The Criminalization of Online Terrorism Preparatory Acts under International Law

Irene Couzigou

Senior Lecturer at Aberdeen University Law School (UK)

Law School

University of Aberdeen

High Street

AB243UB Aberdeen

United Kingdom

Email: irene.couzigou@abdn.ac.uk

Abstract

Terrorist organizations increasingly resort to the Internet to promote terrorism, recruit new terrorists, plan and finance their operations. The paper first proposes a definition of terrorism, cyberterrorism, and online terrorism preparatory acts. It then analyses whether current binding international instruments on terrorism, organized crime or cybercrime could prohibit cyber activities precursor of terrorism. The paper concludes that there is no gap in international law that leaves online terrorism related acts completely unregulated. It

nevertheless recommends the drafting of an international treaty that would respond more comprehensively, precisely and thus efficiently to the use of the Internet for terrorist purposes.

Keywords:

Terrorism, organized crime, cybercrime, terrorism preparatory acts

Introduction

Access to the Internet is now widespread and relatively easy. The Internet connects countries regardless of their physical borders or diplomatic or political relations. Content on the Internet is accessible from all over the world. Furthermore, users of the Internet can hide their identity. All this explains why the Internet has become a strategic device for terrorists in the preparation of their attacks.[1] It is even more the case that increasing tighter physical security measures encourage terrorist groups to explore the Internet as a way to lower the risk of detection for their operations. The Islamic State (IS) in particular has recently revolutionised terrorism with its resort to online social media, on a much larger scale and intensity than previous terrorist groups.[2] Thus, its online propaganda contributed to the radicalization of individuals who travelled to fight along the IS in Syria and Iraq or who perpetrated terrorist attacks on the name of the IS.

The Internet offers an ideal plate-form for propaganda and radicalisation through the posting of messages, videos, songs and photos. Terrorist groups resort to several types of

formats: sharing websites such as YouTube; online social network services such as Facebook, Instagram or Twitter; online forums or blogs; or more traditional means, including mass e-mailings. After Facebook and Twitter began suspending accounts that disseminated terrorist propaganda, from 2015, the IS increased their use of encrypted messaging applications such as Telegram and WhatsApp.[3] Terrorist organizations can also create their own website which serves as platform whereby they present themselves to the world. Furthermore, the Internet provides terrorist organizations with a means for recruitment. For instance, terrorist organizations capture information about users who browse their websites, identify those who seem suited to carrying out their work, and contact them directly. Terrorist groups may also use electronic bulletin boards and roam chat rooms looking for potential terrorists. In addition, the Internet can operate as a virtual training camp. Terrorists can educate themselves without the need to visit a library, enrol in a university, or travel to a terrorist training camp. Extremist websites contain resources including instructions on how to build and use weapons, coordinate a suicide bomb attack, conduct counter-intelligence and hacking activities, and improve the security of online operations through encryption tools and other anonymising techniques. Furthermore, terrorists are very likely to use the Internet when preparing an attack. Much of the information needed for a physical attack is publicly available online, including information on transport, satellite maps, critical infrastructure, and building blueprints. Online searching tools allow terrorists to access to information anonymously, with little effort or expense. The Internet has also of course benefits as mode of communication. E-mails allow for asynchronous communication on Internet Relay Chat, such as Skype or WhatsApp. Anonymising software is available to mask the IP address, reroute Internet communications to other jurisdictions or encrypt traffic data on websites. Finally, some terrorist organizations have extensively resorted to the Internet to generate and transfer funds to support their activities. Various means have been employed, including:

donations – terrorist organizations have added links to their sites which advise visitors how to donate funds electronically –; selling CDs, DVDs, books, badges, and flags online; diverting online funds intended for seemingly legitimate organizations like charities; theft and abuse of credit card or bank account information, and money laundering through Internet banking.[4]

In the early to mid-1990s, cyberspace was regarded as an a-territorial and borderless environment different from the physical and bonded spaces that are subject to sovereign claims. Cyberspace was considered by some as having its own legal system based on self-regulation.[5] Cyberspace can be defined as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies".[6] In practice, electronic information relies on physical elements such as computers, routers, servers and cables that are territorially based. Thus, in reality, States do exercise their jurisdiction over those aspects of cyberspace which are supported by physical infrastructure located in their territory – that includes the State's land area, its internal waters, its national airspace, when applicable its territorial sea and its archipelagic waters – or an area under their exclusive control – for instance, an area occupied by the State.[7] The digital world does not constitute a *sui generis* space where no State exercises its jurisdiction but is subject to the national law of the competent State.[8] In consequence, States can prohibit and criminalize malicious online conduct, in particular online preparatory activities of terrorism, perpetrated from a computer located on their territory. Beside their territoriality-based jurisdiction, the most other common link that could be used by States to exercise their criminal jurisdiction over those activities is the nationality-based link.[9]

Given the international character of the resort to the Internet for terrorist purposes, it is necessary to establish common standards in its criminalization across multiple State

jurisdictions, as well as cooperation between States for its investigation and prosecution. However, despite increasing international recognition of the threat posed by terrorist use of the Internet, it is no dealt with by any binding international instrument. The criminalization of online terrorism-related activities may be organized, at least partly, by international instruments on counter-terrorism. Many legal frameworks addressing terrorism were developed during a time when the threat relating to terrorist use of the Internet was not immediately apparent. While the provisions of counter-terrorism instruments are often not Internet-related, they can nevertheless cover terrorist activities conducted by electronic means. Furthermore, the criminalization of the terrorist resort to the Internet may also be partly covered by international instruments on organized crime, and by instruments on cybercrime. In accordance with the United Nations Convention against Transnational Organized Crime, the main international instrument in the fight against transnational organized crime, an organized crime is a serious crime committed by an organized criminal group – a structure group of three or more people – in order to gain a financial or other material profit.[10] Cybercrime can be defined as criminal activity in which information and communication technology is used as a tool to commit a crime and/or in which this technology is a target of a crime. Such a broad definition is in line with international instruments in this area, and particularly with the landmark Convention on Cybercrime of the Council of Europe. This Convention does not define the concept of "cybercrime" but criminalises specific types of behaviour relating to computer systems and computer data.[11] Resort to the Internet in relation to a terrorist attack can correspond to a cybercrime. For instance, terrorist organizations increasingly fund their activities by engaging in traditional forms of cybercriminality, such as online credit card fraud or identity theft.[12] Furthermore, activities on the Internet may be easier to prosecute as cybercrimes rather than as terrorism related acts because the terrorist intention behind those acts is often hard to detect.[13]

Cybercrimes and more generally any other detrimental cyber operations remain however difficult to detect. Indeed, not only must the cyber operation be traced back to its source, that is, to a computer, but the person who used the computer must also be identified. Devices connected to the Internet are assigned Internet protocol addresses that reveal only the geographic location. Furthermore, perpetrators can mask their IP address by using cost-free anonymization services such as the I2P Network and the Tor Project. They can also reroute their cyber conduct over hacked computers of innocent users which assigns it a different IP address and shows that the operation was perpetrated from a computer in a geographical location different from its original source. In addition, mobile phones are increasingly providing access to the Internet and the wide availability of non-registered SIM cards allow users to surf the Internet without any form of identification required.[14]

This paper will first address definitional issues and proposes definitions of conventional terrorism, cyberterrorism as well as acts precursor of terrorism (cyber or not) perpetrated online. Departing from the proposed understanding of online terrorism preparatory acts, the paper will then analyse which current international binding instruments addressing terrorism, organized crime, and cybercrime provide coverage of preparatory acts of terrorism committed online. A distinction will be made between UN instruments and other international instruments. The last chapter of this article will conclude that, ideally, a comprehensive international treaty should address the criminalization, investigation and prosecution of activities performed on the Internet in relation to the preparation of terrorist operations.

Definitional Issues

Definition of Terrorism

Despite decades of effort, attempts to develop an international accepted legal definition of terrorism failed. The first attempt – in recent times – at drafting a general definition of terrorism was in 1999, in the International Convention for the Suppression of the Financing of Terrorism. Article 2 gives the following definition of terrorism: "[a]ny other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."[15] This definition is only for the purposes of the Convention. However, since the Convention is in force and universal – it entered in force in 2002 and has 188 States Parties[16] – it constitutes the nearest approach today of a comprehensive definition of terrorism agreed on by the international community of States.

Furthermore, in accordance with Article 2 Paragraph 1 of the Draft Comprehensive Convention on International Terrorism, "[a]ny person commits an offence within the meaning of the present Convention if that person … causes: (a) Death or serious bodily injury to any person; or (b) Serious damage to public or private property … or (c) Damage to property, places, facilities, or systems referred to in paragraph 1(b) of the present article, resulting or likely to result in major economic loss; when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act".[17] This Draft Convention aims to consolidate all the previous sectoral conventions on terrorism, dealing with certain acts of terrorism, and covers most instances of terrorism.[18] It provides a definition that is not in itself controversial. The deadlock in its negotiation arises instead from the contrary views on

whether such a definition should be applicable to State terror and national separatist movements.[19]

Reference can also be made to the definition of acts of terrorism given by the UN Security Council Resolution 1566 (2004): "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act".[20] Unlike the Draft Convention, the Council's non-binding conception of terrorism is limited to acts which are already offences under the sectoral treaties on terrorism.

The core of all the differing views about terrorism agree that terrorism refers to acts causing death, injury, serious property damage or major economic loss, in order to instigate fear or serious destabilisation in a society or a group of persons so as to coerce a government or international organization to meet certain requests of the perpetrators. The demands differ and are often political or, more broadly, ideology based. Furthermore, the demands are more and more complemented by a vengeance-factor. Indeed, terrorism seems to deliver justice for suffered wrong, resembling a fight between religions and ways of life in general.[21] A specific motive (political, religious, ethnic, etc.) does not constitute a definitional part of terrorism. The reason for the rejection of such a component by international anti-terrorism instruments is that an assessment of the perpetrator's motivation would raise issues for law enforcement authorities.[22] With the development of the Internet, terrorism could occur through cyber means. The question is then raised as to whether cyberterrorism should be defined differently from terrorism.

Definition of Cyberterrorism

As the reliance on digital technology increases, the damaging consequences of failure in networks and information systems grow as well as the opportunities for those who seek to compromise them. In today's cyberworld, numerous national critical infrastructures from water distribution to transportation, from energy to health services relied on computer networks and are thus vulnerable to cyberattacks. Cyber technology is likely to become an international offensive tool, in particular for non-State actors such as terrorists. Indeed, cyberattacks have the potential to affect a large number of people – such as a cyberattack on an air traffic control system which causes airplanes to crash – and can be carried out with a lower risk of detection than traditional attacks.[23] Thus, NATO's Strategic Concept identified cyberattacks as a security threat.[24]

A cyberattack can be defined as a deliberate action through the use of computer networks to disrupt, manipulate or destroy information that resides in the target information system.[25] Perpetrating a cyberattack could be done for instance in infecting computers and networks with viruses and worms that control, slow down or damage computers. A cyberattack could also take the form of a denial of service attack, with or without the assistance of botnets, to overwhelm websites and networks by flooding them with junk communications.[26] Cyberattacks may produce consequences that are only internal to a computer network, such as limiting electronic communications. It may also produce effects that are external, by causing harm to the connected control system of infrastructures, for example crashing planes, derailing trains, disrupting a power plant or opening the floodgate of a hydroelectric dam. The computer network is then the conduit for an attack on a physical target.[27]

How can a cyberterrorist attack be defined? The adjective "cyber" should not be taken to dilute the requirement that a cyberterrorist act also falls within the legal definition of terrorism itself. Cyberterrorism is not a new form of terrorism, but a new terrorist method. Thus, cyberterrorism is the "convergence of terrorism and cyberspace".[28] Hence, cyberterrorism is here defined as an attack conducted through the use of computer networks that intrude, disrupt, manipulate or destroy information in the target computer information system, that results in death, injury, serious property damage or major economic loss, in order to distil fear into a society or people or to seriously destabilise the organization of this society or people, so as to compel a government or international organization in furtherance of certain objectives.[29] Cyberterrorism, unlike traditional forms of terrorism, does not necessarily require some form of physical violence.[30] Indeed, if a terrorist organization targets the computer system of a State's stock exchange and causes important economic loss, so as to compel a State to meet its requests (whether political, religious or other), the attack is likely to be considered as a terrorist attack by the State. What counts are the harmful consequences of a cyber terrorist attack, provoking terror in a wider audience extending beyond the immediate victims of the attack, in pursuit of a political, religious, social or other goal.[31] Based on the definition given above, no act of cyberterrorism has occurred yet.[32] For the moment, terrorist organizations that are not sponsored by a State lack the IT knowledge as well as the scientific and technological infrastructure necessary to perform important damage through the use of the Internet.[33] Terrorists see cyberspace rather as a facilitating tool for the perpetration of non-cyber terrorist attacks than an offensive weapon. The use of cyberspace in preparation of physical terrorist attacks has a much higher practical importance at present than the use of cyberspace as a conduit for cyber terrorist attacks.

Some have another, broader, definition of cyberterrorism which does not only include terrorist attacks conducted via computer networks, but also online activities precursor of

terrorist attacks such as propaganda, recruitment, training, planning, communication and fundraising. For instance, Gordon and Ford argue that a broad conception of cyberterrorism is needed in order to understand the real impact of cyber infrastructure on terrorism. For them, a narrower understanding of cyberterrorism may obscure the role of the Internet in all aspects of terrorist activities and is contra productive. "By limiting our understanding of cyberterrorism to the traditional 'computer as target' viewpoint, we leave our nation open to attacks that rely on the computer for other aspects of the operation."[34] They suggest that cyberterrorism targeting computers is "pure" cyberterrorism while regular cyberterrorism occurs whenever a terrorist leverages "the other factors and abilities of the virtual world ... to complete his mission", including using the Internet to raise funds and research targets.[35] Following this position, the September 11 attacks qualify as cyberterrorism because the Internet was used to plan the attacks and buy airline tickets.[36]

The scope of the definition of cyberterrorism has several important implications. Indeed, terrorist activities, including those perpetrated online, often allow the triggering of investigative, sentencing and other specific terrorism-related powers and procedures. Many States have adopted derogatory powers and procedures to fight terrorist offences. In the UK, for example, these include specific top and search powers and powers of arrest and an extended period of pre-charge detention.[37] If cyberterrorism were to encompass online preparatory acts of terrorism, terrorism-related legislation would have a much wider scope. It would apply not only to substantive attacks of terrorism conducted via computer networks, but also to online activities precursor of terrorist attacks (cyber or not), such as radicalisation, recruitment, training, planning an attack, and fundraising. The rule of law requires that the derogatory powers of the State are exceptional and strictly delimited.[38] Thus, to implement the specific terrorism-related legislation to acts preparatory of terrorism perpetrated online would show insufficient respect for the rule of law.[39] Furthermore, a narrow conception of

cyberterrorism enables consistency with understandings of non-cyber forms of terrorism. Therefore, this author adopts a narrow conception of cyberterrorism and distinguishes between online terrorism and online terrorism preparatory acts. The paper will now attempt to define those acts.

Definition of Online Terrorism Preparatory Acts

The difficulty in defining preparatory acts of terrorism, cyber or not, is to determine the link that should exist between the preparatory act and the terrorist attack. Actions related to terrorist operations may be remote from the preparation or perpetration of those operations. Furthermore, they may concern actors who did not perpetrate the attacks but had only an associative or facilitating role. This paper favours the criminalization of terrorism preparatory acts. At the same time, however, it argues for a reasonable definition of those acts, based on a concrete relationship between them and a planned or actual terrorist attack. Indeed, overly vague terrorism precursor offences (cyber or not) would be contrary to the principle of legality of criminal law – an essential principle of the rule of law – that requires precision and clarity in the description of offenses.[40] Furthermore, they may be contrary to the right to freedom of expression, as recognized under the constitution of various States and protected by the 1966 International Covenant on Civil and Political Rights to which participation is quasi-universal as well as other international human rights instruments.[41] Restrictions to freedom of expression can be justified in order to guarantee "the protection of national security or of public order", but must then be necessary and proportional to this aim.[42] For instance, the publication of information on weapons could be of interest to terrorist organizations but could also be used in chemistry or physics courses. In our opinion, the

publication of this information should not be criminalized because its link with planned or actual terrorist attacks is too remote. Prohibiting this information would also not be required by the protection of security and would thus be contrary to freedom of expression.

The dangers of expanding by too much the scope of terrorism preparatory offences has been emphasised by the Independent Reviewer of Terrorism Legislation: "[T]he potential for abuse is rarely absent … By seeking to extend the reach of the criminal law to people who are more and more on the margins, and to activities taking place earlier and earlier in the story, their shadow begins to loom over all manner of previously innocent interactions. The effects can, at worst, be horrifying for individuals and demoralising to communities".[43] An example of the issue can be illustrated by section 58 of the UK Terrorism Act 2000. It states that a person commits an offence if, without reasonable excuse, he collects "information of a kind likely to be useful to a person committing or preparing an act of terrorism".[44] This Act was interpreted by the House of Lords in the case *R v G*. While in custody, the defendant in this case collected information on bomb-making and explosives. He also drew a map of a Territorial Army Centre and wrote down plans to attack the Centre. He was then charged with collecting information that may be useful to a terrorist act under section 58 of the Terrorism Act. The House of Lords held that G was guilty of a serious terrorism offence, even though no connection to a terrorist act had been made.[45]

It is here argued that an act should be understood as precursor of a terrorist attack only if it directly relates to a terrorist attack. There should be a connection between the (online) preparatory act and the planned or actual terrorist act so as to justify the qualification of the (online) preparatory act as a terrorism precursor measure.[46] Thus, an online terrorism preparatory act is an activity that encourages, plans or finances a terrorist attack, or trains or recruits perpetrators of a particular terrorist attack. Departing from this proposed definition of online terrorism preparatory activities, this author will now analyse which current

international binding instruments addressing terrorism, organized crime, and cybercrime provide coverage of those activities. UN instruments, likely to have a quasi-universal implementation, will first be studied. The paper will then address other norms, with international or regional scope.

International Instruments Criminalizing Online Terrorism Preparatory Acts

UN Instruments

UN Security Council Resolutions

UN Security Council Resolutions 1373 (2001) and 2178 (2014) could cover certain preparatory acts of terrorism, including those committed through the Internet.[47] Those resolutions were adopted under Chapter VII of the UN Charter and are therefore binding on all UN Member States. They lay down permanent obligations of a general character.

UN Security Council Resolution 1373 (2001) requires from States to criminalize the "provision or collection, by any means … of funds by their nationals or in their territories with the intention that the funds should be used … in order to carry out terrorist acts" (Paragraph 1 (b)). This provision encompasses the financing of terrorism perpetrated on the Internet. States should also suppress the recruitment of members of terrorist groups (Paragraph 2 (a)). Furthermore, States must ensure "[t]hat any person who participates in the

financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice" (Paragraph 2 (e)). The Resolution thus requires from Member States the criminalization of online activities that aim to recruit terrorists or plan terrorist attacks.

Most UN Member States have been willing to criminalize the financing of terrorism. Resolution 1373 (2001), however, has not given any definition of terrorism. The definition enunciated later in Resolution 1566 (2004), not adopted under Chapter VII, is not binding. The consequence is that, what amount to a terrorism financing offence under domestic law varies a great deal from one State to another.[48] The lack of uniform implementation of Resolution 1373 (2001) at the domestic level may prejudice the overall effectiveness of that Resolution.

Resolution 2178 (2014) of the UN Security Council reiterates the obligation set out in Resolution 1373 (2001) on the duty to criminalize the financing of terrorism (Paragraph 6). Furthermore, it obligates all UN Member States to criminalize "the wilful organization, or other facilitation, including acts of recruitment, by their nationals or in their territories, of the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training". This provision covers online propaganda for the recruitment of persons who travel internationally with the aim of committing, preparing, or participating in, terrorist action.

Resolution 2178 (2014) leaves room for some undesirable interpretations. First, it does not, like other Security Council resolutions before it, define terrorism. This omission not only jeopardizes the ability to adopt a uniform implementation of Resolution 2178 (2014), but also provides a tool for oppressive regimes that choose to define terrorism broadly. The Security Council could have limited the scope of the resolution to certain acts of terrorism or, at the very least, relied on the definition of terrorism of Resolution 1566 (2004).[49] Second,

this resolution adopts a broad relationship between the act of recruitment and the terrorist action. For rule of law considerations explained above in this paper, Resolution 2178 (2014) should have linked more closely acts of recruitment States are asked to criminalize to terrorist attacks. Overall, the lack of legal precision in the drafting of Resolution 2178 undermines its capability of effectively countering the phenomenon of foreign terrorist fighters, including their online recruitment. Few States have adopted criminal offences to prosecute the recruitment of foreign terrorist fighters, while many have used existing legislation which may not be sufficient.[50]

UN Treaties

Two treaties dealing with terrorism and organized crime have been concluded under the UN auspices, the International Convention for the Suppression of the Financing of Terrorism and the Convention against Transnational Organized Crime. The first Convention, concluded in 1999, requires from its 188 States Parties the criminalization of the financing of terrorist acts, thus including those perpetrated online.[51] However, the scope of the Convention is less broad than the scope of Security Council Resolution 1373 (2001). Indeed, an offence within the scope of the Convention is the provision of funds with the intention that they are used to carry out an act constituting a terrorist offence of one of the then 11 sectoral treaties in force against terrorism or a terrorist act intended to cause death or serious bodily injury (Article 2 Paragraph 1)). This later definition does not encompass acts that do not lead to death or injury but could nevertheless be perceived as terrorist acts.

The Convention against Transnational Organized Crime of 2000 has been ratified almost universally.[52] It encompasses 190 States.[53] Each State Party to this Convention must

establish as criminal offences the commission of "a serious crime for a purpose relating … to the obtaining of a financial or other material benefit", the "conduct by a person who … takes an active part in [c]riminal activities of the organized criminal group" or "[o]ther activities of the organized criminal group", or "[o]rganizing, directing, aiding, abetting, facilitating or counselling the commission of serious crime involving an organized criminal group" (Article 5). The offence must be transnational. "Serious crime" is equivalent to "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years" (Article 2). "Organized criminal group" is defined as "a structured group of three or more persons … acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain … a financial or other material benefit" (Article 2). Thus, a terrorist organization stealing an important amount of money through a fraudulent resort to the Internet would be an "organized criminal group" and this use of the Internet could be qualified as a "serious crime". The pursuit of some online activities in support of terrorist actions could therefore be classified as crimes under the Convention.

Other legal instruments related to counter-terrorism or cybercrime than the ones prepared under the auspices of the UN may cover online terrorism preparatory conduct, whether at the international or regional level.

Other International Instruments

Other international instruments on terrorism

The Council of Europe's Convention on the Prevention of Terrorism of 2005 is the most important European instrument against the dissemination of terrorist content.[54] Its Articles 5 to 7 require from the 40 States Parties to establish as offences public provocation to commit a "terrorist offence", i.e., the "distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct … causes a danger that one or more such offences may be committed"; recruitment for terrorism; and training for terrorism (Articles 5 to 7).[55] "Terrorist offence" is limited to the offences under the 10 UN sectoral treaties on terrorism then in force, listed in the Convention's appendix. The Convention on the Prevention of Terrorism does not require that the dissemination of the relevant material takes place by means of traditional writings. Therefore, they also apply to the incitement of terrorism, recruitment for terrorism, and terrorist training on the Internet.

Within the European Union, the Directive of the European Parliament and of the Council of 15 March 2017 on combating terrorism urges the currently 28 European Union Member States to criminalize public provocation to commit a terrorist offence, recruitment for terrorism, providing and receiving training for terrorism, travelling or organizing or otherwise facilitating travelling for the purpose of terrorism, and financing of terrorism (Articles 5 to 11).[56] It also asks States to criminalize theft, extortion or forgery with the aim of committing terrorist offences (Article 12). The Directive adopts a broad definition of "terrorist offence" (Article 3). It is a combination of objective elements (murder, bodily injuries, hostage taking, etc.) and subjective elements (acts committed with the objective of seriously intimidating a population, compelling a government or an international organization to perform or abstain from performing actions, destabilising or destroying structures of a country or an international organization).

This Directive is completed by the Framework Decision on combating certain forms and expressions of racism and xenophobia, adopted by the Council of the European Union in 2008.[57] It requires from the European Union States to criminalize public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, colour, descent, religion or belief, or national or ethnic origin. It could cover certain activities perpetrated online to promote terrorist attacks. Although European Union Council Framework Decisions are not meant to have direct effects, the European Court of Justice ruled that "[t]he binding character of framework decisions … places on national authorities, and particularly national courts, an obligation to interpret national law in conformity".[58]

At the African level, under the Organization of African Unity Convention on the Prevention and Combating of Terrorism, adopted as soon as 1999, its 43 States Parties undertake to establish as criminal offences "any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organizing, or procurement of any person", with the intent to commit certain acts of terrorism (Article 2 (a)).[59] Those acts include "any act which is a violation of the criminal laws of a State Party and which may endanger the life of, or cause serious injury to, any person or causes damage to public or private property, natural resources, environmental or cultural heritage" and is intended to "intimidate any government … to do or abstain from doing any act", "disrupt any public service", or "create general insurrection in a State" (Article 1 Paragraph 3 (a)). Thus, this Convention requires from States Parties to penalize the online propaganda, recruitment, training, planning and financing of terrorist action, providing that action is criminalized under the domestic law of the States Parties.

In the American continent, in accordance with the Inter-American Convention against Terrorism of 2002, each of the 24 States Parties should "institute a legal and regulatory

regime to prevent, combat, and eradicate the financing" of terrorist offences (Article 4 Paragraph 1).[60] For the purposes of this Convention, terrorist offences refer to the offences of 10 sectoral treaties against terrorism. Therefore, this Convention requires the criminalization of the online financing of certain terrorist activities.

Finally, in Asia, the Association of Southeast Asian Nations (ASEAN) Convention on Counter-Terrorism, concluded in 2007 and ratified by the 10 ASEAN States, asks States Parties to "[e]nsure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice" (Article VI Paragraph 1 (m)).[61] For the purposes of this Convention, "offence" means any of the offences within the scope of and as defined in 14 treaties on terrorism listed in the Convention. Hence, in accordance with this Convention, States Parties must penalize the online financing and preparation of some terrorist acts.

International instruments on Cybercrime

The most influential instrument against cybercrime is the Council of Europe's Convention on Cybercrime of 2002. It has been ratified or acceded to by most of the Council of Europe Members, as well as a few non-Member States.[62] It is currently the most important multilateral binding instrument addressing criminal activity conducted via the Internet. The Convention on Cybercrime requires its 63 States Parties to criminalize offences against the confidentiality, integrity and availability of computer systems (illegal access, illegal interception, data interference, system interference, misuse of devices), computer-related offences (forgery, fraud), content-related offences on child pornography, and offences related to the infringements of copyrights and related rights.[63] Some online acts preparatory of

terrorism could be prohibited by the Convention as offences against the confidentiality, integrity and availability of computer data as well as computer forgery or fraud.

During the process of drafting of the Convention on Cybercrime, it was difficult to reach an agreement on the criminalization of acts of a racist and xenophobic nature.[64] These acts were addressed in a distinct protocol, namely the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems of 2003. According to the Protocol, each of the 32 States Parties must establish as criminal offences under its domestic law the dissemination of racist and xenophobic material through computer systems, racist and xenophobic material through computer systems as well as racist and xenophobic motivated insult (Articles 3 and 5).[65] These provisions could partly cover the use of the Internet for terrorist purposes.

The EU directive on attacks against information systems of 2013 is based on the European Convention on Cybercrime and, like the Convention, requires from the currently 28 EU Member States to ensure that illegally accessing information systems (Article 3), illegally interfering with systems (Art. 4), and illegally interfering with computer data (Article 5), and illegally intercepting computer data (Article 6) are punishable as criminal offences.[66] As a consequence, it englobes terrorist use of the internet that constitutes illegal access or interference to/with information systems or electronic data.

The Convention on Cybercrime does have similarities with the Agreement on Cooperation Among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information. Concluded in 2001 and currently encompassing 9 States, this Agreement asks its parties to establish as criminal acts "[t]he illegal accessing of computer information protected by the law, where such act results in the destruction, blocking, modification or copying of information or in the disruption of the functioning of the computer, the computer system or related networks" (Article 3).[67] Some

online terrorism related activities may be an offence relating to computer information in the sense of this Agreement. For instance, such would be the case of copying online defence secrets of a State in preparation of a terrorist attack.

At the African level, the Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime of 2011 requires the 15 ECOWAS Members to criminalize fraudulent access to (Article 4) and fraudulent remaining in (Article 5) Information and Communication Technology.[68] Computer-related offences also concern the interference with the operation of a computer system (Article 6), inputting, intercepting, modifying and manipulating computer data (Articles 7 to 9 and Article 12). Further offences include forgery (Article 10) and computer-related fraud (Article 11), but also the mere knowing use of forged data (Article 13). Those acts could be perpetrated when resorting to the Internet in preparation of terrorist activities.

Also in Africa, the Arab Convention on Combating Information Technology Offences, concluded in 2010, is one of the few international instruments that addresses directly acts related to terrorism committed by means of information technology.[69] Article 15 requires from States Parties to criminalize several online terrorism-linked activities: the dissemination and advocacy of the ideas and principles of terrorist groups, the financing and training for terrorist operations, communications between terrorist organizations, the dissemination of methods to make explosives to be used in terrorist operations, and finally the spreading of religious fanaticism and attacking religions and other beliefs. Unfortunately, the Convention omits to define its understanding of terrorism which may lead to abuse. Furthermore, despite having been ratified by 18 States, the Convention has not been formally activated yet. [70]

Conclusion and Recommendations

As showed by this analysis, international terrorism-specific instruments and the Convention against Transnational Organized Crime are applicable in the IT environment; cybercrime-specific instruments are applicable with respect to acts precursor of terrorism. Furthermore, the criminal acts dealt with in these instruments are broadly defined. Thus, international binding instruments addressing terrorism, organized crime or cybercrime cover all online terrorism preparatory acts. This first conclusion must be nuanced by the fact that participation of States to the international instruments addressing terrorism or cybercrime differs greatly and may be restricted. Indeed, some of them have a limited regional scope. For instance, they concern only the 10 ASEAN Members or the 9 States Members the Commonwealth of Independent States.

An issue raised by the multitude of binding international instruments covering online terrorism preparatory acts is the dual or multiple characterisation of the same act in different States, depending on to which instrument(s) the States are bound to. Diverse national legislations about the terrorist use of the Internet work to the advantage of the terrorists who can choose to operate from geographic locations where penalties for online activities precursor of terrorism are less severe or even non-existent. Thus, a legal and primordial reason for concluding a comprehensive international convention on online terrorism preparatory acts is to promote harmonisation and consistency in the criminalization of those acts between domestic legal regimes. Another reason is to restrain national governments when determining the scope of terrorism precursor offenses. Indeed, as demonstrated in this paper, vague and overly broad definitions of terrorism precursor offences would be contrary to the rule of law and human rights, especially to the rights to freedom of expression,

religion, and association. Reaching to a common definition of online terrorism preparatory activities to be criminalized by States should be a starting point.

Establishment of special procedures for the investigation and prosecution of online terrorism preparatory offences is also a good justification for the negotiation of an international treaty on online terrorism preparatory acts. The commission of offences in computer networks poses computer-specific problems with respect to their investigation and prosecution. These problems are due to the invisibility, speed, volatility and transnational character of computer data that make the identification of cyber perpetrators very difficult. The Convention on Cybercrime of the Council of Europe could serve as a model in the negotiation of investigation procedures in a treaty on online preparatory activities of terrorism. It is widely recognised that the investigation methods of the Cybercrime Convention are well-designed.[71] Its Articles 14 to 22 oblige parties to adopt a range of measures necessary to trace back an online conduct. They cover the expedited preservation of stored computer data, production of orders to submit specified computer data, search and seizure of stored computer data, real-time collection of traffic data, interception of content data, as well as jurisdictional rules.

While the use of the Internet enables terrorist groups for international action (using computers in different States), the response of State law agencies is traditionally bound by territoriality or nationality. Given the global character of cyberspace, international cooperation appears essential in investigation and prosecution of online conduct for terrorist purposes. For instance, if a State wants to trace back an international cyber operation whose effects manifested on its territory, it will require assistance from the State in whose territory the operation was launched.[72] A treaty on online terrorism preparatory acts would provide for mutual assistance. It would also establish extradition agreements. Extradition is normally based on the principle of dual criminality and would be made easier once States agree on a

common terrorism precursor offence. Currently, the most highly developed regime of international legal cooperation in cyberspace is found in the Convention on Cybercrime of the Council of Europe.[73] That Convention could inspire the international cooperation set up by a treaty on online terrorism preparatory activities. For instance, its chapter III encompasses computer-specific provisions for mutual assistance in the areas of expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing of stored data, real-time collection of traffic data, and interception of content data. An international framework on online terrorism precursor activities could update and develop the cooperation provisions of the European Convention on Cybercrime. In particular, it could provide for a better cooperation between States and private Internet providers in the monitoring and/or suppression of illegal terrorism-related content online. gStates should regulate the surveillance of the Internet and the removal or disablement of online terrorism content within the limits of human rights, especially the right to freedom of expression and the right to privacy. To summarize, a specific treaty would be necessary to harmonize and enhance the criminalization, investigation and prosecution of online terrorism preparatory acts and to strengthen international cooperation in countering those acts.[74] Such a treaty would constitute a milestone in the fight against the resort to the Internet by terrorists.

If a treaty on online preparatory terrorism acts is to be recommended, its negotiation appears however to be an incommensurable task. Indeed, edification of such a treaty would require a common agreement of what is an online preparatory act of terrorism and would therefore also require an international definition of terrorism. The struggle States have had for more than 20 years to agree on a common understanding of terrorism is well known. Furthermore, even if a treaty on online preparatory terrorism acts is negotiated, it should receive enough ratifications to be efficient. It seems to be a difficult aim to reach given the relatively low number of ratifications of current treaties on terrorism or cybercrime.[75] This is

especially true in the case of the Convention on Cybercrime and the Convention on the Prevention of Terrorism of the Council of Europe, which are the most important international instruments for fighting cybercrime and the dissemination of illegal terrorist content. The Convention on Cybercrime which has 63 States Parties, including the United States, Japan and other 17 States not Members of the Council of Europe, encompass only a bit more than one-third of Internet users in the world. Many States, especially cyber powers like China, Russia, and Israel, have yet to ratify the treaty. The Convention on the Prevention of Terrorism has even less international impact: it encompasses 40 States Parties, all Members of the Council of Europe, although its accession is open to non-Members of the Council.[76]

Even if States agree on the conclusion of a treaty on the criminalization of online terrorism preparatory acts, it is far from certain that that treaty would be properly implemented. Indeed, an international treaty is binding only for those States that accepted to become party to it. Furthermore, under international law, most treaties do not provide for a specific enforcement mechanism.[77] It is unlikely that a treaty on the criminalization of acts precursors of terrorism would organize its own enforcement procedure.[78] In that case, the most effective enforcement means would be at the discretion of the UN Security Council. Indeed, under Chapter VII of the UN Charter, the Security Council could impose sanctions against a State that does respect a treaty on the criminalization of online terrorism preparatory activities to which it is a party. Those sanctions could include the complete or partial interruption of financial or commercial relations. The Security Council would first have to qualify the State's attitude as a threat to the peace, a breach of the peace or an act of aggression.[79] Independently from the Security Council action, States could adopt acts of retorsion or countermeasures against a State that does not implement its treaty obligation to criminalize and prosecute online terrorism preparatory activities. The aim of those acts would be to achieve compliance by the responsible State with its treaty obligation. An act of

retorsion is an unfriendly measure, lawful in itself, adopted by a State in reaction to the unfriendly conduct of another State, whether that conduct is lawful or not. A typical example of an act of retorsion is the disruption of diplomatic relations or the withholding of economic assistance.[80] A countermeasure is a non-forcible measure that would be unlawful if it were not taken by a State in response to an internationally wrongful act by that State. The suspension of a trade agreement or the freezing of the assets of the responsible State are examples of countermeasures.[81]

If a treaty on the criminalization of online terrorism preparatory acts cannot be negotiated or does not receive enough State participation, the UN Security Council could adopt a resolution and ask UN Member States to criminalise the use of the Internet for terrorist purposes. If the resolution is taken within Chapter VII of the UN Charter, it would automatically bind all UN Member States. The Security Council has already resorted to general resolutions, not linked to a particular crisis but to a global phenomenon.[82] In particular, it required from UN Member States to criminalize the financing of terrorism.[83] A Security Council resolution on the criminalization of online terrorism related acts would not however have the same legitimacy than a treaty on the same issue. Indeed, within a traditional reading of Chapter VII of the UN Charter, the role of the Security Council is to act as a policeman of the world.[84] Far-reaching powers were given to the Security Council so that it could efficiently react to a concrete threat to the peace, breach of the peace or act of aggression. The Security Council was meant to confine its powers to short-term measures. Furthermore, composed of only 15 States, the Security Council is not well suited to represent the 193 UN Member States and adopt long-term resolutions or so-called "legislative" resolutions. For these reasons, States criticized the Council's growing "legislative" work.[85] The UN Charter binds its Members if they agree with new interpretations of the Charter made by its organs, including the Security Council. Thus, given the lack of strong and wide consent

of States in favour of a re-interpretation of the Security Council's powers, as provided for by the UN Charter, this author doubts that the Council is allowed to adopt "legislative" resolutions, including a resolution related to the criminalization of online terrorism preparatory acts.

At the end, in face of the current legal and political difficulties of having a binding international instrument addressing online terrorism preparatory acts, adopted by States or, alternatively by the UN Security Council, there is a need to rely on current binding international instruments. A treaty on online activities precursor of terrorism would respond more precisely and thus efficiently to the use of the Internet for terrorist purposes than the existing legal frameworks but the negotiation of that treaty is unlikely to begin soon. A pragmatic approach is necessary. For the moment, States should be encouraged by the UN or the Council of Europe to ratify and apply current instruments against terrorism or cybercrime, whose provisions cover most of the online activities precursor of terrorism.[86] Future efforts should in particular concentrate on achieving a broader ratification and implementation of the Convention on the Prevention of Terrorism and the Convention on Cybercrime, the two main treaties dealing with counter-terrorism and cybercrime and whose accession is open to States not Members of the Council of Europe.[87]

Notes

[1] Phillip W. Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in *A War on Terror?*, ed. Marianne Wade and Almir Maljevic (New York: Springer, 2009), 51, 53-56.

[2] Arthur L. Brocato, "Tackling Terrorists' Use of the Internet: Propaganda Dispersion & the Threat of Radicalization," in *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses,* ed. M.N. Ogun (Amsterdam: IOS Press, 2015), 129, 138-139.

[3] Steve Ragan, "After Paris, ISIS moves propaganda machine to Darknet," CSO (15 November 2015) https://www.csoonline.com/article/3004648/security-awareness/after-paris-isis-moves-propaganda-machine-to-darknet.html (accessed June 14, 2019)

[4] Lord Carlile QC and Stuart Macdonald, "The Criminalisation of Terrorists' Online Preparatory Acts," in *Cyberterrorism, Assessment and Response*, ed. Tom Chen, Lee Jarvis and Stuart Macdonald (New York: Springer, 2014), 155, 159-160. See also UN Office on Drugs and Crime, "The use of the Internet for terrorist purposes," (2012), 3-11, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed June 14, 2019)

[5] David R. Johnson and David G. Post, "Law and Borders - The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1378–1395.

[6] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Lincoln: University of Nebraska Press, 2009), 24, 28.

[7] Irène Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations," *International Review of Law, Computers & Technology* 32, no. 1 (2018): 5.

[8] Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace,* ed. Katharina Ziolkowski (Tallinn: NATO CCD COE Publication, 2013) 189, 193-194.

[9] UN Office on Drugs and Crime, "Comprehensive Study on Cybercrime," (2013), 189, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed June 14, 2019).

[10] Article 2 of the UN Convention against Transnational Organized Crime, *UN Treaty Series*, 2225, 209.

[11] Dominik Brodowski, "Transnational Organised Crime and Cybercrime," in *International Law and Transnational Organised Crime,* ed. Pierre Hauck and Sven Peterke (Oxford: Oxford University Press, 2016), 334, 335.

[12] United Nations Counter-Terrorism Implementation Task Force, "Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects," (2011) 18 and 34, https://www.un.org/counterterrorism/ctitf/en/countering-use-internet-terrorist-purposes-legal-and-technical-aspects-working-group-compendium-2011 (accessed June 14, 2019).

[13] Brunst, "Terrorism and the Internet", 56.

[14] Russell Buchan, "Cyberspace, Non-state Actors and the Obligation to Prevent Transboundary Harm," *Journal of Conflict and Security Law* 21, issue 3 (2016): 430; United Nations Counter-Terrorism Implementation Task Force, "Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects" (2011), 22-23, http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf (accessed June 14, 2019).

[15] *UN Treaty Series*, 2178, 230.

[16] As of June 14, 2019.

[17] UN Doc A/59/894 (2005), annex II, 9.

[18] Convention on Offences and Certain Other Acts committed on Board Aircraft 1963; Convention for the Suppression of Unlawful Seizure of Aircraft 1970; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation 1971; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents 1973; International Convention against the Taking of Hostages 1979; Convention on the Physical Protection of Nuclear Material 1980; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation supplementary to the Montreal Convention 1988; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation 1988; Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf 1988; Convention on the Marking of Plastic Explosives for the Purpose of Detection 1991; International Convention for the Suppression of Terrorist Bombings 1997; International Convention for the Suppression of the Financing of Terrorism 1999; International Convention for the Suppression of Acts of Nuclear Terrorism 2005.

[19] See for instance comments of delegations to the Draft Comprehensive Convention, UN Doc A/C.6/65/L.10 of 3 November 2010, No. 11, 22. Also Bettina Weiβer, "Transnational Organised Crime and Terrorism," in *International Law and Transnational Organised Crime,* ed. Pierre Hauck and Sven Peterke (Oxford: Oxford University Press, 2016), 84, 95-97.

[20] UNSC 1566 (2004) UN Doc SC/1566/2004, Para 3.

[21] Georg Kerschischnig, *Cyberthreats and International Law* (The Hague: Eleven International Publishing, 2012), 222.

[22] Weiβer, "Transnational Organised Crime and Terrorism," 93-92.

[23] Dogrul Murat, Aslan Adil, and Celik Eyyup, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *3rd International Conference on Cyber Conflict*, ed. Christian Czosseck, Enn Tyugu and Thomas Wingfield (Tallinn: CCD COE Publications, 2011), 29, 32-33.

[24] NATO, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Member of the North Atlantic Organization* (Brussels: NATO Public Diplomacy Division, 2010), para. 12.

[25] James E. Cartwright, "Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directorates" (Washington DC: 2013), 3, https://info.publicintelligence.net/DoD-JointCyberTerms.pdf (accessed June 14, 2019).

[26] Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* (2015): 113.

[27] Couzigou, "Securing Cyber Space," 2.

[28] Dorothy E. Denning, "Cyberterrorism," *Global Dialogue,* (2000) 1, http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf (accessed June 14, 2019).

[29] Kerschischnig, *Cyberthreats*, 231.

[30] Süleyman Özeren, "Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task," in *Responses to Cyber Terrorism,* ed. Centre of Excellence Defence Against Terrorism (Ankara: IOS Press, 2008), 70, 72.

[31] Kenney, Cyber-Terrorism, 121.

[32] Kenney, Cyber-Terrorism, 121-125; Eric Luiijf, "Definitions of Cyber Terrorism," in *Cyber Crime and Cyber Terrorism Investigator's Handbook,* ed. Babak Akhgar, Andrew Staniforth and Francesca Bosco (Boston: Syngress, 2014), 11, 16.

[33] Daniel Cohen, "Cyberterrorism: Case Studies," in *Cyber Crime and Cyber Terrorism Investigator's Handbook,* ed. Babak Akhgar, Andrew Staniforth and Francisca Bosco (Boston: Syngress, 2014), 165, 173.

[34] Gordon Sarah and Ford Richard, "Cyberterrorism?," *Computers & Security* 21, issue 7 (2002): 643.

[35] *Ibid,* 637.

[36] *Ibid,* 642.

[37] Carlile QC and Macdonald, "The Criminalisation of Terrorists' Online Preparatory Acts," 156.

[38] Under the rule of law, governmental authorities should in principle be subject to the same law than everyone else, whether natural or legal person. Albert Vein Dicey, *Introduction to the Study of the Law of the Constitution* (London: Macmillan, reprint of the 8th ed. of 1915, 1982), 114.

[39] Carlile QC and Macdonald, "The Criminalisation of Terrorists' Online Preparatory Acts," 156.

[40] Albert Vein Dicey, *Introduction to the Study of the Law of the Constitution*, 110; Lon L. Fuller, *The Morality of Law* (New Haven and London: Yale University Press, revised ed 1964), 46-91.

[41] See Art. 19 of the ICCPR, *UN Treaty Series*, 999, 178. There are 172 States party to the ICCPR as of June 14, 2019.

[42] Art. 19 Para. 3 of the ICCPR, *UN Treaty Series*, 999, 178.

[43] David Anderson, "Shielding the compass: how to fight terrorism without defeating the law," *European Human Rights Law Review* 3 (2013): 240.

[44] https://www.legislation.gov.uk/ukpga/2000/11/section/58 (accessed June 14, 2019).

[45] Jacqueline Hodgson and Victor Tadros, "How to Make a Terrorist out of Nothing," *Modern Law Review* 72, issue 6 (2009): 984 and 987-990.

[46] A.P. Simester and Andreas von Hirsch, *Crimes, Harms, and Wrongs: on the Principles of Criminalisation* (Oxford: Hart Publishing, 2011), 81. See also European Court of Human Rights, Case n° 29590/96, *Yagmurdereli v Turkey*, Judgment of June 4, 2002, Para. 53, expecting evidence of "concrete action" that reveals the *prima facie* intention of the speaker even if the law prohibiting incitement to terrorism does not require a crime to have been committed or attempted.

[47] UNSC 1373 (2001) UN Doc SC/1373/2001 and UNSC 2178 (2014) UN Doc SC/2178/2014.

[48] Andrea Bianchi, "Assessing the Effectiveness of the UN Security Council's Anti-terrorism Measures: The Quest for Legitimacy and Cohesion," *European Journal of International Law* 17, no. 5 (2017): 893.

[49] UNSC 1566 (2004) UN Doc SC/1566/2004, Para 3.

[50] Murmokaité Raimonda (Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism), "Implementation of Security Council Resolution 2178 (2014) by States affected by foreign terrorist fighters: Third Report," UN Doc S/2015/975, Para 2.

[51] *UN Treaty Series*, 2178, 197.

[52] *UN Treaty Series*, 2225, 209.

[53] As of June 14, 2019.

[54] *European Treaty Series* no. 196.

[55] Number of States Parties as of June 14, 2019.

[56] Directive of the European Parliament and of the Council 2017/541 *Official Journal of the European Union* L series 88 of 31.3.2017.

[57] *Official Journal of the European Union* L series 328/55 of 6.12.2008.

[58] European Court of Justice, Case C-105/03, *Pupino*, Judgment of June 16, 2005, Para. 34.

[59] https://au.int/en/treaties/oau-convention-prevention-and-combating-terrorism (accessed June 14, 2019); number of States Parties as of June 14, 2019.

[60] http://www.oas.org/xxxiiga/english/docs_en/docs_items/agres1840_02.htm (accessed June 14, 2019); number of States Parties as of June 14, 2019.

[61] http://asean.org/storage/2012/05/ACCT.pdf (accessed June 14, 2019); number of States Parties as of June 14, 2019.

[62] *European Treaty Series* no. 185.

[63] Number of States Parties as of June 14, 2019.

[64] Marco Gercke, "The Slow Wake of a Global Approach Against Cybercrime," *Computer Law Review International* (2006): 144.

[65] Number of States Parties as of June 14, 2019.

[66] *Official Journal of the European Union* L series 218/8 of 12.8.2013.

[67]

http://itlaw.wikia.com/wiki/Agreement_on_Cooperation_Among_the_States_Members_of_the_Commonwealth_of_Independent_States_in_Combating_Offences_Relating_to_Computer_Information (accessed June 14, 2019); number of States Parties as of June 14, 2019.

[68] Directive C/DIR.1/08/11 on Fighting Cyber Crime within ECOWAS of 19 August 2011. https://issafrica.org/ctafrica/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS.pdf (accessed June 14, 2019).

[69] http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (accessed June 14, 2019).

[70] Joyce Hakmeh, "Cybercrime and the Digital Economy in the GCC Countries," Research Paper, Chatham House, (2017): 12, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf (accessed June 14, 2019).

[71] Ulrich Sieber and Phillip W. Brunst, "Cyberterrorism and other use of the Internet for terrorist purposes," (2008), Expert Report prepared for the Council of Europe: 59.

[72] Susan W. Brenner, "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare," *Journal of Criminal Law and Criminology* 97, issue 2 (2007): 420.

[73] Sieber and Brunst, "Cyberterrorism and other use of the Internet," 61.

[74] UN Office on Drugs and Crime, "The use of the Internet for terrorist purposes," 74 no. 241.

[75] Sieber and Brunst, "Cyberterrorism and other use of the Internet," 66.

[76] Number of States Parties as of June 14, 2019.

[77] On the enforcement of international law in general, see Martin Dixon, International Law (Oxford: Oxford University Press, 7th, 2013) 6-7.

[78] To compare with, the European Convention on Cybercrime requiring States to criminalize some online conduct does not include any enforcement provisions.

[79] See Art. 39 and Art. 41 UN Charter.

[80] Nigel White and Ademola Abass, "Countermeasures and Sanctions," in International Law, ed. Malcolm D. Evans (Oxford: Oxford University Press, 5th, 2018), 521, 527-529.

[81] Art. 49 Draft Articles on Responsibility of States for Internationally Wrongful Acts, 129. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (accessed June 14, 2019). See also Nigel White and Ademola Abass, "Countermeasures and Sanctions," 531, 534-536.

[82] UNSC 1373 (2001) UN Doc SC/1373/2001 ; UNSC 1540 (2004) UN Doc SC/1540/2004 ; UNSC 2178 (2014) UN Doc SC/2178/2014 respectively.

[83] UNSC 1373 (2001) UN Doc SC/1373/2001, Para. 1 (b) and *supra*.

[84] Nico Krisch, "Introduction to Chapter VII: The General Framework," in *The Charter of the United Nations*, ed. Bruno Simma, Daniel-Erasmus Khan, Georg Nolte and Andreas Paulus (Oxford: Oxford University Press, 3rd, 2012), vol. II, 1241, 1246.

[85] Luis Miguel Hinojosa Martinez, ''The Legislative Role of the Security Council in its Fight against Terrorism: Legal, Political and Practical Limits'', *International and Comparative Law Quarterly* 57 (2008): 350-351.

[86] The Council of Europe's Committee of Experts on Terrorism has opined that no "gaps exist" between the Convention on Cybercrime and the Convention on the Prevention of Terrorism, both of the Council of Europe. It thus proposed that the focus should be on the efficient implementation of those conventions, rather than instigating "new negotiations [which] might jeopardize [the existing conventions'] increasing impact on the international fight against cybercrime and terrorism". Committee of Experts on Terrorism (CODEXTER), "Opinion of CODEXTER on cyberterrorism and use of the Internet for terrorist purposes" (2008): 3-4, https://rm.coe.int/information-document-concerning-the-opinion-of-the-committee-of-expert/16802e6ed5 (accessed June 14, 2019).

[87] Accession to both Conventions is possible on the invitation of the Council of Europe. Art. 37 Convention on Cybercrime; Art. 24 Convention on the Prevention of Terrorism.