INTERNATIONAL
COUNTER-TERRORISM
REVIEW

VOLUME I, ISSUE 1

February, 2020

The Evolving Law on Cyber Terrorism

Dilemmas in International Law and Israeli Law

ADV. DEBORAH HOUSEN-COURIEL

ABOUT ICTR

The International Counter-Terrorism Review (ICTR) aspires to be the world's leading student publication in Terrorism & Counter-Terrorism Studies. ICTR provides a unique opportunity for students and young professionals to publish their papers, share innovative ideas, and develop an academic career in Counter-Terrorism Studies. The publication also serves as a platform for exchanging research and policy recommendations addressing theoretical, empirical and policy dimensions of international issues pertaining to terrorism, counter-terrorism, insurgency, counter-insurgency, political violence and homeland security. ICTR is a project jointly initiated by the International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center (IDC), Herzliya, Israel and NextGen 5.0.

The International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world. Founded in 1996, ICT has rapidly evolved into a highly esteemed global hub for counter-terrorism research, policy recommendations and education. The goal of the ICT is to advise decision makers, to initiate applied research and to provide high-level consultation, education and training in order to address terrorism and its effects.

NextGen 5.0 is a pioneering non-profit, independent, and virtual think tank committed to inspiring and empowering the next generation of peace and security leaders in order to build a more secure and prosperous world.

COPYRIGHT

CONTENTS

Introduction **5**
Current Trends and Dilemmas **6**
Legal Initiatives **9**
Other Initiatives **11**
Comparison and Analysis **15**
The Spectrum of Cyber Terrorism Activities **16**
The Israeli Case **18**
Four Observations **23**
Conclusion **25**

ABSTRACT

Cyber attacks present one of several new challenges to global, national and personal security that result from cyber space weapons development and deployment. These new threats are a daily occurrence in every country and range from ongoing attacks on governmental institutions to the January 2012 "Saudi hacker" breaches of Israeli credit card databases. International law is currently taking important initial steps to address the illegality of cyber attacks and states' right to defend against them in general, and is making inroads regarding cyber terrorism in particular. Nonetheless, much ambivalence remains in both international and Israeli law regarding its definition and ramifications.

This ambivalence has so far curtailed the development of definitive normative prescriptions applicable to cyber terrorism. Nonetheless, a present focus of threat assessment is the vulnerability of critical infrastructures and networks to cyber terrorism attacks. Due to the ability of terrorists to leverage potentially devastating cyber attacks at relatively low cost to themselves, this area of asymmetry should become prioritized as new arena for counter-terrorism law and policy. Indeed, it seems to be garnering "fast track" treatment due to the particular threats these attacks pose.

In this article, the emerging international legal norms prohibiting cyber terrorism will be examined; and the relevant provisions of Israeli legislation will be analyzed in a comparative context. In conclusion, four observations about present trends and global legal developments will be offered.

Keywords: *cyber, international law, cyber terrorism, Israel*

INTRODUCTION[1]

Hostile cyber attacks have become front-page news. Increasingly, they are described as cyber terror attacks by journalists, decisionmakers and the perpetrators themselves. Several recent examples are representative:

- In January 2012, tens of thousands of Israelis were the unwilling victims of 0xOmar, a hacker claiming to be a Saudi national whose plan was to use cyber terrorism in order to "...hurt Israel -- politically, economically and culturally," as the hacker wrote in an email exchange with an Israeli media source[2]. The 0xOmar attacks targeted and exposed the personal and credit card data of Israelis, Jewish and Arab alike, on readily accessible websites. They caused uproar in the Israeli media, and among government leaders, politicians and consumer privacy groups, instigating an unprecedented public debate over the state of the country's cyber security readiness[3].

- On May 22, 2012 an Al-Qaeda video calling for "electronic jihad" against infrastructure and other targets was shown by the FBI to the US House of Representatives' Homeland Security and Governmental Affairs Committee. Chairman Senator Joe Lieberman stated: "This is the clearest evidence we've seen that Al Qaeda and other terrorist groups want to attack the cyber systems of our critical infrastructure ...."Congress needs to act now to protect the American public from a possible devastating attack...on our electric grid, water delivery systems or financial networks, for example." [4]

- In retaliation for the anti-Muslim video called "The Innocence of Muslims" that was posted on Google's YouTube in September 2012, the Izz ad-Din al-

---

[1] This article was initially published in 2013

[2] H. Sternlicht, I. Gattegno, Z. Klein, "Striking again, Saudi hacker says 'I want to hurt Israel', Israel HaYom, January 6, 2012 (http://www.israelhayom.com/site/newsletter_article.php?id=2536); and D. Housen-Couriel and R. Levi, "The Saudi Hacker: A New Era in Israel's Cyberspace", Israel Defense, 17.1.2012

[3] D. Or-Hof, "This is How the Country Abandons You During a Cyber Terror Attack" (Hebrew), The Marker, 9.2.2012 (http://www.themarker.com/hitech/1.1637778); Knesset Committee on Science and Technology, Protocol #116, January 10, 2012 (Hebrew) ; Housen-Couriel and R. Levi, *ibid*.

[4] CNN, "US senators: Al-Qaeda calls for 'electronic jihad'", May 23, 2012 (http://edition.cnn.com/2012/05/23/politics/al-qaeda-electronic-jihad/index.html). See also M. Moss and S. Mekhennet, "An Internet Jihad Aims at US Viewers, New York Times, October 15, 2007 (http://www.nytimes.com/2007/10/15/us/15net.html?pagewanted=all); and T. Nouveau, "FBI Says It is Concerned Over Cyber Terror", TG Daily, March 9, 2012 (http://www.tgdaily.com/security-features/61983-fbi-says-it-is-concerned-over-cyber-terror).

Qassam Cyber Fighters launched Operation Ababil, a series of DDoS attacks against major banks in the West which utilize Google cloud hosting, including Bank of America, Citigroup, Wells Fargo, BB&T and HSBC[5].

- During Operation Pillar of Defense, Israel's Minister of Finance proclaimed that Israel had been exposed to 100 million internet attacks on private, commercial and government websites, including 44 million on government sites.[6] Many of these were carried out by elements hostile to Israel and made their hostile intent clear by "signing" websites and malevolent messages.

All of the above incidents raise clear and urgent questions about the nature and scope of real-world damage that can - and cannot - be wreaked by hostile actors leveraging the power of the internet, and the ways in which the international legal system and global policymakers should be coping with such threats.

But are they cyber terrorism?

CURRENT TRENDS AND DILEMMAS

Terrorists aim to inflict psychological and physical damage on civilian, commercial and governmental targets, in order to make a political and ideological statement[7]. Terrorism differs in a crucial way from other criminal activity because of the determination of its perpetrators to cause widespread fear and panic. Yet precise, legally-enforceable definitions of terrorism have

---

[5] See "Cyber Terrorists Threaten Fresh Attacks against US Banks", Fox Business, December 11, 2012 (http://www.foxbusiness.com/industries/2012/12/11/cyber-terrorists-threaten-fresh-attacks-against-us-banks/); The Huffington Post headline was "Izz Ad-Din Al-Qassam Cyber Fighters Group Takes Break From Hacking Banks To Celebrate Eid Al-Adha Holiday", 23 November 2012. (http://www.huffingtonpost.co.uk/2012/10/23/muslim-hacktivist-al-qassam-takes-holiday-break_n_2005637.html). US officials have since decided that Iran is behind these attacks, see N. Perlroth and Q. Hardy, "Bank Hacking Was the Work of Iranians, Officials Say", New York Times, January 8, 2013. See also R. Levi, "Did Iran Attack the US Banks?", Israel Defense, January 11, 2013.

[6] N. Tucker and O. Hirschauge, "Cyber offensive against Israel: 100 million attacks with little to show for it", HaAretz, November 12, 2012.

[7] Definitions of terrorism abound, and a full review of them is well beyond the scope of the present analysis. See, for example, B. Ganor, The Counter Terrorism Puzzle: A Guide for Decisionmakers, IDC Herzliya, 2005; and E. Gross, Democracy versus Terror: Where are the Limits?, Haifa University, 2002.

so far eluded international legal experts and policymakers[8]. Tellingly, one of the leading efforts at international codification, the UN Draft Convention on International Terrorism has been in committee since 2000 and is currently deadlocked over definitional issues[9].

Likewise, there is no agreed concept at the international level of what cyber terrorism is, and it is a controversial and divisive term even among those decision makers who have responsibility for preventing hostile cyber attacks[10]. Jim Harper, the Director of Information Policy Studies at the CATO Institute, has said "There's no such thing as cyber terrorism." "Both cyber terrorism and cyber warfare are concepts that are gross exaggerations of what's possible through internet attacks."[11] Moreover, in its recent re-evaluation of cyber preparedness among member states, the OECD has refrained from defining cyber terrorism as a key threat in the international arena.[12]

On the other hand, the threat of cyber terrorism is unmistakably on the global agenda. UN Secretary General Ban Ki-Moon has said:

> *The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner*[13].

And a recent survey of top-level information security professionals meeting in the US has noted that 79% of them believe there will be a "major" cyber terrorism event in 2013[14]. The World Economic Forum has identified cyber

---

[8] See M. Scharf, "Special Tribunal for Lebanon: Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, Introductory Note, 50 ILM 509 (2011), pp. 509-602, at 509.

[9] See the website of the Ad Hoc Committee established by UN Resolution 51 / 210 of 17 December 1996 (http://www.un.org/law/terrorism/).

[10] See V. Baranetsky, "What is Cyberterrorism: Even Experts Can't Agree", Harvard Law Record, November 5, 2009, p. 1.

[11] Quoted in an interview with RT, July 31, 2009 (http://rt.com/news/no-cyber-terrorism-obama/)

[12] See OECD, Cybersecurity Policy Making at a Turning Point, OECD Digital Economy Papers, No. 211, November 2012, p. 5 and p.16. The non-economic cyber threats listed include hacktivism, destabilization, espionage, sabotage and military operations.

[13] Quoted in the prologue of United Nations Office on Drugs and Crime (UNODC), The use of the internet for terrorist purposes, New York, September 2012.

[14] S. Gallagher, "Security pros predict “major” cyber terror attack this year", Ars Technica, January 4, 2013

terrorism, in the form of "digital wildfires" as a global risk in 2013[15]. And in the legal arena, several key international bodies have initiated draft treaties or codes to cope with cyber terrorism, as will be seen herein. One current example is the European Commission's CleanIT framework to prevent terrorists' exploitation of the internet[16].

The legal and policy complexities of defining "cyber terrorism" in order to serve the aims of deterrence, operational prevention and enforcement[17] are burdened with two interlocking sets dilemmas. The first set consists of those surrounding the definition and prohibition of "terrorism" itself; and the second encompasses the additional complexities around the new threats posed by state and non-state actors in cyber space[18].

The latter set of cybersecurity dilemmas is addressed in a recent edition of Foreign Affairs, where Valeriano and Maness write in "The Fog of Cyberwar" about the threat of cyberwar not living up to the hype around it, as a new dynamic of deterrence is already in effect:

> *Far from making interstate cyberwarfare more common, the ease of launching an attack actually keeps the tactic in check. Most countries' cyberdefenses are weak, and a state trying to exploit an adversary's weakness may be similarly vulnerable, inviting easy retaliation. An unspoken but powerful international norm against civilian targets further limits the terms of cyberwarfare[19].*

---

15 World Economic Forum, Global Risks 2013, 8th ed., January 2013.

16 See http://www.cleanitproject.eu and the discussion at note 39 *infra*.

17 See a different triad of aims in "Cyber warfare: hype and fear", The Economist, December 8, 2012, where computer security expert Jarno Limnell of Stonesoft identifies the following as key: "...resilience under severe attack; reasonable assurance of attribution so that attackers cannot assume anonymity; and the means to hit back hard enough to deter an unprovoked attack."

18 A recent example of the ambivalence around rules of jurisdiction in cyber space is the inconclusiveness International Telecommunications Conference in Dubai, held in December 2012. There, member states could not arrive at consensus on internet governance, permitted content, and other issues. See S. Cherry, "ITU Succeeds in Doing Nothing", IEEE Spectrum, December 14, 2012

19 B. Valeriano and R. Maness, "The Fog of Cyberwar", Foreign Affairs, November 21, 2012. See also D. Betz and T. Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power, International Institute for Strategic Studies, 2011. See also M. Iqbal, "Defining Cyberterrorism" in 22 J. Marshall J. Computer & Info. L. 397 (2003-2004) and G. Weimann, "Cyberterrorism: How Real is the Threat?", Special Report, United States Institute of Peace, 2009.

And yet they are much more ambivalent about the prevention of cyber terrorism:

> *To be sure, cyberterrorism is still a danger. This is a development that will be more difficult to deter*[20].

In light of this challenge, the international community has turned its attention to elucidating the key definitional elements of cyber terrorism in order to meet the three aforementioned aims of deterrence, operative prevention and enforcement. Several initiatives are currently under development, as discussed in the following section.

INTERNATIONAL LEGAL INITIATIVES TO DEVELOP A PROHIBITION OF CYBER TERRORISM: NATO'S TALLINN MANUAL

In the National Cybersecurity Framework Manual of 2012[21], a group of NATO experts sets out the challenge of forging appropriate rules of international law in cyber space:

> *It is reasonable to presume that cyberspace could be used as a vector for initiating physical attacks to further the aims of a terrorist: terrorist groups also use cyberspace to recruit, spread propaganda and organise their activities…. Cyber terrorism is not specifically proscribed in any international convention, which is of special importance due to the fact that international law on terrorism is scattered, and the means used (cyber technique, kinetic energy, etc.), have an effect on the applicable law*[22].

Nonetheless, the process of defining "cyber terrorism" in a way that furthers the development of a prohibitory norm has been furthered in NATO's recently published Manual on the International Law Applicable to Cyber

---

[20] Valeriano and Maness, *ibid*.

[21] A. Klimburg (ed.), "Cyber-enabled terrorism", in National Cybersecurity Framework Manual, CCDOE, Tallinn, 2012, pp. 155-7.

[22] *Ibid*, pp. 155-6. The "scattering" of norms is also evident in the variety of treaties dealing with "ordinary" terrorism. See *infra* at note 43.

Warfare ("the Tallinn Manual").[23] There, a group of international experts has distinguished cyber terrorism from cyber crime, cyber harassment, sabotage, hackerism and terrorism that is not cyber-related, by defining cyber terrorism attacks as follows, in Rule 36:

> *".... Cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population...."*[24]

Where a "cyber attack" is defined 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."*[25]

The commentary on Rule 36 elucidates several additional, crucial characteristics of cyber terrorism:

- Its purpose is to instill terror among civilians, not military personnel, although the latter may also be terrorized as a result of the same act;[26]
- The intent to terrorize must be directed toward a wide population and go beyond the intent to influence a few individuals;[27]
- A threat to attack by cyber terrorism is also prohibited.[28] The example given by the Group of Experts is instructive:

> *"For instance, the threat to use a cyber attack to disable a city's water distribution system to contaminate drinking water and cause*

---

[23] The Tallinn Manual on the International Law Applicable to Cyber Warfare, ed. Michael Schmitt, Cambridge University Press, 2013, pp. 104-6 (web draft). See also M. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", Harvard International Law Journal, Online Version, Vol. 54, December 2012.

[24] Tallinn Manual, Rule 36, *ibid*, p. 104.

[25] Rule 30, *ibid*, pp. 91-92.

[26] "It must be emphasized that the essence of the prohibition is its focus on the purpose of a cyber attack, specifically the spreading of terror among a civilian population. While a lawful cyber attack against a military objective, including combatants, might cause terror, this is not the type of attack covered in this Rule."(*ibid*)

[27] *Ibid*, "A violation of Rule 36 requires an intent to spread terror amongst the population....terrifying one or only a few individuals, even if that is the primary purpose of the act or threat, does not suffice, although engaging in an act of violence against one person in order to terrorize a significant segment of the population would violate this Rule." (*ibid*)

[28] "The prohibition in this Rule extends to threats of cyber attacks, whether conveyed by cyber or non-cyber means." (*ibid*)

death or illness would violate the Rule if made with the primary purpose of spreading terror among the civilian population. On the other hand, consider the example of a false tweet (Twitter message) sent out in order to cause panic, falsely indicating that a highly contagious and deadly disease is spreading rapidly throughout the population. Because the tweet is neither an attack nor a threat thereof, it does not violate this Rule."[29]

In summarizing Rule 36, it is important to provide the context of the more general work of the group of experts on the use of force in cyber space, formulated in Rule 11. This Rule proposes that a cyber attack having the same "scale and effects" as a physical attack should be categorized as a use of force, giving rise to a right of self-defense under international law[30]. The scope of the present article does not permit analysis of this compelling and core issue, which has ramifications for the activities of states in cyber space during peacetime and war[31].

In summary, the Tallinn Manual addresses cyber terrorism as a particular type of cyber attack, with the main distinguishing factor being the perpetrator's intent to terrorize a large civilian population. There is no specification that the terror be politically or ideologically motivated, nor does the Tallinn definition encompass terrorist's utilization of the internet for purposes such as recruitment, fundraising and propaganda. In line with the Manual's treatment of the use of force in general, the prohibition encompasses any threat of cyber terrorism, as well as an actual cyber terrorism attack[32].

OTHER INITIATIVES

Other leading policy and law-enforcement bodies other than NATO that have developed working definitions and characterisations of cyber terrorism include:

---

[29] *Ibid*.

[30] Rule 30, *ibid*.

[31] For a detailed discussion and analysis of the "scope and effects" paradigm, see M. Schmitt, 'Cyber Operations and the Jus in Bello' (2011) 87 Naval War College Intl L Studies 89, 92–94 and M. Schmitt, "Classification of Cyber Conflict", J Conflict Security Law (Summer 2012) 17 (2):245-260, at 251-2.

[32] See the analysis of international cyber conflict carried out by non-state actors, including issues of state responsibility, in M. Schmitt, "Classification of Cyber Conflict", *ibid* at 253-4.

- the US Department of Defence[33];
- The Center for Strategic and International Studies (CSIS)[34];
- the FBI[35];
- FEMA[36]
- OSCE[37];
- the UN's Working Group on Countering the Use of the Internet for Terrorist Purposes[38];
- the ITU[39];
- the EC[40]; and
- the Council of Europe.[41]

The latter two bodies have progressed to common definitions of terrorism that are binding on EU member states via the 2002 Council Framework

---

[33] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, 15 August 2005, p. I-4: "Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves."

[34] CSIS has defined it as "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population." (James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, 2002, p. 1).

[35] "The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." As cited in S. Gordon and R. Ford, Cyberterrorism?, Symantec White Paper, p.4 (no date).

[36] Referenced in ENISA Threat Landscape, 8.1.2013 (https://www.fas.org/sgp/crs/terror/RL32114.pdf).

[37] Brussels Ministerial Declaration of 7 December 2006, Decision No. 7/06, "Countering the Use of the Internet for Terrorist Purposes", at #9 (http://www.osce.org/mc/23078).

[38] UNODC, *supra* note 12.

[39] See the ITU's 2010 Toolkit for Cybercrime Legislation , and its analysis below.

[40] See "Definition" and "Terrorist Use of the Internet" in "CleanIT Draft Document: Reducing Terrorist Use of the Internet", on the website of the EU's CleanIT initiative (http://www.cleanitproject.eu/about-the-project/). A document from CleanIT was leaked in September 2012 and became subject to criticism for its erosion of civil liberties (http://theintelhub.com/2012/09/27/leaked-eu-cyber-terror-proposal-would-erode-civil-liberties/). See also EC Regulation 881/2002 of 27 May 2002, art. 1.2, which prohibits the provision of internet services to terrorists.

[41] Council of Europe, "Cyberterrorism – the use of the internet for terrorist purposes", 2008 (http://book.coe.int/EN/ficheouvrage.php?PAGEID=36&lang=EN&produit_aliasid=2227).

Decision on combating terrorism[42] and the subsequent 2005 Convention on the Prevention of Terrorism[43]. These two legal instruments prohibit all offences defined as terrorism under the 12 existing international counter-terrorism conventions in force, in a variety of contexts such as airspace and the high seas[44].

Additionally, in the academic context, a 2001 draft treaty against cyber crime and terrorism was proposed by Stanford University's Hoover Institution[45], prohibiting acts using a cyber system "as a material factor" in offenses defined in existing counter-terrorism treaties, such as the 1963 Tokyo Convention.[46]

Finally, the 2001 Budapest Convention on Cyber Crime[47], the sole example of treaty law regulating cyber space, establishes an important legal base for the future development of cyber terrorism law at the multilateral level. Although the Convention addresses cyber crime without specifically addressing cyber terrorism, it does establish a framework for international cooperation at three levels: (a) standardizing the legal concepts of cyber crime; (b) establishing common concepts of prosecution of cyber crime; and (c) requiring

---

42 Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA), Official
Journal of the European Union, L 164; updated by the Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, Official Journal of the European Union, L 330.). The definition of a terrorist crime was not changed as a result of the 2008 Decision.

43 Referenced in Klimburg, supra note 20 at p. 157 (http://conventions.coe.int/Treaty/en/Treaties/html/196.htm). The text notes: " A defining feature of the Convention is Article 5, which contains a definition of a 'Public Provocation to Commit a Terrorist
Offence', the first attempt by international law to define incitement to terrorism. It is controversial due to the inclusion of 'indirect' incitement. The limits of this concept are not defined; however Article 12 requires parties to implement the offence in a way that is compatible with the right to freedom of expression as recognised in international law. States face a challenging task balancing the prevention of terrorism (including cyber-enabled terror) with the requirements of the Convention and relevant human rights principles."

44 "Since 1963, the international community has elaborated 14 conventions (of which 12 are in force), and four amendments to prevent terrorist acts. Those conventions are developed under the auspices of the UN and they address specific terrorist acts, like bombings, or specific environments, like the maritime safety." (*ibid*, at Note 494).

45 Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, in A. Sofaer and S. Goodman (ed.'s), The Transnational Dimension of Cybercrime and Terrorism, Hoover National Security Forum Series, 2001, p. 249.

46 See *ibid*, Article 3(1)(f).

47 Council of Europe, Convention on Cybercrime, European Treaty Series #185, 23.11.2001. The 8th Plenary Session of the signatories ' Convention Committee took place in December 2012.

cooperation among member states for data exchange and early warning of cyber threats[48]. Thirty-eight states have ratified the Convention[49] (as of winter 2013, Israel has nearly completed its accession) and have thereby committed to harmonizing their domestic legislation with its substantive categories of prohibitions: offences against the confidentiality, integrity and availability of computer systems and data[50], computer-related offenses[51], and content-related offenses[52].

These latter offenses are elaborated in the Additional Protocol to the Convention Concerning the Criminalization of Acts of a Racist and Xenophobic Nature committed through Computer Systems[53]. The Protocol prohibits several actions that are relevant to the prevention of terrorism, such as the dissemination of racist and xenophobic material through computer systems and racist and xenophobic-related threats delivered through computer systems[54].

In this same context of the prevention of cyber crime, the work of the International Telecommunications Union (ITU) is worth noting, both for its survey of national legislation on cybercrime and its valuable 2010 *Toolkit for Cybercrime Legislation*, which provides sample legislative prohibitions of cyber

---

[48] The Convention serves as the basis for the Council's Global Project on Cybercrime, which holds an annual Octopus Conference. See http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus2012/Interface2012_en.asp.

[49] See the chart of accessions and ratifications at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[50] Ibid, Title I.

[51] Ibid, Title II.

[52] Ibid, Title III.

[53] Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature committed through Computer Systems, Strasbourg, 28.1.2003, European Treaty Series #189. Article 2 defines “racist and xenophobic material” as "...any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors. Twenty states have ratified the Additional Protocol. Israel is not presently considering accession. (http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG).

[54] Articles 3 and 4, respectively. Israel is not considering accession to the Additional Protocol at present.

terrorism in line with the Budapest Convention's proscriptive categories.[55] The relevant provisions include unauthorized access for purposes of terrorism, unauthorized access to or acquisition of computer programs or data for purposes of terrorism, intent to cause interference or disruption for purposes of terrorism, and intent to furtherance of terrorism[56].

The *Toolkit* notes that these provisions extend beyond the existing provisions of most ITU member countries, as well as the existing provisions of the Budapest Convention.[57] The updated 2012 ITU publication on cybercrime legislation addresses "terrorist use of the internet", as well[58], to include ancillary activities to the terrorist attack itself such as the abovementioned recruitment, fundraising and propaganda. This trend of identifying a spectrum of terrorism activities in cyber space, beyond the terrorism attack itself, will be elaborated upon below.

COMPARISON AND ANALYSIS OF INTERNATIONAL INITIATIVES

The definitions and characterizations of cyber terrorism analyzed above are all relatively new. Many share a reticence to definitively distinguish cyber terrorism from other forms of terrorism. Several advocate a co-reading of prohibitions on terrorism in existing international counter-terrorism treaties with the 2001 Budapest Convention on Cybercrime, reviewed below. Some utilize a definitional framing of "terrorist use of the internet" rather than "cyber terrorism", emphasizing that cyber attacks are more of a tool of terrorism rather than a type of terrorism.

---

55 ITU, Toolkit for Cyber Crime Legislation, ITU and American Bar Association, Draft Rev., December 2010.

56 Respectively, Articles 2(d), 3(f), 4(f), and 6(h). The text is as follows: "Whoever commits an offense under [article] with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to cyberterrorism, shall be punished by a fine of [amount]and imprisonment for a period of [_]."

57 See p. 32: "The substantive provisions in the Sample Language are harmonized with the language and intent of cybercrime laws in most developed nations and the CoE Convention. The provisions go beyond these laws in that they set forth sample provisions for cybercrimes against (a) critical infrastructure; and (b) cybercrimes that are committed with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyberterrorism."

58 ITU Telecommunication Development Sector, Understanding Cybercrime: Phenomena, Challenges and Legal Response, September 2012, pp. 34-37.

Several emphasize the particular threat that cyber terrorism holds for critical infrastructures. The magnified asymmetry that terrorists may leverage through cyber attack against financial and banking systems, national media, GPS systems, cellphone networks, electricity grids, water distribution systems is expressed as follows by the CSIS definition of cyber terrorism:

> *…The use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population*[59].

The EU Programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-13 also addresses the aggravated risk to critical infrastructure posed by terrorism, although not cyber terrorism specifically[60].

A comparison of selected definitions of cyber terrorism adopted by these bodies appears in Annex A below.

THE SPECTRUM OF CYBER TERRORISM ACTIVITIES

Under all of these definitions, terrorist use of the internet might leverage the ubiquity and anonymity of cyber space for a range of prohibited activities. This spectrum is well-known from various analyses of terrorist activity in general[61], and includes:

- Cyber attack constituting terrorism;
- Dissemination of unlawful content;
- Fundraising and funding of operations;
- Research of the target's vulnerabilities;
- Recruiting;

---

[59] *Supra* note 33.

[60] See Council Decision 2007/124/EC of 12 February 2007 and, more generally, the summary of European critical infrastructure protection initiatives at europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.

[61] See for instance Y. Schweitzer, G. Siboni and E. Yogev, "Cyberspace and Terrorist Organizations", Military and Strategic Affairs, December 2011, p.4; N. Veerasamy, "A Conceptual High-Level Framework of Cyberterrorism", International Journal of Information Warfare, Vol. 8(1). pp 1-14; and R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework", International Journal of Computer Science and Information Security, Vol. 10, No. 2, 2012.

- Planning;
- Real-time operational support;
- Post-facto notification and attribution of attacks, and
- Propaganda.

It is crucial to note that only the first category addresses the actual terror attack or the threat thereof. As noted above, the others may be considered ancillary or secondary types of terrorist activity. Relevant international treaties and domestic criminal law make this distinction regarding non-cyber terrorist activity to different degrees; a distinction which is likely to be reflected in developments related to the legal norms applicable to cyber terrorism.

Discussions of the specific tactical and strategic advantages that terrorists might glean from cyber attacks, or from combining real-world terrorist attacks with cyber capabilities, abound in both the popular and professional literature, and will not be reviewed here[62]. It is nevertheless worth noting the emphasis in the literature on the terrorist threat to computerized critical infrastructures, where terrorists' ability to leverage cyber attacks to cause massive damage is magnified. For example, the ITU's 2012 *Understanding Cybercrime* summarizes as follows:

> *This shift in the focus of the discussion had a positive effect on research related to cyberterrorism as it highlighted areas of terrorist activities that were rather unknown before. But despite the importance of a comprehensive approach, the threat of Internet-related attacks against critical infrastructure should not be removed from the central focus of the discussion. The vulnerability of and the growing reliance on information technology makes it necessary to include Internet-related attacks against critical infrastructure in strategies to prevent and fight cyberterrorism[63].*

This author advocates the development of legal norms through treaties and domestic legislation to prohibit cyber terrorism in line with the spectrum of

---

[62] See M. David and K. Sakurai, "Combating cyber terrorism: countering cyber terrorist advantages of surprise and anonymity", Advanced Information Networking and Applications, 2003. AINA 2003, pp. 716-721; Use of Internet for Terrorist Purposes, *supra* note 12; and Weimann, *supra* note 18.

[63] Supra note 54 at p. 36.

terrorist activities described above. In this view, cyber terrorism may eventually be defined to encompass any of the above activities, as well as those which will surely develop in the future. A cyber terrorism event may stand on its own as a discrete virtual occurrence; and it may also serve as a force multiplier for more "traditional" forms of terrorism in the physical world[64]. Differences lie in the tools and the targets but, in line with Rule 11 of the Tallinn Manual, not in the "scope and effects" of the terrorist act. Legal norms, as they evolve, should reflect these nuances and treat cyber terrorism activity as a comprehensive whole.

THE ISRAELI CASE: THE DEFINITIONS OF "AN ACT OF TERRORISM" UNDER ISRAEL'S PROHIBITION ON TERRORIST FINANCING LAW AND DRAFT FIGHTING TERRORISM LAW

Individual countries have, naturally enough, not waited for the international legal community to develop binding global norms for the prohibition and prosecution of cyber terrorism. Like several other countries, the United Kingdom has initiated measures to train special police units to confront cyber terrorism threats, to intervene in websites of radical groups, to authorize telephone wiretaps and to survey email traffic and content in police investigations connected to crimes of terrorism[65]. A recent legislative development in the U.S. authorizes the National Counterterrorism Center of the US Homeland Security to access almost any database the government collects that it says is "reasonably believed" to contain "terrorism information."[66] Other countries, including the UAE, Saudi Arabia, China and India have adopted different approaches to criminalizing aspects of terrorists' activities in cyber space, including prohibiting online incitement to terrorist acts[67]. Finally The Council of Europe's CODEXTER project has recently

---

[64] "Thus, while most conventional terrorist attacks are limited in time and space, a cyber attack magnifies terrorism's psychological impact through fear and intimidation", Schweitzer et al *supra* note 60 at p.3.

[65] *Ibid*, p. 7.

[66] "US Terrorism Agency to Tap a Vast Database of Citizens", Wall Street Journal, December 13, 2012. See also Homeland Security Act of 2002, Section 2, (http://www.whitehouse.gov/deptofhomeland/analysis/); Uniting and Strengthening America
by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act of 2001), Pub. Law 107-56, Section 1016(e), 42 U.S.C. Section 5195c(e) (http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm).

[67] Council of Europe, "Cyberterrorism – the use of the internet for terrorist purposes", *supra* note 40 at 28-36 and 134-5.

established a database to track 31 countries' legislative readiness to prosecute terrorist use of the internet[68].

Israel's law on prohibiting terrorism is currently set to undergo a transformation, with the proposed bill for the Fighting Terrorism Law, 5721-2011 having passed a first reading in the Knesset in the summer of 2011 and expected to be re-tabled in the wake of the January 2013 national elections[69]. Leaving aside the broader issues raised by the bill in the context of civil liberties[70], the key issue in the new bill relevant to the present analysis is that neither it nor the existing Prohibition on Terrorist Financing Law, 5765-2004[71] (herein- Terrorist Financing Law) address the issue of cyber terrorism directly.

We begin the analysis with the relevant section of the Terrorist Financing Law. Article 1 defines "an act of terrorism"[72], and represents Israeli legislation's most cogent definition thereof. The full definition follows, and the salient points are summarized below:

"An act of terrorism" –

(a) an act that constitutes an offence or a threat to commit an act that constitutes an offence that was committed or was planned to be committed in order to influence a matter of policy, ideology or religion if all of the following conditions are fulfilled:

(1) it was committed or was planned to be committed with the goal of causing fear or panic among the public or with the goal of coercing a government or another governing authority, including the government or governing authority of a foreign country to take action

---

68 Database on Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe (http://www.coe.int/t/dlapil/codexter/cyberterrorism_db.asp).

69 The bill passed its first reading on August 3, 2011, Proposed Laws (Government). 611, p. 1408, 27 July 2011. Text available from Ministry of Justice website: http://www.justice.gov.il/NR/rdonlyres/77CD3245-3A1D-4F8E-AA54-5D8C25344888/29272/611.pdf

70 The bill has been criticized for its infringement of civil liberties. See, for instance, the critique of Israel's Association for Civil Rights in Israel (http://www.acri.org.il/en/knesset/fighting-terrorism-bill)

71 Prohibition on Terrorist Financing Law, 5765-2004, unofficial translation to English from website of the Israel Money Laundering and Terror Financing Prohibition Authority.

72 Additional Israeli laws that are less relevant to the present analysis include the Mandatory 1945 Defense (Emergency) Regulations and the 1948 Prevention of Terror Ordinance, respectively.

or to refrain from taking action; for the purposes of this paragraph – foreseeing, as a nearly certain possibility, that the act or the threat will cause fear or panic among the public is equivalent to having a goal to cause fear or panic among the public;

(2) the act that was committed or that was planned or the threat included:

(a) actual injury to a person's body or his freedom , or placing a person in danger of death or danger of grievous bodily injury;
(b) the creation of actual danger to the health or security of the public;
(c) serious damage to property;
(d) serious disruption of vital infrastructures, systems or services;

(b) if the aforementioned act or threat was committed or was planned to be committed using weapons as defined in Section 144(c)(1) and (3) of the Penal Law, excluding a weapon part or accessory, it will be considered an act of terrorism even if the conditions of paragraph (1) of subsection (a) are not met, and if it was committed or planned to be committed using chemical, biological or radioactive weapons that are liable, due to their nature, to cause actual mass harm – even if the conditions set forth in paragraphs (1) and (2) of subsection (a) are not met;

The definition of "act of terrorism" in the draft bill for the Fighting Terrorism Law, 5721- 2011 (herein – Draft Bill) is similar to this one, with three specific differences noted in the bill's Explanatory Notes which will be discussed below.[73] According to the Notes, both definitions are based on the UN General Assembly's Resolution of 1995, "Measures to Eliminate International Terrorism"[74] and resemble the laws of other democracies such as Canada, the UK and Australia.

The four differences in parts (a) (1) and (2) of the definition between "act of terrorism" under the Draft Bill and the current Terrorist Financing Law are not

---

[73] Explanatory Notes (*Divrei Hesber)* for Fighting Terrorism Law, 5721- 2011, *supra* note 70, at pp. 1413-1416.

[74] UN Doc. A/RES/50/53, 11 December 1995. In a subsequent, related Resolution the General Assembly made explicit reference to terrorism via electronic means. See note77 below.

major, yet they serve to sharpen the language and focus the intent of this important concept. In brief, they are as follows[75]:

- The phrasing in (a) "...or was planned to be committed..." is eliminated in the proposed law, as the intent to commit the act is covered either in its commission or in the threat of its commission;

- Also in (a), an act of terrorism committed "...in order to influence a matter of policy, ideology or religion..." is proposed to be altered to reflect the motivations of the perpetrator, as opposed to his or her goal in committing the prohibited act. It is also proposed to add racism to the three existing motivating factors.

- In (a) (1) it is proposed to replace the word "coercing" in the phrase "...with the goal of coercing a government or another governing authority..." with the word, "influencing", as a more accurate description of the goal of the terrorist act[76].

- The language of (a) (2) is proposed to be altered in order to clarify that the legislative prohibition of the 4 proscribed acts regards the act that was threatened and not the threat itself. Also, the bill adds an additional prohibitions to (a) (2) (b) regarding an act that causes severe damage to national security; to (a) (2) (c) regarding damage to property that is not severe in and of itself, but may have severe ramifications, such as damage to a holy place.

Finally, in (a) (2) (d), the bill expands the prohibition from

> *"... serious disruption of vital infrastructures, systems or services." to "... serious harm to vital infrastructures, systems or services; or serious disruption of them; serious damage to the country's economy or environment, or damage to the environment that has caused or is liable to cause serious economic harm."*

Despite the latter expansion of the prohibition coming close to an acknowledgement of the serious damage that may be caused by cyber

---

[75] At page 1414 of the Explanatory Notes, *supra* note 70.

[76] The present author cannot agree with the Explanatory Notes on this point. The goal of the terrorist is to coerce, not to influence, as reflected in his or her choice of violent action.

terrorism, neither the legislative text nor the Explanatory Notes of either the law or the bill explicitly takes into account the threats posed by cyber terrorism.[77] This is surprising and unsatisfactory, given the global developments reviewed above. Moreover, the UN General Assembly Resolution following up to that on which both Israeli laws were explicitly based according to their Explanatory Notes and which predates them both, refers specifically to electronically-abetted terrorism in its Article I (c):

> *To note the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and the need to find means, consistent with national law, to prevent such criminality and to promote cooperation where appropriate[78];*

We argue that the Draft Bill needs to be amended in order to incorporate cyber terrorism as a particular type of terrorism, in a manner that takes into account the recent global efforts to characterize its specific characteristics and threats. The Draft Bill, in its current form, has not taken this step.

Nonetheless, at present Israeli legislation does provide a "bridge" for certain cases of cyber terrorism being covered by the expanded article (a) (2) (d) prohibiting "... serious harm to vital infrastructures, systems or services; or serious disruption of them; serious damage to the country's economy or environment, or damage to the environment that has caused or is liable to cause serious economic harm."

The bridge is inherent in the recently declassified Government Decision 84B, Responsibility for the Protection of Computerized Systems in the State of Israel[79]. The decision sets out a mechanism of authorities and responsibilities for the protection of specified, computerized systems that are determined to be vital to Israel's national functioning by a statutory oversight committee and other specialized bodies. The original scope of protected infrastructures in

---

[77] *Supra* notes 68 and 70 and Explanatory Notes for Prohibition on Terrorist Financing Law, 5765-2004, Draft Law (Government) 43, 21 July 2003, p. 552, at 553.

[78] UNGA A/RES/51/210, Measures to eliminate international terrorism, 17 December 1996.

[79] The original Decision of 11 December 2002 remained classified until November 2011, when it was published by the National Security Authority on 13.2.2011and distributed among selected government ministries as an unclassified document (document in author's possession). The relevant authority for determining critical infrastructure that requires protection mechanisms was transferred to the National Cyber Headquarters under Government Decision 3611 of August 7, 2011.

84B, detailed in its Appendix A, was limited to "vital computerized infrastructures" such as the electricity grid, cabled and wired national telephone communications networks, the national water carrier, the stock exchange, El Al and Arkia aviation companies, Zim and pharmaceutical companies[80]. Expansion of the scope to additional infrastructures, such as food distribution networks and traffic grids, is currently under consideration[81].

FOUR OBSERVATIONS

Since Dorothy Denning's well-known observation in May 2000 that "[c]yberterrorism is the convergence of terrorism and cyberspace[82]", progress has been slow in developing legal definitions and global policies that may serve as effective deterrents and enforcers of a broad prohibition on cyber terrorism. In part, this process is anticipatory: there is a dearth of actual cyber terror events. In the words of Brookings' Peter Singer, writing in December 2012, there are over 30,000 articles on cyber terrorism and zero events of cyber terror[83]. Singer is referring to the dearth of cyber terror attacks – or, in any event, those that have been identifiable up until the present time. Nonetheless, legal and policy experts are moving ahead with several initiatives to forge effective definitions of cyber terrorism in the broader context of cyber attacks and the secondary activities that support these attacks. The Tallin Manual and the EU's CleanIT are especially notable.

Four observations regarding the trends and dilemmas of the developing law prohibiting cyber terrorism:

- The definitional challenge is preceding the normative challenge - Since cyber terrorism has not yet been defined with any degree of international

---

[80] See Appendix A of the 2002 Decision for the complete list.

[81] For an overview of cyber threats to critical infrastructure, see G. Siboni, "The Protection of Critical Assets and Infrastructure from Cyber Attack – The Statutory Dimension"(Hebrew), Army and Strategy, April 2011 and L. Tabenkin, "Protection of Critical Infrastructures from Cyber Threat", (Hebrew) Army and Strategy, November 2011 and the sources cited therein.

[82] "Cyberterrorism", Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives by Dorothy E. Denning, Georgetown University, May 23, 2000 (http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html).

[83] "About 31,300. That is roughly the number of magazine and journal articles written so far that discuss the phenomenon of cyber terrorism. Zero. That is the number of people that who been hurt or killed by cyber terrorism at the time this went to press." P. Singer, "The Cyber Terror Bogeyman", November 2012 (http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer).

consensus, it is at present difficult to discern how it differs from other cyber security issues, on the one hand; and with "ordinary terrorism" issues, on the other. Distinguishing cyber terrorism from better-defined cyber crime is an additional challenge. It may prove preferable to widen the Budapest Convention and domestic criminal codes to deal also with cyber terrorism, rather than duplicating global and domestic efforts on two separate normative tracks.

- Critical infrastructure is currently perceived as the most vulnerable to cyber terrorism, due to its dependence on electronic networks. Much definitional and normative work has been successfully undertaken over the past two decades on protecting critical infrastructure from at several jurisdictional levels, such as the 2006 Communication from the EC on a European Programme for Critical Infrastructure Protection[84] and Israel's Government Decision 84B as incorporated into Government Decision 3611. This work should be leveraged to encompass the protection of infrastructures from cyber terrorism.

- Cyber forensics brings important advantages to the identification, prosecution and prevention of terrorism, including cyber terrorism. Clearly, there are strong overarching law and policy concerns regarding the protection of individual privacy and freedom of communication in cyber space. This challenge is an ongoing one, and includes issues such as the admissibility of digital evidence in international tribunals and domestic courts.

- Finally, as with other cyber security issues, effective international cooperation to enforce the eventual definitions and norms prohibiting cyber terrorism will be crucial to the success of any future legal and policy regimes. The Tallinn Manual, which embodies a serious international effort to define cyber terrorism as well as other cybersecurity terms; and provides the legal analysis relevant to eventual codification of international norms, is an example of the necessary joint efforts required.

---

[84] Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final, Official Journal C 126 of 7.6.2007.

CONCLUSION

Important inroads to address the new threats posed by cyber attacks in general and cyber terrorism in particular, are currently being made by key international organizations and states that are leaders in cyber security. These efforts to cope with new global dynamics of deterrence, prevention and enforcement in cyber space are characterized, at the present stage, by the challenge of defining these new threats at the legal and policy levels. Some actors, such as NATO and the European Community, have moved beyond the definitional challenge and have begun to address the normative challenges.

Although we agree with Singer's evaluation that actual acts of cyber terrorism in the narrow sense of the Tallinn Manual's cyber terrorism attacks have not yet occurred as of this writing, threat assessment around the probability of cyber terrorism events in the future should continue to focus on the vulnerabilities of critical infrastructures. There the ability of terrorists to leverage potentially devastating cyber attacks at relatively low cost to themselves should become prioritized as new arena for counter-terrorism law and policy. This asymmetry is more pronounced in cyber space than in the strictly physical world due to the dependence of critical systems on computer networks. Thus, compared to other global efforts to define cyber threats and develop normative frameworks for addressing them, cyber terrorism seems to be garnering "fast track" treatment from some global decision makers due to the particular threats it poses to critical infrastructures and networks.

In Israel, the expanded and refined definition of "act of terrorism" in the Draft Bill is a welcome improvement over the present definition in the Terrorist Financing Law, especially because of the better understanding of critical infrastructure vulnerability in the draft law. Nonetheless, the draft law does not specifically address cyber terrorism, a glaring shortfall in light of current international developments and the growing understanding within Israel of the need to prohibit cyber terrorism as part of a broad national policy for cybersecurity. This shortfall should be remedied before the Draft Bill is next tabled.

Finally, we conclude with the observation that forging the legal and policy tools to address the threat of cyber terrorism is an increasingly important challenge both globally and domestically within Israel. As the world becomes more and more electronically interconnected by "the internet of things", "the

matternet", satellite and GPS networks, lawmakers need to provide better protection for these new vulnerabilities.

ANNEX 1:

A COMPARISON OF SELECTED DEFINITIONS OF CYBER TERRORISM

Tallinn Manual, 2012	…. Cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population…."[where a "cyber attack" is defined 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.
US Department of Defense, 2005	Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves.
Center for Strategic and International Studies, 2002	The use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population.
FBI, no date	The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
FEMA	Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.
OSCE	[T]he threat posed by the use of the Internet for terrorist purposes, including incitement, recruitment, fund raising, training, targeting and planning terrorist acts….

UN's Working Group on Countering the Use of the Internet for Terrorist Purposes, 2012	A functional approach has been adopted regarding the classification of the means by which the Internet is often utilized to promote and support acts of terrorism. This approach has resulted in the identification of six sometimes overlapping categories: propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyberattacks.
ITU Toolkit, 2010	Whoever commits an offense under [article] with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to cyberterrorism, shall be punished by a fine of [amount]and imprisonment for a period of [_].
EC CleanIT , 2012	Terrorists use the Internet on a daily basis. From a technical perspective, terrorist use of the Internet is not substantially different from regular, legal use of the Internet. Terrorists use the same popular, easy to use or more advanced Internet services as other users do, and they also use tools to conceal their identity and activities. Terrorists do not primarily use the Internet as a weapon to attack other targets, but mainly as a resource. Terrorist activities on the Internet can be found in the easy to access part of Internet where social media are used, and many forms of user-generated content are exchanged. This is also the place where violent propaganda material is spread, and the process of finding new recruits for terrorist acts and radicalization begins. Those who are interested are attracted to more ideological websites and social media that often contain illegal material. The illegality of content may depend, however, on the context in which the material is presented. These ideological websites often glorify and encourage violence, and are used to distribute training manuals and other information on how to commit terrorist acts. The Internet is also used to plan and organize deadly attacks. This takes place in hidden parts of the Internet, the hard-to-access terrorist forums.

Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (Stanford Draft), 2001	Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission or consent: [….] Uses a cyber system as a material factor in committing an act made unlawful or prohibited by any of the following [counter-terrorism] treaties:[…]
Desouza and Hensgen, 2003, Semiotic Emergent Framework to Address the Reality of Cyberterrorism, 2003,cited in N. Veerasamy.	A purposeful act, personally or politically motivated, that is intended to disrupt or destroy the stability of organizational or national interests, through the use of electronic devices which are directed at information systems, computer programs, or other electronic means of communications, transfer, and storage.

THE AUTHOR

Adv. Deborah Housen-Couriel is a Research Associate at the International Institute for Counter-Terrorism (ICT) and Adjunct Professor at the Interdisciplinary Center (IDC) Herzliya, Israel. She is the Chief Legal Officer and VP Regulation at Konfidas Ltd. and serves as a member of the Advisory Board of the Federmann Cyber Security Center at the Hebrew University of Jerusalem in Israel. Deborah's expertise focuses on global and Israeli cybersecurity law and regulation. Her law practice advises clients on high-level strategies for legal planning and regulatory compliance in the areas of corporate governance, preparedness, data protection and retention, internet fraud and cybercrime. Her practice at Konfidas Ltd. is supported by ongoing research on critical cybersecurity issues. She is a research fellow at IDC Herzliya's Institute for Counter-Terrorism (ICT), the Interdisciplinary Cyber Research Center at Tel Aviv University, and the Minerva Center at Haifa University's Law Faculty. Deborah teaches several university courses on cybersecurity law and regulation, with a focus on the interaction among public international law, domestic legal systems and contemporary technological developments in cyberspace.

IDC HERZLIYA

ICT International Institute for Counter-Terrorism

With the Support of Keren Daniel

NEXTGEN 5.0

ABOUT US

ICTR serves as a platform for exchanging research and policy recommendations addressing theoretical, empirical and policy dimensions of international terrorism and other security issues.

FOLLOW US

Facebook: **@ICTRJournal**
Twitter: **@ICTR_journal**
Linkedin: **@ictr-journal**