, the emerging view in the literature claims that no solid evidence exists supporting the claim that stricter criminal sanctions result in reduced crime rates. These academics posit that absent proof of correlation between stricter punishment and decreased criminality, deterrence-

deviation from the principle of proportionality on general deterrence grounds is incommensurate with the principles of Israeli constitutional law or with those of Amendment 113 can be found in Oren Gazel-Eyal, *Improper Limitations: On the Principle of Proportionality and Its Application to Adequate Sentencing*, 6 MISHPATIM AL-ATAR, 1 (2013) (Hebrew); Ruth Kanai, *Structuring the Judge's Discretion in Determining Sentencing Pursuant to the Goldberg Committee Report*, 15 BAR-ILAN U. LEGAL STUD. 147 (1999) (Hebrew).

³⁶ Gary Becker, *Crime and Punishment: An Economical Approach*, 76 J. POL. ECON. 168 (1968).

by-punishment sentencing policies should be abandoned.³⁷ The proposed explanations for this apparent lack of correlation are diverse, but the prominent explanation is the theory that human beings are not necessarily rational actors.³⁸ However, even going beyond the criticism on the limits of rationality, another drawback to the deterrence-by-punishment model comes from within the rational-economic framework, which identified the deterring effect of punishment as dependent not only on the severity of the stipulated sanction, but also on the expectancy of punishment - the actual likelihood that a perpetrator will be caught and convicted.³⁹

³⁷ For a detailed presentation and assessments of this literature, see Anthony N. Doob & Cheryl Marie Webster, *Sentence Severity and Crime: Accepting the Null Hypothesis*, 30 CRIME & JUSTICE, 143 (2003); Cheryl M. Webster & Anthony N. Doob, *Searching for Sasquatch: Deterrence of Crime Through Sentence Severity*, THE OXFORD HANDBOOK FOR SENTENCING AND CORRECTION, 173 (2012). For the adoption of those insights in Israeli context, see Oren Gazal-Ayal & Ruth Lazer, *The Implications of starting Sentences*, 3 HUKIM – J LEG. 31 (2011) (Hebrew).

³⁸ This is added to other shortcomings, such as "inelastic demand" for the benefits of the offense or the increased value of the offense owing to stricter sanctions.

³⁹ Haim Wismonskey, *Sentencing Guidelines for Computer Crimes*, 24 BAR-ILAN L. STUDIES, 81, 106 (2008) (Hebrew). The approach whereby the severity of the sentence ought to correspond to the likelihood of being caught can already be found in the writings of John Locke, who focused on the instrumental aspects of sentencing as a means to guarantee rights. According to Locke's approach, which focuses on the deterring and preventative aspects of sentencing, a desirable punishment of a crime is not the one actually inflicted on a convicted felon, but should rather be the one a criminal might expect to face (likelihood of actual sentencing times the conventional sentence). See JOHN LOCKE, TWO TREATIES OF GOVERNMENT, Chap. II (1960).

Therefore, in the case of cyber-crime (and specifically cyber-NSOs), which is characterized by serious enforcement challenges, the increased severity of sentencing is limited in its ability to facilitate deterrence, even if we assume that the perpetrators think rationally. As the Israeli courts have emphasized, as more elements of a crime are committed in the cyber realm, the more difficult it becomes for authorities to identify the crimes and perpetrators. So, stricter sentencing does not tip the balance between the benefits afforded by the crime and the statistical probability of apprehension in the minds of the perpetrators. When the potential benefits of a crime reach a certain level, the would-be criminal will not be deterred no matter how severe the punishment because the chances of apprehension are too low. These insights pertain to the present discussion: the limited capacity to monitor potential terrorists, and the nearly infinite character of cyberspace, significantly restricts the ability of law enforcement agencies to locate and punish perpetrators. Therefore, perpetrators of cybercrimes assume a very small risk when considering the miniscule chances of ever being caught. Consequently, the deterring potency of criminal sanctions is undermined, regardless of their relative severity.⁴⁰

⁴⁰ One of the possibilities for dealing with the challenges of detecting and prosecuting online offenses, including cyber-NSOs, is placing significant weight on the cooperation of the accused with law enforcement agencies, out of a recognition that the accused's cooperation somewhat alleviates the limitations on enforcement stemming from the monitoring and identification difficulties. See Wismonskey, *Id.*, at 103. Wismonskey's argument can be viewed in a broader context: the enforcement difficulties that present themselves when dealing with online activity may be resolved by the application of

*C. Instrumental Criticism: The Limits of
Deterrence in Counter-terrorism*

The second limitation on the efficacy of deterrence, in our context, is the emerging understanding that traditional concepts of deterrence are unlikely to effectively influence terror agents, as indicated by multi-disciplinary terror-related studies.⁴¹ The explanations for this phenomenon are based on the unique characters of terror action incentives, or in Abrahms' words - "Terrorist tend to be undeterrable".⁴² These studies suggest that terrorists are not motivated by simple utilitarian aims. Therefore, achieving deterrence only through imposing higher penalties on their actions may not be possible, because one of the basic incentives fueling acts of terror is the expectation that the public and the state will discover and react to the illegal action. Also, because terrorists are commonly fanatical ideologues, they tend to perceive the risk of their own apprehension and punishment as irrelevant to the subjective value of their criminal actions. Those insights are supported by a broad body of scholarly work, which suggested that deterrence has

incentives rather than sanctions.

⁴¹ See GLENN H. SNYDER, *DETERRENCE AND DEFENSE: TOWARD A THEORY OF NATIONAL SECURITY* (1961); Todd Sandler & Kevin Siqueira, *Global terrorism: Deterrence Versus Pre-emption*, 39 CANAD. J. OF ECO., 1371 (2006); Robert F. Trager & Dessilava P. Zagorcheva, *Detering Terrorism*, 30 Int. Sec. 87 (2006); Bruno S. Frey & Simon Luechinger, *How to Fight Terrorism: Alternatives to Deterrence*, 14 DEFENSE & PEACE ECO. 237 (2003).

⁴² Max Abrahms, *Detering Terrorism: A New Strategy*, 3(8) PERSPECTIVES ON TERRORISM 2 (2014).

limited efficacy as a counter-terrorism policy.⁴³

The complexity of deterring terrorism is extensive, but even when accepting this basic understanding, it has great consideration when debating deterrence-by-punishment as a legal policy in the war against terror. In this paper, the aforementioned analysis strongly suggests that a sentencing policy that hopes to achieve deterrence through severe criminal punishments cannot apply to NSOs in the manner that it can be applied to other criminal offenses. Israeli courts have not yet realized this, however. They attempt to equally apply the deterrence-by-punishment principal in NSOs as in other criminal offenses. And moreover, courts actively state that deterrence is the prominent consideration of sentencing terror crimes to be achieved through punishment severity.

D. Conclusions: possible policy guidelines

Even though these insights somewhat undermine the basis for the judicial policy of punishing cyber-NSOs harshly, the policy need not be rejected in its entirety. It should simply be acknowledged that stricter sentencing is of limited utility, on its own, for deterring cyber-NSOs. Accordingly, we ought to consider more refined solutions to this phenomenon.

To begin with, it should be stressed that the above criticism does not mean that stricter sentencing fails in achieving deterrence, but rather that no significant link was ever found between strict sentencing and deterrence. This does not necessitate

⁴³ For an elaborate explanation of the phenomenon, see Abrahms, *Id*; Andrew H. Kydd & Barbara F. Walter, *The Strategies of Terrorism*, 31 INT. SECURITY, 49 (2006).

the conclusion that no such link exists. In light of that, are the rationales underlying the criticisms dealing with cybercrimes and traditional NSO fully applicable to cyber-NSOs?

It is important to specify that those insights mainly address the fundamental terrorist, and not necessarily their supporters, who typically behave according to a more common incentive structure.⁴⁴ Therefore, the effectiveness of deterrence-by-punishment regarding the terror supporters might be greater. In light of this analysis, Abrahms concluded: "terrorism is deterrable, even if many of its practitioners are not."⁴⁵ Most of the criminal cases adjudicated in courts dealt with different supporters of terror. Typically, these defendants committed NSOs by facilitating attacks or information leaks, but were less ideologically involved than the core terror perpetrators and did not commit attacks themselves.

So adoption of a deterrence-by-punishments policy is likely to be more effective on cyber-NSOs, because the perpetrators of those offenses tend to be secondary supporters of the 'hardcore terrorists'. The Israeli cases discussed above are examples of this trend: the defendants all sought lenient sentences because before their prosecuted crimes they were "law-abiding" citizens.

This observation leads to a second important insight: the phenomenon of a 'conceptual gap' regarding the subjective perception of cyber-NSOs. The case law presented above demonstrated a recurring theme in the defendants' claims. They described themselves as "law abiding citizens" and relatively unaffiliated with the terrorist ideology. If

⁴⁴ Abrahms, *supra* note 42, at 5-7.

⁴⁵ *Id.* at 11.

those arguments accurately reflect the defendants' authentic views, one may deduce there exists a conceptual gap between citizens at large (particularly those inclined to assist in committing NSOs) and the authorities (the Israeli court system) trying to deter this conduct. In other words, the defendants' arguments, described above, may reflect their subjective perception of the severity of the acts committed and their actual criminality; they may genuinely believe that a criminal act committed in cyberspace should result in lighter sentences because the crimes are less serious.

I believe this gap, as identified in numerous fields of online criminal activity, is caused by the shift into cyberspace that creates a certain distance between the agents committing the act and their criminal environment. Moving criminal activity online significantly blurs the physical aspect of the crime, and by so doing may lead perpetrators to pursue their transgressions with greater abandon. This hypothesis is supported by academic literature that examines the intersection of law and technology. One example is the perceived normalization of copyright infringement by digital means – namely, the false subjective notion that digital copyright infringement (copying, public performance, etc.) is morally permissible, or, at the very least, that such acts are of lesser severity when compared to their physical counterparts.⁴⁶ In other words, the online nature of the act had influenced the way it is morally

⁴⁶ See Geraldine Scott Moohr, *The Crime of Copyright Infringement: An Inquiry Based on Morality, Harm, and Criminal Theory*, 83 B.U. L. REV. 731 (2003); SAMEER HINDUJA, MUSIC PIRACY AND CRIME THEORY (2006); George Higgins et al., *Digital Piracy: a Latent Class Analysis*, 27 SOC. SCI. COMP. REV. 24 (2009).

perceived by users. A possible explanation for this phenomenon suggests that the ease with which the act is committed, coupled with the low probability of being caught, leads perpetrators to rationalize the crime by comparing it to traditional crime, which is often more difficult to accomplish and carries a higher likelihood of apprehension and punishment. If cybercrime is so much easier and the chance of apprehension so much lower, the perpetrator concludes that the crime must not be as “bad.” As we saw earlier, the Court is cognizant of this phenomenon, as it addresses the relative ease of committing the forbidden act and the low likelihood of being caught by law enforcement agencies. These characteristics of cybercrime, in the courts’ view, warranted more severe punishment.

Can these insights apply to cyber-NSOs as well considering they constitute a unique class of offenses? It appears that we should not rule out, when dealing with cyber-NSOs, the possibility that the shift towards cyberspace may also result in a false notion of normalization. The technological nature of cyberspace – with its ready availability, globalism, and anonymity – ideally accommodates the needs of terrorism-related actions, but it might also result in the perpetrators of such crimes perceiving their actions as less serious or reprehensible. In the past, security offenses involved various physical acts that substantially deviated from the routine lives of “normal” individuals (such as actual proximity to foreign operatives, the delivery of physical items, social circles that allow access to terrorist elements, etc.). Cyber NSOs, however, eliminate much of the foregoing. Perpetrators of NSOs no longer need to make physical contact with enemy agents, travel in the same social or political circles as those

individuals, take possession of tangible property, or even leave the comfort of their own homes. This may cause a false sense of normativity concerning cyber-NSOs.

Assuming that such a phenomenon exists, it would require further exploration of the legal policy regarding cyber-NSOs. A possible answer comes from expressive approach to criminal law, which posits that the declarative role of criminal law itself plays an important role in creating desirable social norms.⁴⁷ The expressive approach regards criminal law as a means of communicating with potential offenders, as well as the public at large, and emphasizes the clarity of messages conveyed by such means. This approach maintains that specifically defined criminal law offenses send a clearer message to the public regarding the unacceptability of a proscribed behavior. In other words, legislation that entails greater specificity results in higher declarative-expressive value, which reinforces the perception of a certain behavior as non-normative.⁴⁸ This approach is especially relevant to anti-terrorism legislation, which specifically contains an

⁴⁷ Elizabeth S. Anderson & Richard H. Pildes, *Expressive Theories of Law: A General Restatement*, 148 U. PA. L. REV. 1503 (2000); Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338 (1997).

⁴⁸ Naturally, court rulings also fulfill a declarative role, but their expressive contributions alone are limited, compared to the legislature. In the substantive context, legislation constitutes an expressive act engaged in by the legislature in its sovereign capacity. In practice, the majority of the public is more familiar with legislation than with case law. Nevertheless, even assuming that case law has substantial expressive value, the added endeavors of legislation seeking to better convey the message would significantly augment its potency.

expressive-declarative purpose.⁴⁹

Explicit references to security offenses committed in cyberspace may, therefore, substantially affect the false perception of normalization described above. This conclusion is supported by the fact that the Israeli Criminal Code does not expressly address the online aspects of security offenses. This limits the capacity of the judicial branch to independently manage changes in social norms, especially when its chief purpose comprises imposing sanctions, rather than formulating criminal prohibitions. The laws prohibiting cyber-NSOs would have a greater deterring effect if they were amended to specifically address NSOs committed in the cyber realm. The reference to cyber activity need not identify the cyber nature of the crime as an aggravating or mitigating factor; it need only clarify that the online version of the offense is of a different character, but equally reprehensible. One possible way that new legislation may be adjusted would be the formulation of sanctions that restrict the defendant's ability to use online systems, in addition to the deprivation of liberties (the general sanction provided by penal law).

Academic literature has addressed the possibility of dealing with the challenges of cyber-crime by using specific legislation. Although this argument was raised in connection with "offenses against computers,"⁵⁰ the rationale underlying the formulation of contextual-specific legislation can be readily applied to offenses *by* computers, including cyber-NSOs. In the Israeli literature on law and

⁴⁹ Walker, *supra* note 13, at 61.

⁵⁰ Wismonskey, *supra* note 39.

technology, specific legislative reference to the circumstances of the criminal act were defined as "necessary surgical tools" for delineating prohibitions,⁵¹ and this surgical tool can be used to answer many of the challenges mentioned in this context.

The proposed legislative amendments to criminal laws address both the institutional and instrumental challenges created by cyber-NSOs as mentioned above. As to the institutional difficulties, the solution proposed here is clear: legislative changes necessitate the legislature's involvement, which would likely entail a public debate. Regarding the instrumental limitation of deterrence-by-punishment, if we accept the argument that stricter sentencing does not necessarily lead to reduced crime rates or deterrence, then it may be argued that stricter laws will also fail to substantially affect social conduct. In the author's view, however, in the particular case of cyber-NSOs, these amendments would increase deterrence by diminishing the false notion of normativity commonly ascribed to acts committed in cyberspace.

VI. CONCLUSION

The basic conclusion drawn from the above discussion is that courts and policy-makers must be aware of the deterrence limitations regarding cyber-NSOs. Deterrence-based sentencing makes false promises, since as long as we believe that crime can be deterred through harsh sentences, there is no need

⁵¹ Assaf Harduf, *Criminal Law Surfs the Internet: The Physical-Virtual Element*, 52 HAPPRAK'LIT 67, 73 (2003) (Hebrew).

to consider other approaches. When accepting the limitations of deterrence-by-punishment as a legal response to cyber-NSOs, we may develop insights regarding counter-terrorism or cyber-crimes, such as how to effectively focus on terrorist supporters, or how to use incentives mechanisms rather than severe sanctions to fight terrorism. These proposals are not a silver bullet for fully dealing with the challenges and threats posed by cyberterrorism. As experience teaches us, criminal law fails to fully eradicating criminal behavior of any kind, let alone cybercrime, no matter how well-written and effectively enforced the criminal law may be. The justice system is only one of many tools used for combating terrorism. The Supreme Court's policy, as presented in this paper, indicates that the Court does, in fact, assume an active role in dealing with cyber threats, and has identified the challenges facing the legal system, especially regarding combating cyber-NSOs. But for a deterrence-oriented policy to attain its purpose, efforts by the legislature are needed as well, so that, in collaboration with the courts, the national security and justice systems may form a unified, clear and visible front. And although this paper specifically addresses cyber-NSOs, it may be relevant in a broader context adding to a substantial corpus of work that deals with the legal and criminological aspects of online activity. It is clear that the challenges arising in the transition from physical to online acts are not unique to security offenses. Therefore, the proposed solutions for dealing with the specific challenges of online security offenses may apply, *mutatis mutandis*, to other instances of regulating online activity.

