Università
Ca'Foscari
Venezia

Master's Degree

in Relazioni internazionali comparate –
Comparative International relations

Final Thesis

Cyberterrorism: A study of the issue in the framework of the Council of Europe

Supervisor
Ch. Prof. Sara De Vido

Assistant supervisor
Ch. Prof. Arianna Vettorel

Graduand
Silvia Michielin
857760

Academic Year
2019/2020

Cyberterrorism: A study of the issue in the framework of the Council of Europe

Ai miei nonni. Arnaldo, Flora, Tomaso e Maria.

List of abbreviations

CDCT = Council of Europe Committee on Counter-Terrorism

CDPC = European committee on crime problems

CECPT = Council of Europe Convention on the Prevention of Terrorism

CODEXTER = Council of Europe's Committee of Experts on Terrorism

CoE = Council of Europe

ENISA = European Union Agency for Cybersecurity

GTD = Global Terrorism Database

ICCT = International Centre for Counterterrorism

ICJ = International Court of Justice

ICT = Information and Communication Technology

ILC = International Law Commission

PC-CY = Committee of Experts on Crime in Cyber-space

PCIJ = Permanent Court of International Justice

T-CY = Cybercrime Convention Committee

TRI = Terrorism Research Initiative

UN = United Nations

Abstract

Negli ultimi anni, il campo delle Tecnologie dell'Informazione e della Comunicazione (ICT – Infomation and Communications Technology) è stato scenario di importanti e continui sviluppi, che hanno radicalmente cambiato svariati aspetti della società contemporanea. Basti pensare a come si sia passati in pochi anni, precisamente dal 1969 al 1991, dalla rete di comunicazioni ARPANET (Advanced Research Project Agency) limitata a 4 nodi all'interno del territorio statunitense e con fini prettamente militari; al World Wide Web, composto da nodi disseminati in tutto il mondo e collegati tra loro per i fini più disparati. Col consolidarsi e la diffusione di questo *network of networks*, rete di reti, il concetto di cyberspazio, che fino a qualche anno prima sembra destinato a essere appannaggio esclusivo di racconti fantascientifici, è mutato in qualcosa che viene percepito come parte integrante e fondamentale per la società contemporanea.

Tuttavia, se da un lato il cyberspazio e le opportunità da esso offerte hanno permesso di realizzare importanti sviluppi e miglioramenti negli ambiti più disparati; d'altro canto, queste stesse opportunità hanno finito per attrarre anche utenti del cyberspazio mossi dalle intenzioni meno nobili. Va infatti specificato che le caratteristiche originali del cyberspazio stesso, ne implicano la sua vulnerabilità e, di conseguenza, la possibilità che esso possa essere sfruttato per fini diversi, tra cui fini illeciti, da quelli previsti al momento della sua realizzazione. La vulnerabilità implicita del cyberspazio risiede nel fatto che il protocollo su cui esso è basato, il *TCP/IP protocol*, sia stato realizzato per una rete destinata a essere utilizzata da utenti ritenuti affidabili, quali agenzie governative. Alla luce di ciò, particolari misure di sicurezza non vennero ritenute necessarie.

Lo sfruttamento della vulnerabilità del cyberspazio da parte di utenti mossi da intento criminale ha portato alla nascita di un nuovo concetto, il crimine informatico o *cybercrime*. Il crimine informatico si compone sia di crimini preesistenti commessi con nuovi metodi, che di nuovi crimini nati grazie alle possibilità offerte dal cyberspazio. Nel primo caso, si tratta di crimini già contemplati, la cui perpetrazione non richiede necessariamente lo sfruttamento del mezzo informatico; che tuttavia vengono commessi sfruttando i nuovi mezzi informatici. Questa dinamica si verifica a causa delle caratteristiche peculiari del cyberspazio, che offre agli utenti con le competenze necessarie, la possibilità di commettere attività illecite in anonimato, nascondendo la posizione da cui si opera e in un lasso di tempo incredibilmente breve. Nel secondo

caso, si tratta invece di crimini che senza l'ausilio del mezzo informatico non potrebbero essere commessi.

Con lo sviluppo e il proliferare della criminalità informatica o *cybercrime*, essa è arrivata all'attenzione di esperti e accademici, governi e istituzioni internazionali. Sono in vero emersi numerosi studi volti a dimostrare la necessità di affrontare questa minaccia, tra cui studi di carattere economico in grado di dimostrare l'ingente danno che il crimine informatico comporta per la società.

Sebbene la problematica del crimine informatico non si possa dire del tutto risolta, è stata affrontata da un numero considerevole di Stati a livello nazionale e dalle varie istituzioni internazionali. Da qui l'emergere di nuovi strumenti volti a contrastare e prevenire il crimine informatico; sia di carattere vincolante, quali la Convenzione sulla Criminalità Informatica del Consiglio d'Europa (2001); che di carattere non vincolante, come il Global Programme on Cybercrime dell'ONU.

Tuttavia, non è stato l'ambito del crimine informatico nella sua interezza l'oggetto di questa tesi; ma in vero, uno dei suoi più recenti e controversi sviluppi: il terrorismo informatico o *cyberterrorism*. È stato riscontrato, infatti, che lo sfruttamento delle possibilità offerte dal cyberspazio per fini illeciti è stato preso in considerazione e, in alcuni casi, già messo in atto anche da individui mossi da intenzioni terroristiche. Gli scenari che fanno già parte del *modus operandi* di attori terroristico comprendono le attività che vengono comunemente classificate come attività di supporto all'attacco terroristico in sé. Queste attività illecite che non costituiscono di per sé un attacco terroristico, ma sono necessarie per poter portarlo a termine, includono: la disseminazione degli ideali terroristici, l'attività propagandistica, l'istillazione di un sentimento di paura nella società attraverso minacce, il reclutamento e la formazione di nuovi terroristi, il finanziamento e il riciclaggio di denaro. A queste attività illecite finalizzate a rendere possibile il compimento dell'atto terroristico in sé, si aggiungono delle altre attività svolte nel cyberspazio, che tuttavia non hanno carattere illegale. È il caso della comunicazione interpersonale e della pianificazione. L'utilizzo del cyberspazio per comunicare tra individui, infatti, non rientra tra le attività illecite; così come la consultazione delle mappe satellitari che possono facilmente essere reperite su google non comporta l'effrazione di nessuna legge. Tuttavia, anche queste due attività, inserite nel contesto della nostra analisi hanno una rilevanza particolare. Ciò è dovuto al fatto che, attività apparentemente semplici come la comunicazione tra individui, in

assenza del messo informatico sono in realtà molto più macchinose da svolgere e richiedono sicuramente un dispendio di tempo più elevato. Al contrario, lo sfruttamento del cyberspazio per le attività finalizzate al supporto dell'attività terroristica implica una serie di vantaggi. In primis, la velocità con cui le funzioni possono essere svolte. Attraverso il cyberspazio è possibile svolgere azioni che producono effetti in qualsiasi punto del globo in pochi secondi. A ciò si aggiunge la possibilità di preservare il più totale anonimato, che, in fase di pianificazione di un attacco terroristico risulta essere cruciale. L'identità e la localizzazione dell'individuo che sta effettuando l'azione possono essere infatti facilmente nascosti quando si agisce nel cyberspazio.

A questa categoria di azioni, che utilizzano il cyberspazio come mezzo, si aggiungono quelle in cui il cyberspazio diventa il target dell'attacco in sé. Spesso ci si riferisce a queste eventualità come *pure cyberterrorism*, cyberterrorism puro. In questo caso, lo sfruttamento del cyberspazio è incluso nell'attacco terroristico vero e proprio e non solamente a supporto di esso. Ad oggi, la maggior parte degli esperti sostengono che casi come questi non si siano ancora verificati; ma dagli stessi viene anche riconosciuto che, alla luce delle possibilità offerte dal cyberspazio e dalle competenze che sono state acquisite da vari attori terroristici, il cyber terrorismo, anche nella sua variante pura, costituisce una minaccia imminente per la comunità internazionale. Tra gli scenari più plausibili che sono stati identificati fino ad ora sono inclusi attacchi su larga scala, che possono essere effettuati a mezzo di DDoS (*Distributed Denial of Service)* o attraverso lo sfruttamento dei cosiddetti *Botnets* ad esempio. Inoltre, anche le tecnica dell'*hacking* può essere utilizzata per portare a termine un attacco cyber terroristico. È infatti sufficiente che il target dell'attacco sia un sistema SCADA (*Supervisory Control and Data Acquisition System)*, ovvero dei sistemi generalmente collegati a Internet che hanno il compito di controllare altri sistemi informatici. Spesso questi sistemi, nonostante la loro interconnessione implichi svariate vulnerabilità, sono utilizzati per controllare infrastrutture cruciali per la società contemporanea, come il sistema idrico, elettrico, delle comunicazioni e così via. Un'ulteriore scenario che potrebbe verificarsi in un prossimo futuro è il cosiddetto attacco ibrido, ovvero la combinazione delle tecniche usate da un tradizionale attacco terroristico con uno dei metodi sopraelencati. Ad esempio, il tradizionale attacco bomba potrebbe essere combinato all'hackeraggio del sistema SCADA al controllo del sistema di comunicazione di primo soccorso, permettendo di moltiplicare il danno causato alla popolazione civile in modo esponenziale.

Le competenze necessarie per portare a termine questo tipo di attacco sono sfortunatamente di facile accesso, spesso addirittura sono accessibili tramite una semplice ricerca Google; facendo sì che non si possa escludere l'eventualità di un attacco cyber terroristico sulla base della necessità di conoscenze informatiche estremamente raffinate. Ad aumentare la possibilità che questi scenari ipotetici si concretizzino, ci sono inoltre tutta una serie di vantaggi che comporta la scelta del cyberspazio come strumento terroristico. In primis, la velocità d'azione e l'anonimato di cui abbiamo già parlato. A ciò si aggiunge la possibilità di sferrare un attacco in qualsiasi luogo, senza il bisogno di essere fisicamente presenti in quel luogo. Infine, il mezzo informatico risulta essere relativamente economico; sono infatti necessari solamente una postazione PC e un accesso a Internet.

Passando dal piano fattuale a quello teorico, il panorama accademico e giuridico che circonda il tema del cyberterrorist è caratterizzato da un acceso dibattito. Allo stato attuale, infatti, non si può ancora dire di essere giunti a una definizione di cyberterrorism che sia accettata a livello globale. Il dibattito accademico si divide in due filoni, uno che sostiene che l'argomento in questione debba essere definito in modo più ampio, includendo anche le attività di supporto al cyber terrorismo; di modo tale da contrastare tutti gli aspetti legati a questa minaccia. Il secondo filone, invece, sostiene che dare una definizione troppo ampia di cyber terrorismo rischiarerebbe di renderla troppo vaga e di far sì che questa nuova definizione vada a sovrapporsi a quella di altre minacce, come l'*hacktivism* o il *cracking*. Per quanto riguarda il piano giuridico, nessuna definizione di cyber terrorismo è stata adottata e, tanto meno, esistono degli strumenti internazionali volti a contrastare questa minaccia. Tuttavia, in più occasioni le organizzazioni internazionali hanno riconosciuto la possibilità che la minaccia del cyber terrorismo si concretizzi. La mancanza di una definizione largamente accettata sul piano giuridico è principalmente da ricondursi al fatto che il termine in questione si componga di due termini altamente controversi, per cui a loro volta non è stata concordata una definizione: cyberspace e terrorismo.

Nonostante la mancanza di strumenti internazionali pensati per contrastare la minaccia del cyber terrorismo, questa ricerca ha preso in analisi degli strumenti internazionali già esistenti per valutarne la loro applicazione ed eventuale efficacia nell'eventualità di un attacco terroristico. Dopo una breve panoramica sugli strumenti ONU mirati a contrastare le varie manifestazioni del terrorismo, dato che la maggior parte dei trattati

in questo ambito vi fanno riferimento dato la mancanza di una definizione universalmente accettata di terrorismo, sono stati analizzati infatti tre diversi strumenti del Consiglio d'Europa, rispettivamente la Convenzione sulla criminalità informatica[1], il suo Protocollo addizionale relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici[2] e la Convenzione per la prevenzione del terrorismo[3]. Per quanto riguarda la Convenzione sulla criminalità informatica, o Convenzione di Budapest, essendo uno strumento internazionale pensato per la criminalizzazione di condotte perpetrate contro o attraverso il cyberspazio, l'applicazione degli articoli a eventuali casi di cyber terrorismo è chiaramente concepibile; ciò vale anche per il Protocollo addizionale di questa Convenzione. Tuttavia, questi due strumenti risultano essere efficaci solamente per la criminalizzazione di attività illecite che sono dei prerequisiti per la perpetrazione di un attacco cyber terroristico o, principalmente per quanto riguarda le condotte criminalizzate dal protocollo addizionale, delle summenzionate attività di supporto al cyber terrorismo. Nel caso della Convenzione per la prevenzione del terrorismo, nonostante essa non sia stata pensata per questa forma di manifestazione dell'attività terroristica, la formulazione degli articoli permette l'estensione della loro validità anche a tutti i casi in cui le condotte criminalizzate sono portate a compimento grazie ad un mezzo informatico. Data l'assenza di uno strumento internazionale finalizzato alla prevenzione e al contrasto di questa minaccia, la combinazione di questi tre strumenti internazionali, dunque, può garantire una parziale copertura di un eventuale attacco, seppur solo per i suoi stadi iniziali.

Dopo aver preso in analisi gli strumenti del Consiglio d'Europa che possono essere considerati come maggiormente rilevanti per il tema in oggetto, si è presa in analisi una proposta accademica per una Convenzione internazionale finalizzata al contrasto del

[1] Council of Europe, (2004) *Convention on Cybercrime ETS No. 185*, Budapest, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[2] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, Strasbourg, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.
[3] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, Strasbourg, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

cyber terrorismo: la cosiddetta Stanford Draft[4]. Questa proposta accademica risulta essere particolarmente rilevante per i fini della nostra analisi, perché si basa sulla Convenzione sulla criminalità informatica che, negli anni in cui questa bozza è stata elaborata, era nelle ultime fasi della sua stesura. Questa proposta accademica è particolarmente interessante perché propone in primis una definizione per il termine *cyberterrorism* e, assieme a essa definisce anche altri concetti che possono dal ruolo cruciale in questo ambito, come ad esempio cosa si deve intendere per *core infrastructures*, ovvero quelle infrastrutture fondamentali per la società contemporanea che vengono comunemente identificate come il target più plausibile di un eventuale attacco cyber terroristico. Questa proposta accademica, tuttavia, non è mai stata convertita in uno strumento internazionale con valore legale, probabilmente proprio per l'ultimazione della Convenzione di Budapest, che copre gli aspetti relative al crimine informatico in genere e non tocca la tematica più controversa del terrorismo, rendendo dunque più facile il raggiungimento di un consenso.

L'ultimo aspetto che è stato preso in analisi è quello della *cyberjurisdiction*, ovvero la giurisdizione informatica. I principi di giurisdizione sulla base dei quali viene conferita giurisdizione extraterritoriale a uno Stato sono stati stabiliti nel 1935 nella cosiddetta Harvard Draft e da allora, a parte per lo sviluppo di nuovi approcci nei loro confronti, non sono stati modificati. Infatti, quando si parla di giurisdizi0one informatica, ci si riferisce principalmente all'applicazione dei principi di giurisdizione esistenti al cyberspazio. Ciò implica che, nonostante nel caso preso in analisi da questa tesi si stia trattando un crimine che si svolge nel cyberspazio, quindi in una dimensione che nel 1935 non poteva certamente essere presa in considerazione, non ci siano dei principi di giurisdizione che tengano presente le peculiarità di questo spazio. Quest'ultimo, infatti, non rispetta le divisioni territoriali stabilite dagli Stati; inoltre all'interno di esso l'identità e la localizzazione degli individui possono essere nascosti. Alla luce di ciò, i tradizionali principi di giurisdizione, territorialità, nazionalità attiva e passiva, giurisdizione protettiva e universale, presentano una serie di limiti che rendono la loro applicazione al cyberspazio problematica. Tra i cinque principi elencati, quello che prevale su tutti è il principio di territorialità e questa prominenza viene mantenuta anche nella sua applicazione al cyberspazio. La Convenzione di Budapest, infatti, stabilisce

[4] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, pp. 25-45, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf.

come principio di riferimento proprio quello della territorialità, immediatamente seguito da quello della nazionalità. Date le peculiarità del cyberspazio che abbiamo menzionato poco fa, questi due principi potrebbero sembrare i meno indicati; tuttavia, la convenzione non vieta l'applicazione di altri principi che siano inclusi negli ordinamenti nazionali degli Stati che hanno ratificato la Convenzione in oggetto. Per quanti riguarda la Stanford Draft, anch'essa propone come base di giurisdizione il principio di territorialità e, in sostituzione, quello di nazionalità; ma, allo stesso tempo, ammette l'applicazione di altri principi a condizione che siano inclusi nell'ordinamento internazionale. Questa clausola permetterebbe l'applicazione dei principi di giurisdizione protettiva e universale, che a livello accademico vengono spesso proposti come le migliori alternative per definire la giurisdizione su un caso di cyber terrorismo. Tuttavia questi principi, essendo svincolati dal nesso della territorialità o della nazionalità, allo stato attuale della loro formulazione, implicherebbero un'alta probabilità di conflitti di giurisdizione, dato che conferirebbero il diritto a più stati di reclamare la giurisdizione su un ipotetico attacco.

Alla luce di quanto riscontrato, la nostra proposta per poter contrastare la minaccia del cyber terrorismo e coprire gli aspetti che vengono lasciati scoperti dagli strumenti esistenti, sarebbe quella di elaborare un ulteriore Protocollo addizionale relativo alla Convenzione sulla criminalità informatica. Ciò permetterebbe di evitare la sovrapposizione tra strumenti internazionali, non dovendo trattare gli aspetti già coperti dalla Convenzione stessa. Inoltre, un Protocollo addizionale richiede comunque la ratifica da parte dello Stato prima di produrre su di esso degli obblighi vincolanti; di conseguenza, un'eventuale soluzione non avrebbe ricadute negative sul numero di ratifiche raggiunto dalla Convenzione di Budapest. Inoltre, il Consiglio d'Europa sta attualmente elaborando un secondo Protocollo addizionale, con lo scopo di ampliare l'efficacia della Convenzione di Budapest. La criminalizzazione del terrorismo informatico sarebbe in linea con tale finalità e garantirebbe un approccio preventivo e non reattivo al problema del cyber terrorismo. Infine, un eventuale Protocollo addizionale potrebbe essere utilizzato per risolvere gli aspetti problematici legati all'ambito della giurisdizione informatica, portando chiarezza su questo campo ancora molto controverso.

Introduction

Since the introduction of the cyberspace and the consolidation of its role in contemporary society, the latter has grown more and more dependent on it. Nowadays, the possibilities offered by the cyberspace and ICT are made available to most of global population and can accessed almost from all over the world. However, all that glitters is not always gold and the flaws of such a pivotal system have been discovered and exploited by maliciously-intended users. As a matter of fact, technology is not the only aspect that has been evolving in the last decades; on the contrary, criminality has been changing as well by learning how to exploit the chances offered by this new frontier.

The most alarming aspect of this issue is that the exploitation by maliciously-intended users of the cyberspace does not limit itself to regular criminals, quite on the contrary it can be claimed that terrorist actors have been taking advantage of the cyberspace as well. As a matter of fact, international terrorism has been changing for centuries, both on the motivational aspect underlying the terrorist act per se[5] and on the methodological level, expanding its means to newer and more detrimental techniques. The cyberspace is probably the last frontier approached by international terrorism and such a threat seems to be growing more and more concrete. For this precise reason, the purpose of this dissertation is to take into consideration an issue that was labelled as "the combination of the two of the great fears of the late 20th century[6]".

In the last years the presence of the issue of cyberterrorism in the academic debate has become more and more prominent. In addition to that international organisations have acknowledged it as a concrete threat and in some cases they contributed in the first place in the literature on the matter. However, to date there is no international legal instrument dealing with the issue of cyberterrorism. Such a situation led to the choice to face this dissertation by focusing on the two constituent elements of cyberterrorism: the cyberspace and terrorism. As a matter of fact, as far as the judicial matter is concerned, the two core Conventions that will be analysed in detail are the Council of Europe Convention on Cybercrime and the Convention on the Prevention of Terrorism.

---

[5] Rapoport, D. C. (2008) *The four waves of modern terrorism*, In *Terrorism Studies: A Reader*, eds. John Horgan and Kurt Braddock, pp. 46-73, available at https://www.international.ucla.edu/media/files/Rapoport-Four-Waves-of-Modern-Terrorism.pdf.

[6] Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, p. 8.

Being cyberterrorism a relatively new threat to contemporary society, for the purpose of a better understanding of the matter the first chapter will try and provide an answer to the question *what is cyberterrorism?* The chapter will open with an overview of the most plausible scenarios, an assessment of the risks and the individuation of possible targets. We will then leave aside the possible concrete manifestations of cyberterrorism to take into account the definitional matter. If answering the research question of this chapter on the basis of the possible manifestations of cyberterrorism is a less controversial matter; trying to do the same on the basis of the current debate on how to define cyberterrorism is more complicated. As a matter of fact, there is no agreement on a consensus definition yet cyberterrorism yet. Such a situation allows the development of different schools of thought on the matter, which propose different approaches to the matter rendering the task of answering the question at stake more complicated. However, if on the academic level several and different definitions of cyberterrorism can be found, no international organisation has given its contribution on the definitional matter. The reasons to which this choice can be attributed to, will be taken into consideration in this chapter as well. Finally, due to the fact that this dissertation could not be broad enough in order to take into account all the possible international legal frameworks, the choice of the Council of Europe will be justified.

The aim of the second chapter is to assess whether the existing CoE international legal instruments can be of use in case of a cyberterrorist attack. Due to the premise that we made above, the focus will be on the Convention on Cybercrime and its Additional Protocol and on the Convention on the Prevention of Terrorism. We will evaluate which aspects of cyberterrorism can be covered by these two international legal instruments and which are left uncovered. In order to do so, the applicability of the provision of the Conventions at stake to instances of cyberterrorism needs to be pondered; due to the fact that, as anticipated, no international legal instrument has been realised with the purpose of addressing the threat of cyberterrorism yet. The second chapter will conclude with an overview of the so-called Stanford Draft, which is an academic proposal for a international convention explicitly addressing the issue of cyberterrorism. Such a proposal is relevant for the framework of analysis of our dissertation, because it basis itself on the CoE Convention on Cybercrime and on the standard it has contributed to creating.

The third and final chapter will address the matter of cyberjurisdiction. Being cyberjurisdiction nothing but the extension of the pivotal concept of jurisdiction under international law, the traditional jurisdictional basis will be taken into analysis. Subsequently, their application to the cyberspace and, more precisely, to possible instances of cyberterrorism, will be taken into account. Such a passage will allow us to highlight the difficulties that arise in the process of assessing jurisdiction over a crime that has been committed by means of or against the cyberspace. Cyberjurisdiction, just like cyberterrorism is one of the debated subjects of the last years, however there seems to be no consensus on this field either. As a matter of fact, some call for a reform of the jurisdictional framework, on the basis of the peculiarities of the cyberspace that distinguish it from other *loci* on which jurisdiction might need to be assessed. On the other hand, others affirm that the existing jurisdictional framework needs to be applied to the cyberspace as well, just like it is applied in other instance. The former approach is the one that is mainly proposed in the academic field; while the latter is the one that is preferred by international organisations. As a matter of fact, the jurisdictional basis proposed by article 22 of the CoE Convention on Cybercrime will be taken into analysis as a proof of the previous statement. In addition to that, we will also analyse how the Stanford Draft proposes to assess jurisdiction on instances of cyberterrorism and evaluate if its proposal is in line with the current approach of international organisations or if it could be seen as a watershed.

Chapter 1: An analysis of the phenomenon of cyberterrorism

Introduction

The following chapter is aimed at introducing the topic of cyberterrorism and at illustrating the complexity of this issue. Cyberterrorism is deemed to be a concrete and imminent threat to our society by more and more actors and the consequences of such issue are already dramatically foreseeable[7]. Nonetheless, there is no unitary discipline on this issue, establishing how actors should deal with this phenomenon[8]. The aforementioned lacuna contrasts with the for a coordinated and joint effort by actors having to deal with this topic[9], due to the danger that such a transnational threat constitutes for the whole society. In starting research on the topic of cyberterrorism, another contrast that strikes the observer's attention: despite the fact that several possible scenarios have been identified by experts, who worn about the risk that they pose to our society, there is still no globally accepted definition of cyberterrorism. As a consequence, the lack of the very basic step of defining the object at stake, does not cause only merely descriptive problems, but it renders operations in all other related fields, such as criminalisation and prosecution, extremely more complicated[10].

This chapter will open with an overview of the ways in which terrorist actors exploit the cyberspace, both using the internet as a tool and choosing it as a target of their illicit actions. On the basis of this first step, the chapter will go on with the evaluation of the possible targets and main threats to international security. Subsequently, this chapter will move from factual aspect to the descriptive one, dealing with the issue of cyberterrorism definition, analysing the difficulties in establishing a universally accepted definition. The chapter will also bring examples of the most relevant academic definitions that have been provided so far. Moreover the common elements of the latter, as well as the distinctive ones, will be analysed. The first chapter will close with a paragraph explaining the reasons that led us to the choice of the Council of Europe as framework of analysis for this dissertation.

---

[7] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, pp. 57-118.

[8] Conway, M. (2007) *Cyberterrorism: Hype and Reality*, in Armistead, Leigh, (ed.) Information warfare: separating hype from reality. Potomac Books, Inc., pp. 73-93.

[9] Bogdanoski, M., & Petreski, D. (2013) *CYBER TERRORISM– GLOBAL SECURITY THREAT*, International Scientific Defence, Security and Peace Journal, Vol. 13, Issue 24, pp. 59-73.

[10] Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, pp. 139-192.

1.1 The cyberspace as a target of cyberterrorism

Cyberterrorism is a debated subject nowadays and different opinions have risen about it in the academic discussion. However, if on the one hand the theoretical debate about cyberterrorism, which will subsequently be analysed, seems to be far from an agreement; on the other hand, there seems to be a higher degree of unity in the study of the possible concrete manifestations of cyberterrorism. The starting point of such analysis is the so-called TCP/IP protocol, on which the Internet, just like other ICT systems, is based. Such protocol, as explained by author Kelly Gable, executes the role of the 'language[11]' of the cyberspace, as it allows information to flow from server to server and computer to computer. The crucial point is that, such protocol was realised for the exclusive use of government agencies in the period of Cold War; making it unnecessary to take specific security measures against criminals. As a matter of fact, at the dawn of the ICT only governments had access to this system, thus the priority was efficiency and not security. Being governments regarded as trustworthy users, no security measures to hinder the malicious exploitation of the system were included. In the light of this acknowledgment, it can be affirmed that vulnerability is inherent to the cyberspace, due to the inherent weakness that characterises the TCP/IP protocol[12].

The main problematic aspect about the TCP/IP protocol, is that it allows to move from the Internet, which has no barriers to access, to all other networks that are based on the same protocol. This condition creates a situation in which a cybercriminal, just like a cyberterrorist, can skip not only from a computer to another, but also from a network to another. This phenomenon is known as 'island-hopping[13]' and it allows cyberterrorists to considerably amplify the effects of their attacks. As a matter of fact, this security flaw in the cyberspace allows cybercriminals to disregard any kind of border and to

[11] As explained in Gable, K. E., (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*: The TCP/IP Protocol operates by a sequence of communications between the sending computer or network and the receiving computer or network, known as a "three-way handshake." Essentially, Computer 1 tells Computer 2 that it wants to communicate. Computer 2 responds that it is willing to communicate. Computer 1 then sends Computer 2 a message confirming that they are going to communicate.

[12] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, p. 78.

[13] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, pp. 57-118.

potentially strike their attacks everywhere in the world, despite of their physical location.

The flawed structure of the TCP/IP protocol at the basis of ICT renders the cyberspace itself one of the possible targets of cyberterrorism. Furthermore, the interconnectedness of cyberspace is probably the distinctive element that renders it vulnerable the most. Indeed, when targeting an object in the cyberspace, a whole net is potentially targeted and therefore, what is in danger is not the unit, but a whole system.

Cyberterrorist attacks directed against the computer system usually compromise the confidentiality, integrity and availability of the network[14]. This branch of cyberterrorist attacks is referred to as "pure cyberterrorism" by a considerable number of scholars, who agree with the distinction outlined by Gordon and Ford. Indeed, for them pure cyberterrorism is limited to those attacks targeting computers, networks, online facilities and so on; in other words, targeting the elements operating in and constituting the cyberspace[15]. The counterpart to pure cyberterrorism is "traditional cyberterrorism", which includes as cyberterrorism also the use of the cyberspace and its constituents as a weapon and not just as target[16].

The information system officer Jonolan Brickey classified cyberterrorism in three different clusters, which can be helpful to understand what is meant when we say that the cyberspace can be a target of as well as a tool for cyberterrorists. He divides these attacks into *enabling*, *disruptive* and *destructive*[17] cyberterrorist attacks. The first category does not belong to pure cyberterrorism, while the other two do. Indeed, the first category refers to all those illicit activities perpetrated in the cyberspace that contribute to the striking of the attack; this category will be analysed later.

Disruptive cyberterrorist attacks are aimed at activities like taking down pivotal websites or harming or destroying that part of a society's lifestyle, which is dependent on cyberspace facilities. These activities are carried out though techniques like web

[14] Clarke, P., & Garnett, R. (2005) *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 474-488.
[15] Ford, R., & Gordon, S. (November 2002) *Cyberterrorism?*, in Computers & Security, Vol. 21, No. 7, pp. 636-647, available at https://www.researchgate.net/publication/222546033_Cyberterrorism.
[16] Ibid.
[17] Brickey, J. (August 2012) *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, CTC Sentinel, Vol. 5, Issue 8, pp. 5-6, available at https://www.researchgate.net/publication/235782714_Defining_Cyberterrorism_Capturing_a_Broad_Range_of_Activities_in_Cyberspace.

defacement, distributed denial of service (DDoS), the unauthorised access, modification, disclosure or elimination of confidential information[18]. Cyberterrorism, just like ordinary terrorism, can envisage serious injury to human lives and property. In the case of disruptive cyberterrorist attacks, the possibility of injury to property results to be the most possible one. Indeed, we just need to think about the economic field to understand how property in the cyberspace can be as tangible and of core relevance for individuals as in the physical world. Nowadays, more and more aspects of the economic sphere are dependent on digital technology[19], implying that they can be liable to an attack perpetrated on the cyberspace, by regular cybercriminals, just like by cyberterrorist. Once again, it is important to underline the fact that these two categories of perpetrators of crimes do not overlap, even though the means with which their crimes are perpetrated might coincide. Indeed, what distinguishes them is the underlying intention that spurred them to take action. For instance, when it comes to hackers committing illicit activities in the economic field of the cyberspace, most of the times they are driven by the economic gain they can derive from it. On the other hand, when we are dealing with cyberterrorists perpetrating cybercrimes in the economic sphere, though the economic gain is not excluded at all and it will be analysed in the following sections, the terrorist intention lies in the willingness to coerce the authorities into an economic change, by means of the use of violence or threat to use of violence resulting in injury to human lives or property. For this reason, the whole e-commerce system, the Stock Exchange Market as a whole, large part of the banking system, bank accounts, economic transactions related to international trade and so on, are all possible targets for this kind of attack. In affirming that these are plausible targets, we are referring to the core elements of the definitions of cyberterrorism that will be analysed later on in this chapter. However, to briefly anticipate the matter we can claim that an attack by cyberterrorists towards these targets would be among the aims included in the mainstream definitions of cyberterrorism and in the ones of terrorism; would imply a critical role of the cyber element in the carrying out of the illicit actions and finally, would cause a considerable harm to property. Indeed, in the abovementioned cyber-facilities we witness the circulation of the two elements that practically compose the online market itself: purchasable goods made available by the e-commerce and money, whether they are in the form of capital and stored in bank accounts or they are in the

[18] Ibid.
[19] Rossi, S. (25 March 2019) *Moneta e banche: le origini strutturali della crisi*, Conference held at Ca' Foscari University of Venice, stable URL https://www.unive.it/data/16437/1/26936.

form of shares of the Stock Exchange[20]. The international economic transactions are the element that links these two parts of the online market together, leading us back to the vulnerability that interconnectedness implicates in this field.

A potential and realistic scenario was proposed by the CoE in 2007: it is rather easy for terrorist groups to exploit the cyberspace to spread misinformation and they could use this possibility to direct investors towards a specific company or bank and then take down that company or bank by means of a distributed denial of service (DDoS). Such a situation, in which communication is either compromised or blocked, could have the long-lasting consequence of a lack of confidence in the reliability of the financial system[21]. Unfortunately, such a scenario is not just an hypothesis, but on the contrary it already concretised. Indeed, we have already witnessed this kind of strategy the 18th June 1999 in conjunction with the Cologne G8, when the "J18" group incited people to act individually in order to disrupt "financial centres, banking districts and multinational corporate power bases[22]". This call for action resulted in hackers from Indonesia, Israel, Germany and Canada targeting the computers of companies and, worst of all, of the Stock Exchange[23]. Though the aforementioned precedent as been classified an example of hacktivism, this episode, together with a lot of others, is the proof of how this kind of scenario is likely to happen, also at the hand of terrorist actors.

Historically speaking, economical targets have always been among the main ones for terrorist groups[24], that is why the vulnerability of the online market self-evidently reflects on all those societies, whose economy strongly relies on the cyberspace[25].

---

[20] Bruce, S. L., Flynn, S. M., & McConnell, C. R. (2010) *Essenziale di economia*, McGraw-Hill, second edition, Milan.

[21] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

[22] Denning, D. E. (2001) *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defence Research Institute RAND, p.257, available at https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.

[23] Denning, D. E. (2001) *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defence Research Institute RAND, pp. 238.288.

[24] Probably, the most relevant evidence of this statement in contemporary history is 9/11 which targeted the Twin Tower of the World Trade Centre, popularly recognised a symbol of the free market economy and all the values it implies.
See Lewis J. (2004) *Cultural Studies - The basics*, SAGE Publications.

[25] We have already underlined the fact that one of the reasons explaining the different perceptions over cyberterrorism is the different level of dependence on cybertechnology, which is peculiar for each society. Most scholars have made the case for years that those societies that should be concerned the most about this threat due to their dependence on cybertechnology are the Western ones. However, this classification can no longer be considered as an up-to-date one. Proof of this, is the unparalleled role that

Moreover, as highlighted in the Council of Europe report of 2007, this kind of attack implies "economic confusion" and the "discrimination of the opponent", which are strictly correlated. Indeed, a successful attack demonstrates the capabilities of the terrorist group, generates fear and proves a lack of technical competence by the authorities, causing a loss of trust on them by civil society. The willingness to cause both economic confusion and the discrimination of the opponent is justified, according to this study, by the tendency of terrorist group to act in order to reach long-term goals[26]. This perspective is a further helpful element to use, in order to differentiate cyberterrorists from other kinds of cybercriminals.

The third and last cluster of cyberterrorism identified by Brickey is the destructive one. The goal of cyberterrorists in this case is "to manipulate computer code and to corrupt information system functions to damage or destroy virtual and physical assets[27]". This kind of cyberterrorists attack is strictly linked to one of the core elements of terrorism and cyberterrorism: the psychological effect of fear. As a matter of fact, a peculiarity of cyberterrorism compared to regular terrorism, is the fact that the lack of claim for responsibility can be aimed at causing the loss of confidence in critical systems and their competent authorities[28]. In almost every case of successful terrorist attacks, the last act is the claiming of responsibility for such acts; as a consequence, anonymity results to be relevant only during the preliminary stages of the act itself. When it comes to cyberterrorism, the relevance of anonymity changes and it acquires a different value, due to which it might be convenient for cyberterrorists not to claim responsibility for the act at all. This situation happens mainly for two reasons. First of all, when a terrorist group claims responsibility for an attack, the consequence is public opinion pitying the victims of the attack. However, when the terrorist attack happens due to the exploitation of the cyberspace and there is no claim for responsibility, this leads the public opinion

countries like China and Japan play nowadays in the field of cybertechnology. Moreover, resilient and safe cybertechnology is promoted as an effective tool to reach the goals set by the United Nations Sustainable Development Goals (SDGs). Therefore, hopefully the digital divide will become smaller and smaller; however implying as a downside that more and more societies will be exposed to this threat. See New America, *Appendix: the SDGs and Cybersecurity*, Securing Digital Dividends, stable URL https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/appendix-the-sdgs-and-cybersecurity/ , last accessed 21st March 2020.

[26] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

[27] Brickey, J. (August 2012) *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, CTC Sentinel, Vol. 5, Issue 8, p. 5, available at https://www.researchgate.net/publication/235782714_Defining_Cyberterrorism_Capturing_a_Broad_Range_of_Activities_in_Cyberspace.

[28] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

to think that the harm was caused by technical incompetence of the competent authorities, which, in the end leads to a loss of trust and esteem. In addition, publicly claiming responsibility for a cyberterrorist attack, would imply the confirmation that terrorist groups have the means and the capabilities to exploit this crucial space. This implicit acknowledgment would spur the competent authorities to reinforce cybersecurity, rendering it much more difficult to exploit the cyberspace for terrorist purposes and criminal ones in general[29]. For this reason, the psychological harm in the case of the destructive cluster of cyberterrorism is dual in nature. This argumentation acquires particular relevance as a counter-thesis to the reasoning of the academics, who make the case that cyberterrorist attacks have never occurred yet. On top of that, in the recent years we have witnessed cyberattacks directed against governments, such as the attacks against Estonia in 2007, Georgia in 2008, Iran and Burma in 2010[30] that is why the lack of claim for responsibility cannot be considered enough to exclude this lead[31].

It is therefore clear that pure cyberterrorism is a plausible threat, which could target one of the core aspects of our societies. This threat can be carried out by means of several types of cyberattacks, which have already taken place in recent history. The wide array of possible cyberattacks that can be perpetrated by cyberterrorists just like by regular cybercriminals can result in fraud, identity theft, theft of sensitive data or intellectual property, espionage, sabotage, demonstrative attacks and extortion[32]. As we have

[29] Ibid.
[30] Luiijf, E. (2014) *Cyber Terrorism: Case studies*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, pp. 163-174.
[31] Up to date, some of the most relevant examples are: the facts occurred during the conflict in Nagorno-Karabakh in 1999, when hackers modified the blood types registered in the hospital database exposing people to a life-threatening situation (see Luiijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 16.); *The Titan Rain Case* affecting US computer systems and network from 2003 to 2006; *The cyber-attack against Estonia* of April 2007 against the infrastructures linked to the websites of ministries, the two major banks of the country and several political parties; the distributed denial of service (DDoS) against Georgia of 2008, which turned down Georgian servers; the digital worm that stopped Iran's nuclear program in 2010; (see Kyriakopoulos, G. D. (2017) *Cyber-attack, Cyber-warfare: arranging definitions*, in J.-P. Jacqué, F. Benoît-Rohmer, P. Grigoriou & M.-D. Marouda (Eds.), Liber Amicorum Stelios Perrakis, I. Sideris, Athens, pp. 497-511.)
[32] Zappa, F. (2014) *Cybercrime: risks for the economy and the enterprises at the EU and Italian level*, United Nations Interregional Crime and Justice Institute, available at http://www.unicri.it/in_focus/files/Cybercrime_and_the_Risks_for_the_Economy_Flavia_Zappa_2015_06_11.pdf.
Definitions provided in the text for the aforementioned crimes related to the cyberspace:
"Fraud is the act of entering computer systems without permission in order to unlawfully access the services provided by the victim company.
Identity theft is a scam in which the objective is to steal the identity of a person or company in order to obtain resources, information, or unlawful authorization.
[..] espionage is an activity in which the main objective is to illegally obtain [..] information.

already clarified, we are now dealing with the so-called pure cyberterrorism and therefore, that kind of cyber terror, which has the computer systems itself as a target. Indeed, these attacks take place in the cyberspace and their targets are in the cyberspace as well, therefore fulfilling one of the conditions set by the definitions we will analyse in the next section of this dissertation; precisely the one according to which "cyber must play a consequential or essential role in the act[33]".

So far, we have only analysed that kind of cyberterrorist attack that takes place in the cyberspace and whose target is an aspect of the cyberspace itself. However, the most harmful effects of pure cyberterrorism are caused by those attacks against the cyberspace, which target websites, networks, programs and so on that are directly linked to the real world for several reasons. Indeed, here lies the main source of fear generated by cyberterrorism: the developments in the branch of technology created a situation in which it is convenient and efficient to rely more and more on technology in a wide array of fields of our society; that is why a lot of experts claim that "it is only a matter of time before the danger of life-threatening cyberterrorism manifests itself[34]".

This kind of cyberterrorist attacks target IT-infrastructures that are linked or control core infrastructures in the real world. Once again, what classifies these attacks as cyberterrorism and not regular cybercrime is the underlying intention; with regard to this, the Council of Europe report on the issue of cyberterrorism of 2007 states that these attacks are basically the same as those launched by "common" cybercriminals, but with a terrorist interest or intention[35]. In this instance just like in the case of cyberterrorist attacks confined to the cyberspace, these attacks imply the corruption of the integrity and confidentiality of computer systems and data in case of circumvention of security measures and the loss of the availability of a wide array of online services caused cyberattacks, which are able to render a system useless or no longer working.

Sabotage is an action that aims to slow down or block the activities of the victim [..] through the hindrance of normal operations - using means such as destruction of important material or equipment used by the victim [..].
Individuals or groups of people usually cause this type of attack as a protest against the victim [..] accused of misconduct by end users or private citizens.
Information extortion is a criminal act in which the perpetrator installs software such as malware or ransomware on the victim's computer without the victim's permission".

[33] Douglas, C. A., Griffith, C.,. Murray, G. R, Heslen, J. J., Davies, K. L., Hunter, Y., Jilani-Hyler, N., & Ratan, S. (23 March 2019) *Towards Creating a New Research Tool: Operationally Defining Cybeterrorism*, Augusta University, p. 5.

[34] Hiryaev, Y. S. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, p. 141.

[35] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

However, when the cyberattack is directed to an IT-infrastructure that has a tangible link to the real world, there is another important consequence to be added. Indeed, if the IT-infrastructure controls core infrastructures in the real world, such as transportation, energy facilities, water facilities and so on, the potential attack would imply physical harm to individuals if not their death[36]. Several kinds of attacks and combinations of them could lead to this scenario, however, the CoE highlighted four main types of attacks, which are in line with the objectives and means of the terrorist actors and groups.

a. Large-scale attack

This first cluster mainly exploits the so-called *bot-nets*, the abbreviated term for 'network of robots'[37]. The Specialist in Technology and National Security Foreign Affairs, Defence, and Trade Division Clay Wilson stated that these networks are composed by a large group of computers that have been compromised and thus, that can be remotely controlled by means of Internet. The effects of this kind of attack are amplified by the possibility to have a huge number of compromised computers working at the same time, either to disrupt of block Internet traffic or to collect private information[38].

Bot-nets can be easily purchased or rented online, where bot-net designers, the so-called 'botmasters' sell the result of their illicit activities to the highest bidder[39], making them available for terrorists, who could exploit the anonymity that can be obtained in the web to buy them undercover. Terrorist groups buying or renting bot-nets is a plausible scenario, because it would allow a wide range of actions, from the less detrimental such as propaganda, to the most harmful ones[40], such as the taking down of the IT-infrastructure, which controls the first aid communication system for instance.

[36] Ibid
[37] Ibid
[38] Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service, p. 5.
[39] "For example, Jeanson Ancheta, a 21-year-old hacker and member of a group called the "Botmaster underground", reportedly made more than $100,000 from different Internet Advertising companies who paid him to download specially-designed malicious adware code onto more than 400,000 vulnerable PCs he had secretly infected and taken over. He also made tens of thousands more dollars renting his 400,000-unit "botnet herd" to other companies that used them to send out spam, viruses, and other malicious code on the Internet. In 2006, Ancheta was sentenced to five years in prison."
See Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service, p. 5.

[40] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

Furthermore, bot-nets can be rented as well, implying that they could be a source of income if rented to third parties. Last but not least, being bot-nets available-for-sale, there is no need for the terrorist actors to have particular technological skills or abilities.

These networks of robots are exploited to implement large-scale distributed denial of service, or DDoS. A DDoS is defined as

> "A cyber attack in which a cracker[41] bombards a targeted computer with thousands (or more) of fake requests for information, causing the computer to run out of memory and other resources and to either slow down dramatically or to stop. The cracker uses more than one (typically hundreds or thousands) of previously cracked computers connected to the Internet to start the attack. These computers are called "zombies," indicating that they operate under somebody else's control who has evil intentions. The multiple origins of the attack make it difficult to defend against[42]."

The "zombies" must then report to a bot-net regularly and they are controlled and instructed by the bot-master. This technique is used to bring down computer systems or to stop the data flow, but cannot allow the access to protected data.

An example of the exploitation of this combination of bot-nets and DDoS was the FloodNet attacks launched by pro-Israeli hackers to make the Hezbollah's website collapse[43].

b. Hacking attacks

Hacking technique cover the void left by the combination of bot-nets and DDoS, exploiting the weaknesses of the system to access it without authorisation. A successful hacking attack often culminates in the so-called *defacement*. This procedure is constituted by the replacement of the main page of a website with another page[44]. This move is aimed at making it clear that the website has been hacked, publicly showing to the users its vulnerability and the weakness of the system and, at the same time,

[41] Crackers can be defined as hackers driven by broad criminal intents.
[42] Martin, C., & Schell, B. (2006) *Websters' New World Hackers Dictionary*, Wiley Publishing Inc, p. 102. See "DDoS".
[43] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[44] Martin, C., & Schell, B. (2006) *Websters' New World Hackers Dictionary*, Wiley Publishing Inc, p. 102. See "DDoS". See "Deface".

demonstrating the technical abilities of the terrorist group[45]. The damage to the image of the victim of the attack and the spread of fear resulting from the display of the cyber capabilities of terrorist actors can be reached also by means of the former type of cyberattack. However, as we have previously anticipated, what can be reached solely by means of hacking is the access to data. This action opens the door to a wide number of possibilities, including the destruction of the vital data of a system or the mere access to data, which should never fall into the hands of terrorists; such as financial instruction's records, national security plans, health system organisation data, military secret documents or nuclear research centres[46].

The lack of claim for responsibility by cyberterrorist actors is plausible in this case as well. Indeed, in most cases of defacement by regular hackers, they have only made it explicit that the website had been hacked and just a few hint at their identity. In the case of cyberterrorism, it would also be advantageous not to make it explicit that the illicit act was perpetrated by cyberterrorists for the reasons we have already explained at the beginning of the section. In addition, when it comes to the successful hacking of core IT-infrastructures or to the access of pivotal data, it is likely that they prefer to act without any explicit admission. This is because an explicit admission would spur authorities to fix the security flaws, which could no longer be exploited[47]. A plausible attack to be exploited in this eventuality are the so-called *Zero-Day exploits*. These exploits are attacks that are not known to anybody yet, including the manufacturer of the targeted item[48]. These attacks and the dangers they imply for the cyberspace and its users are defined as:

> "Abbreviated as 0-day exploit, it capitalizes on vulnerabilities right after their discovery. Thus, zero-day attacks occur before the security community or the vendor of the software knows about the vulnerability or has been able to distribute patches to repair it. For this reason, these exploits allow crackers to wreak maximum havoc on systems. The term "0-day" relates to the fact that the value of exploits decreases rapidly as soon as they are announced to the public .The next day after the announcement, for example, exploits are half as valuable to crackers. By the second day after the announcement, they are one-

[45] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[46] Ibid.
[47] Ibid.
[48] Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service, p. 9.

> fourth as valuable, and 10 days later, they are one one-thousandth as valuable as on day 0[49]".

This definition lets us infer that, just like in the case of bot-nets, zero-day exploits can be purchased online, more precisely in the dark web[50]. That is why, the latest vulnerabilities are exploited to develop and sell hacking tools and cyber weapons to the highest bidder, regardless of their intention[51]. As a matter of fact, the 'decentralised character of the Internet' allows demand and offer to meet and the trade of cyber weaponry to prosper. To date, the offer varies from cheap one-time DDoS to expensive and elaborated systems that enable the purchasers to systematically exploit the weaknesses of the ICT[52].

c. Hybrid attacks

This scenario is even more worrisome than the previous ones, because it combines classic terrorist attacks with pure cyberterrorism. The likeliest kind of attack is the DDoS. This is due to the fact that, as we have already seen, through DDoS it is possible to forbid the fruition of online utilities and this possibility has some extremely dangerous implications for our society. For instance, the CoE portraits as a plausible[53] scenario a bomb attack in conjunction with a DDoS targeting the voice communication systems of emergency services or the communication devices of police. This concerning situation would allow terrorist actors to go undisturbed and cause a much greater harm to their victims than they regularly would[54].

However, the physical injury is not the only consequence that would be exacerbated by the combination of pure cyberterrorism and classical terrorism. Indeed, the

---

[49] Martin, C., & Schell, B. (2006) *Websters' New World Hackers Dictionary*, Wiley Publishing Inc, p. 37. See "Zero-Day exploits".

[50] Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service.

[51] Ibid.

[52] Cohen, D. (2014) *Cyber terrorism: case studies*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 170.

[53] All the scenarios depicted by the CoE in the volume *Cyberterrorism- the use of internet for terrorist purposes* are based on actual weakness of the cyberspace, which have been spotted and demonstrated. In addition, most of the hypothesized cases are derived from cyberattacks, which have already been witnessed in our history. However, has we have already highlighted, the possible scenarios could potentially be even worse, if we recall the definition of zero-day exploits and the several reasons for which it can be convenient to let a successful cyberattack go unnoticed.
See Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing and Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service..

[54] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

physiological harm to the victims would be considerably intensified, due to the fact that the presence of cyberterrorism in conjunction with the regular one puts together all the psychological consequences we have highlighted so far: fear, which is inherent to all forms of terrorism, though in this case it would be even greater due to the acknowledgment that such dangerous actors have such detrimental capabilities; and the loss of trust in the authorities, caused by pure cyberterrorism showing the technical incompetence of the authorities and putting the victims into a completely helpless position.

The terroristic attack by the Islamic State against the French newspaper *Charlie Hebdo* editorial staff on 7th January 2015 can be regarded as an instance of the combination of conventional terrorism, with the terrorist exploitation of the cyberspace. As a matter of fact, it has been esteemed that approximately 19.000 French websites were hacked contemporary to the actual terrorist attack. Most of the websites that were targeted belonged to other Newspapers and they were defaced in order to use them as means to spread propaganda and threats[55]. It is true that the hacking of these websites did not produce further victims, but it certainly contributed to spread and exacerbate fear in the population. This aspect is relevant, due to the fact that causing a strong sense of fear can be regarded as one of the aims of terrorist actors.

d. Attacks resulting in physical damage

Though the aforementioned case includes physical damage, it is because it is combined with classical forms of terrorism. However there can be instances of pure cyberterrorism, which can produce physical damage on their own. The main means to achieve this goal is exploiting the Supervisory Control and Data Acquisition systems, generally known as SCADA systems. These systems are used to control other IT-systems and in some cases they are connected to the Internet as well. This interconnectedness would not be advisable for security reasons; indeed each system should be controlled on-site by a physical workers. However, being SCADA systems economically convenient and efficient in terms of time, they are preferred to the safer way of managing systems. It was esteemed that 17%[56] of the malfunctions in SCADA

[55] Giantas, D., & Stergiou, D. (2018) *From Terrorism to Cyber-terrorism: The Case of ISIS*, Hellenic Institute of Strategic Studies, pp. 1-32, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927.

[56] This number is referred to the study conducted to realise the CoE report of 2007, therefore the number has plausibly varied in these years.

systems are caused by a direct Internet access, VPN connection, modem connection or trusted connections. Moreover, a lot of these control systems are based in Windows or Unix operating systems, which are popular systems, whose weaknesses are well-known by most cybercriminals[57].

The dangers implied by the vulnerability of using a SCADA system to control other IT-systems were proved in 2000 by the cyberattack against the SCADA system controlling a water treatment facility Queensland, Australia, in 2000. Vitek Boden, the operator who had installed the targeted SCADA system, after resigning from his job released 800,000 of raw sewage into the rivers and green spaces nearby. This attack destroyed the marine life involves, created come health problems to people living nearby and spread a sense of fear and confusion[58]. Another scenario by historical record is the power-down of energy of 2003 in the United States and Eastern Canada, during which 21 power plants were shut down by the W32.Lovsan worm, leaving 60 million households with no electricity. Had cyberterrorist known about this security flaw, they could have exploited it just like regular cybercriminals[59]. An even more dangerous instance was proven to be possible by the Stuxnet cyberattack, which was aimed at disrupting and sabotaging the nuclear program of the Iranian government[60].

However, the worst aspect about cyberattacks directed against SCADA systems is the high possibility for such an attack to cause the loss of human lives. That is why, despite being the hardest cyberattack to launch, it would reasonably be the most attractive one for terrorist actors. The CoE depicts as a plausible scenario cyberterrorists gaining control over a SCADA system controlling hydroelectric dams, being able to open the gates in order to flood the urban areas nearby[61]. This scenario is not derived from fantasy, quite on the contrary these systems have already been accessed twice so far, though not resulting into injury[62]. Another particularly detrimental scenario in case of exploitation of SCADA systems affects the transportation system. The derailment of a train caused by the missed relocation of the rail would implicate physical injury for the

[57] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] Giacomello, G. (2004) *Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism*, Studies in Conflict & Terrorism, Vol. 27, pp. 387-408.

victims, if not their death[63]. The last scenario depicted in the analytical report of the CoE foresees SCADA systems controlling nuclear power plants as a target. Even in this case, even though the attack did not manage to get to cause harm to individuals, we have already witnessed a similar scenario. Indeed, the Slammer worm of 2003 corrupted the control system of the Davis-Basse nuclear power plant in Ohio[64]. It is true that these kind of attacks require more technical knowledge compared to the case in which it is simply needed to buy a bot-net in the dark web and that more levels of security need to be turned down to strike such an attack; however, the esteemed damage and the resulting fear are deemed to be enough of a "pay-off" for terrorist actors pondering whether or not to go cyber[65]. On top of that, as we will see in the section below, terrorist actors are not new to using the Internet to proselytise, creating the worrisome phenomenon of the so-called *foreign fighters*. That is why we cannot exclude that an individual with the technical capabilities to perpetrate the aforementioned acts might be reached out and convinced by terrorist proselytism. About these last points, Daniel Cohen affirmed that the idea of a terrorist organisation purchasing attack services offered by mercenary hackers is realistic in the near future. Therefore, the capabilities of cyberterrorists are destined to become better and such a threat cannot be ignored[66].

The conclusion of this section is rightfully the words of Barry Collin on this issue, who, years after coining the word cyberterrorism, stated that:

> "Like conventional terrorists, CyberTerrorists are out for blood. They try to do things like break into subway computer systems to cause a collision or use computers to tamper with power grids or food processing. However, unlike suicide bombers and roof-top snipers, CyberTerrorists attack from the comfort of home and can be in more than one place at a time through cyberspace .... CyberTerrorism can be far more damaging, and far more violent, than a 55-gallon drum of fuel and fertilizer. ... CyberTerrorists' isolation from the results of their actions and the consequent lack of personal risk, make them particularly dangerous.... [T]he ease and low cost of CyberTerrorism combine to offer an attractive tool for once-conventional sociopaths[67]".

[63] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[64] Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service.
[65] Ibid.
[66] Cohen, D. (2014) *Cyber terrorism: case studies*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 174.
[67] Iqbal, M. (2004) *Defining Cyberterrorism*, in The John Marshall Journal of Information Technology &

1.2 The cyberspace as a tool for cyberterrorism: cyberterror support

We will now examine the other way in which the cyberspace is exploited by terrorist actors, that is not by targeting the cyberspace, but rather seeking to exploit it in order to achieve a wide array of goals linked to the perpetration of terrorist attacks themselves. As it will be explained further in this chapter, there is still an ongoing debate on whether cyberterrorism should be defined in broad or narrow terms and thus, if the cases we are about to examine should be included or not in the definition of cyberterrorism[68]. Professor Kenney dealt with this issue and acknowledged the fact that these two contrasting perspectives still characterise the discussion on cyberterrorism. On the one hand, some argue that the concept of cyberterrorism 'itself is flawed and needs to be expanded to include terrorists' use of the Internet', including the of propaganda videos, the creation of websites aimed at recruiting and training , the exploitation of Internet to collect funds and so on[69]. On the other hand, other academics argue that illicit behaviours that are preparatory or of support to cyberterrorism, should not be regarded as such.

As we have explained in the previous section, Gordon and Ford affirm that pure cyberterrorism is that form of terrorism, which has the cyberspace as a target; but they admit a second category as well. Indeed, they stated that cyberterrorism is constituted of all acts of terrorism, which use "information systems or computer technology as either a *weapon* or a *target*"[70]. Like Gordon and Ford, other scholars agree with this conceptual organisation: distinguishing pure cyberterrorism from the rest of possible actions, but considering both elements.

An important contribution about this issue was given by Nelson *et al*, who better clarified what should be intended with those expressions referring to the cyberspace as a tool. Indeed, he clarifies that this category should be intended as 'cyberterror support', which is defined as "the unlawful use of information system by terrorists which is not intended, by itself, to have a coercive effect on a target audience. Cyberterror support

---

Privacy Law, Vol. 22, Issue 2 Journal of Computer & Information Law, p. 403, available at https://repository.jmls.edu/cgi/viewcontent.cgi?article=1091&context=jitpl.

[68] Conway, M. (2007) *Cyberterrorism: Hype and Reality*, in Armistead, Leigh, (ed.) Information warfare: separating hype from reality. Potomac Books, Inc., pp. 73-93.

[69] Kenney, M. (2015) *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, Vol. 59, Issue 1, p. 125, available at https://www.sciencedirect.com/science/article/pii/S0030438714000787.

[70] Conway, M. (2004) *Cyberterrorism: Academic Perspectives*, 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, p. 48.

augments or enhances other terrorist acts[71] ". With this clarification one thing immediately results to be clear: whether cyberterror support acts should be included in the definition of cyberterrorism or not remains undecided; however, the relevance of this issue is undeniable because they constitute a predicate offence for the perpetration of cyberterrorism itself.

We will now examine the way in which the cyberspace is used as a tool to allow the better achievement of terrorist goals and not as a target.

a. Dissemination of terrorist ideas

One of the first ways in which the cyberspace is exploited by terrorists to better achieve their goals is the communication with and, if possible, the influence on media. Leaflets and mouth-to-mouth propaganda have been replaced with well-structured websites, in which terrorist groups make their aims, their successful attack, their ideology, their history and so on public[72]. This allows them to reach a much wider audience in and extremely shorter time[73], producing the so-called *amplification effect*[74]. What worries the most about this aspect, is the fact that these websites enjoy thousands of visitors per month and that in some cases they are able to exploit the so-called c*ensorship resistance* systems[75]. These systems forbid a third party to remove or modify the content that was uploaded in the website, making extremely dangerous and detrimental materials available on the net, without the possibility to be removed[76].

b. Propaganda and threats

There is a further development of the previous point, which is the one that results in propaganda and threats. As we have already pointed out, carrying out these tasks online allows terrorist actors to reach an impressive number of users and allows them to do it

[71] Nelson B. *et al*, (1999) *Cyberterror: Prospects and Implications*, Centre for the Study of Terrorism and Irregular Warfare, Monterey, CA, p. 10, available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a393147.pdf.
[72] Weimann, G. (2004) *www.terror.net - How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report, available at https://www.usip.org/sites/default/files/sr116.pdf.
[73] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[74] Combs, C. C. (2018) *Terrorism in the Twenty-first Century*, Routledge, eighth edition.
[75] Denning, D. E. (2001) *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defence Research Institute RAND, pp. 289-288, available at https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf..
[76] Kauffman, J. (2019) *What Is Censorship Resistance, And Why Does It Matter?*, stable URL https://lbry.com/news/what-is-censorship-resistance-and-why-does-it-matter, last accessed 27 March 2020.

in few seconds. Related to propaganda, the Professor of International Security Maura Conway stated that the Internet result to be the best way for terrorists to propagandize their acts. As a matter of fact, the exploitation of this network allows them to 'disseminate their information undiluted by the media and untouched by government sensors[77]'.

In addition, rudimental means of propaganda and of spreading fear among societies have been replaced with refined techniques. For instance, we just need to think about the video that self-proclaimed Islamic State (IS) spread through its platform in 2015[78]. The video threatened Rome in particular, but Italy as a whole and Europe as well. It was realised with professional shots taken around Italy, Europe and about IS soldiers. One evidence of the clear intent to reach as many people as possible is that the language of these propaganda and intimidatory videos switched from being the mother-tongue one both for the spoken language and the subtitles to more recent videos with English subtitles, just like in the case at stake[79]. These footages are not spread solely by means of the official websites of terrorist organisation, on the contrary they proliferate in well-known video-sharing platforms like You Tube as well. On top of that, these videos often end up in traditional information mass media, leading to a further broadening of the audience for terrorist actors[80]. The end of these footages is twofold: it allows terrorist actors to display their capabilities both to governments and societies as a threat, and to the members or future ones of the terrorist organisation as a glorification of their acts[81].

c. Recruitment and training of new terrorists

A further way in which terrorist actors exploit the cyberspace for their purposes is constituted by recruitment and training. When it comes to recruiting, the cyberspace offers the possibility to reach individuals all around the world, considerably increasing

[77] Conway, M. (2002) *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet*, Trinity College Dublin, Ireland, First Monday, Vol. 7, No. 11, p. 3, available at http://doras.dcu.ie/498/1/first_mon_7_11_2002.pdf.
[78] To watch the video at stake https://www.ilgiornale.it/video/mondo/video-choc-dellisis-conquisteremo-roma-1081531.html , last accessed 27th March 2020.
[79] Combs, C. C. (2018) *Terrorism in the Twenty-first Century*, Routledge, eighth edition.
[80] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[81] Halopeau, B. (2014) *Terrorist use of the Internet*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by Akhagar, B., Staniforth, A., & Bosco, F., pp. 123-132.

the odds of initiating new individuals[82]. The exploitation of computer technology and the cyberspace allows this kind of operations to take place without the need of a physical contact and, most of all, it allows the initiates to strike from wherever they are. Therefore, mobilisation can take place at every time and everywhere[83]. Indeed, in the case of cyberterrorism and the exploitation of computer technology by terrorist actors there is no longer the need for the organisation to be physically close. This virtual closeness boosts the problematic phenomenon of the so-called lone wolves[84] and foreign fighters. In this case, the anonymity that can be guaranteed by the Internet sets the cyberspace in an unparalleled position compared to classical means of communication. Indeed, individual can easily get access to files like the *Terrorist's Handbook*, the *Anarchist Cookbook*, the *Mujahedeen Poison Handbook*, the *Encyclopaedia of Jihad*, the *Sabotage Handbook* and *How to Make a Bomb* through the net and there are several ways in which their anonymity can be guaranteed[85]. Terrorist groups rely more and more on the Internet to spread training materials aimed at recruiting new actors, for instance Al-Qaeda owns a an online library solely for training materials, where experts use chatrooms to answer the questions of the users[86].

d. Financing and cyber-money laundering

The last of the most relevant illicit ways in which terrorists exploit the cyberspace is related to financing and cyber-money laundering. When speaking of financing of terrorism, the activities that are being referred to are "the distinct activities of fund-raising, storing and concealing funds, using funds to sustain terrorist organizations and infrastructure, and transferring funds to support or carry out specific terrorist attacks[87]". The ways that are use by terrorist to finance themselves online range from activities that

[82] Cohen, D. (2014) *Cyber terrorism: case studies*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, pp. 165-174.
[83] Weimann, G. *www.terror.net* - *How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report, available at https://www.usip.org/sites/default/files/sr116.pdf.
[84] Halopeau, B. (2014) *Terrorist use of the Internet*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, pp. 123-132.
[85] There are several websites created with the aim to create fake digital identities for Internet users. Some of the list the instructions to get the process done, other sell their services and create a fake digital identity for whoever is willing to pay for it.
[86] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[87] United Nations, (October 2009) *Tackling the Financing of Terrorism*, CTITF Working group report, CTITF publication series, available at https://www.un.org/counterterrorism/ctitf/sites/www.un.org.counterterrorism.ctitf/files/ctitf_financing_eng_final.pdf.

are legal per se, such as the selling of merchandising or soliciting donations[88], to activities that are not legal, such as cyberfraud. In the former case, those activities that are not illicit *per se*, change their status once they are used in order to finance a crime, in this case terrorism[89]. The illicit ways in which money are obtained by terrorist actors range from the combination of identity theft and credit card fraud to access bank accounts to the use of fake company websites and emails to obtain personal information and money[90]. In addition to these new ways of collecting money for the purpose of the perpetration of terrorist acts, the effects of 'traditional' crimes, such as drogue trafficking and the taking of hostages[91], can be amplified by means of ICT. As a proof of that, we just need to compare the size of a hypothetical drogue trade relying solely on a physical network, to the one that can be reached by the same hypothetical trade that exploits the network offered by the cyberspace. Moreover, we need to stress once again the fact that cyberspace allows several possibilities that are not available in the physical world also in this field, due to the fact that virtual currencies[92] are not tangible like regular currencies and their location can easily be disguised. The features that allow their exploitation for the purpose of terrorist financing and money laundering are "anonymity, internet, and fragmentation". In other words, there is no identification required in order to use this kind of currency and, on top of that, internet and the cyberspace in general disregard territorial borders, leading to a difficulty in establishing

[88] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[89] De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova, Cedam, vol. 7.
[90] Bansted, G. (2012) *Hi terrorist financing and the Internet: dot com danger*, Information & Communications Technology Law, Vol. 21, Issue 3, pp. 237-256.
[91] *Supra, 85.*
[92] "Virtual currency is a digital representation5 of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)6 in any jurisdiction.7 It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status."
Financial Action Task Force (2014) *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, available at https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

jurisdiction. This situation in clearly a convenient one for terrorist actors, who have proven to be able to exploit it for their interests[93].

The convenient aspect of anonymity guaranteed by the cyberspace and its resources plays a pivotal role in the process of cyber-money laundering as well. On the light of that, the fundamental steps of money laundering, placement, layering and integration, become much easier and, most of all, much harder to trace[94]. Terrorists can carry out all the transaction that are needed to go through the stages of placement, layering and integration, without the need to be physically present and identifiable[95]. For this precise reason, not only terrorists can exploit the illicit activities that can be perpetrated by means of the cyberspace to earn money for their ends, but they also have the possibility to hide the illicit origin of those funds.

1.3 The cyberspace used for the ends of cyberterrorist actors

There is one last cluster which needs to be taken into consideration to have a comprehensive overview over cyberterrorism and it is what Nelson *et al* name the 'terrorist use of the Net'. These activities consist of the ways in which terrorist actors make use of the cyberspace in legal ways[96] to reach their goal. These actions are 'seemingly harmless[97]', but this does not imply that terrorist actors do not benefit from them. As a consequence, this aspect should not be neglected, despite the fact that most scholars agree that including the legal use of cyberspace by cyberterrorists would render the definition considerably too broad. By all means, we will examine the main ways in which the cyberspace is legally used by cyberterrorists due to the fact that these actions concur in the striking of the final attacks. It is important to keep in mind that the following scenarios are not hypothetical ones, quite on the contrary, the terrorist use of

[93] De Vido, S. (2019) *All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive*, in DPCE Online, vol. 38, pp. 59-76.
[94] G. Bansted*, Hi terrorist financing and the Internet: dot com danger*, Information & Communications Technology Law, Vol. 21, Issue 3, 2012, p. 244.
[95] Hunt, J. (2011) *The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them*, Information & Communications Technology Law, Vol. 20, No. 2, pp. 133-152.
[96] Nelson B. *et al*, (1999) *Cyberterror: Prospects and Implications*, Centre for the Study of Terrorism and Irregular Warfare, Monterey, CA, available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a393147.pdf.
[97] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

the cyberspace for these ends has been proven and is recognised as a threat by governments and experts of the relevant fields[98].

a. Personal communication

If on the one hand, dissemination of terrorist ideas and recruitment of new terrorists require visibility; on the other hand, interpersonal communication among the members of a terrorist organisation or among more terrorist organisations requires a high degree of secrecy. Also in this case, the cyberspace results to be a convenient option. Indeed, it is cheap and accessible almost everywhere; the communication is extremely fast and allows individuals spread all over the world to communicate despite their physical distance; there are several techniques that can guarantee anonymity of the user and hide the actual location of that user; finally encryption techniques allow to hide the real content of the conversation guaranteeing secrecy[99]. Secrecy plays a pivotal role in this cluster of cyberterrorism and that is due to the fact that this kind of use of the cyberspace by terrorist actors is linked to the organisational part, when a leak would imply the automatic fail of the attack. One of encryption techniques that is mainly used exploits steganography[100]: images containing secret messages are uploaded in regular photo sites, but only members of the organisations know that there is a secret message hidden in that photo. A further technique exploits free mailer email accounts in a way that successfully circumvents governmental control systems: two members log in the same email account communicating by means of draft. In this way, the message never becomes an email leaving that account and leaves no trace. These techniques are more

[98] Conway, M. (2002) *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet*, Trinity College Dublin, Ireland, First Monday, Vol. 7, No. 11.

[99] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

[100] An evidence of terrorist organisations exploiting this technique was described by Professors M. Bogdanoski and D. Petreski, who wrote: Evidence for the use of steganography by al-Qaeda terrorist organization is the arrest in Berlin in 2012 of a 22 year old Austrian who had just arrived from Pakistan. Later it was confirmed that he is a member of this terrorist organization. The digital storage and memory cards he tried to hide were password protected and the information were invisible. After the initial analysis it was found that inside memory cards was buried a pornographic video "Kick Ass" and a file named "Sexy Tanja". A few weeks later, after great efforts to combat a password and the software to make the file almost invisible, German researchers encoded in the video of a treasure trove of intelligence – over 100 documents including al-Qaeda firsthand about some of the plots of the terrorist group and a bolder road map for future operations for which there were not specified neither the date nor the location. Also various terrorist training manuals used by this organization were found. All these data were hidden using steganographic tools.
Bogdanoski, M., & Petreski, D. (2013) *CYBER TERRORISM– GLOBAL SECURITY THREAT*, International Scientific Defence, Security and Peace Journal, Vol. 13, Issue 24, pp. 59-73.

and more preferred to the classical encryption of texts contained in emails, due to the rising telecommunication surveillance[101].

All the customary text-based techniques that are available free of charge, such as emails, chatrooms, VoIP, mailing lists and so on, are available to terrorist users as well. A proof that terrorist groups are actually using these technologies emerged with the tragic events of 9/11. Indeed, it was found out the organisers of the attacks had simply used anonymous email services, such as Hotmail, to communicate among each other and plan such a disastrous attack[102].

The possibility to establish a stable contact net among members of the terrorist organisations all over the world, allows them to strike wherever they are and to operate on several levels pursuing multiple goals[103]. This issue, combined with the fact that the launching of a cyberterrorist attack does not require the terrorist to physically be in the place of the attack, creates a particularly worrisome scenario.

b. Planning and support operations

Compared to the classical organisational process of a hypothetical terrorist attack, the use of the cyberspace in the organisational aspect surely makes the process quicker and more efficient. Indeed, without the technologies operating in the cyberspace, a survey in the target place would be required to efficiently organise the attack, where to hide the weapons, the escape routes and all other possible aspects related to the terrorist act itself. However, this step can be avoided by means of the extremely detailed satellite maps that can be accesses by all Internet users. These satellite maps offer the unparalleled opportunity to have a street-view of the area, allowing terrorist actors to know exactly how the place where they want to strike looks like. It is for this precise reason that some security-relevant spots have been removed by these satellite maps on the specific request of governments. However, reports about security weaknesses and flaws still circulate around media, regardless of the fact that it has been esteemed that

[101] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[102] Conway, M. (2002) *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet*, Trinity College Dublin, Ireland, First Monday, Vol. 7, No. 11.
[103] *Supra, 97.*

these public sources constitute up to the 80% of the information that are needed by terrorist organisations to plan an attack[104].

1.4 An overview of vulnerabilities and possible targets

For the purposes of our analysis, we have already mentioned some of the possible targets of cyberterrorism due to the need to give some examples for the scenarios we have dealt with. However, we will now focus directly on the most plausible and crucial targets, on the basis of the aforementioned vulnerabilities. Even though the topic of the legal instruments concerning the issue of cyberterrorism will be dealt in the next chapter, it is important to anticipate that some of the following possible targets are included in the sectoral conventions about terrorism, though attacks perpetrated by means of the cyberspace are not explicitly included. As we have already clarified, the deadlock over a generally agreed definition of terrorism led to the choice to face this threatening issue in a pragmatic way, addressing the possible manifestations of terrorism[105].

One of the most realistic targets, which we have already analysed, is the economic and financial spheres relying on computer technology. As we have already explained, basically all the core components of the economy have strong links to the cyberspace and cybertechnology. As a result, these IT infrastructures related to our economy are in danger. Moreover, we have seen how such an attack would be included into the scopes of terrorist actors. Indeed, the aim to reach an economic change is included with their broad goals and, in addition, such an attack could cause a serious damage to property for a potentially wide number of individuals, economic activities and government[106].

When dealing with attacks affecting human lives we have already mentioned the possibility for cyberterrorists to target the transportation system. Nowadays an attack against an aircraft seems hardly possible due to the several stages of security[107] that have been instituted from 9/11 on. However, some experts claim that the 'insider threat' should not be underestimated. Indeed, individuals with the technical knowledge required to perpetrate this kind of acts are not excluded from the possibility of

[104] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[105] Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, pp. 139-192.
[106] Ibid.
[107] Giacomello, G. (2004) *Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism*, Studies in Conflict & Terrorism, Vol. 27, pp. 387-408.

radicalization[108]. An attack against other transportation means, such as trains, would be worryingly much more feasible[109]. As explained above, SCADA controlling systems can be accessed and manipulated in order to put other crucial systems out of order[110], such as the ones controlling the railway movements. Such a target would allow to reach one of the main goals of terrorist actors, which is causing physical harm to the victims, if not their death, and a high degree of fear among society.

The way in which SCADA systems can be exploited in the field of transportation is worth for another crucial aspect of our society: the supply network of basic resources, such as water, power energy, gas, fuel and so on[111]. We have already mentioned examples of power-down perpetrated by means of this kind of attack or the possibility to sabotage a water dam[112]. However, targeting the SCADA system controlling the core infrastructures of a society can result not only in the blocking of the supply of vital resources, but it can also result in the dispersion in the environment of harmful substances[113]. In our recent history we have already witnessed the aforementioned cyberattack launched to release raw sewage and damage the surrounding environment, however, more harmful substances could be released as well if cyberterrorists were to gain control of the related SCADA systems. For instance, some academics depict as a particularly worrisome threat the one including the release of nuclear scum[114]. An attack towards this kind of target could result into physical harm and death of individuals, harm to property and doubtlessly the spread of fear.

The health care system can be considered as a plausible target of cyberterrorism as well. Not only can the emergency system be hindered by hacking the communication system as part of a hybrid attack[115], but also the hospital unit itself can be targeted. Such an

---

[108] Halopeau, B. (2014) *Terrorist use of the Internet*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by Akhagar, B., Staniforth, A., & Bosco, F., pp. 123-132.
[109] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[110] Kenney, M. (2015) *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, Vol. 59, Issue 1, pp. 111-128.
[111] Cohen, D. (2014) *Cyber terrorism: case studies*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, pp. 165-174.
[112] Brenner, S. W. (2007) *"AT LIGHT SPEED": ATTRIBUTION AND RESPONSE TO CYBERCRIME/TERRORISM/WARFARE*, Journal of Criminal Law & Criminology 379, Northwestern University, School of Law.
[113] Giacomello, G. (2004) *Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism*, Studies in Conflict & Terrorism, Vol. 27, pp. 387-408.
[114] Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, pp. 139-192.
[115] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

attack, though not perpetrated by cyberterrorists, was witnessed in 2005; when the computers of the intensive care unit of the Seattle hospital were shut down and operating door rooms were put out of order by a bot-net[116]. Needless to say, that an attack targeting the health care system can result in physical harm or death of the victims and create fear, just like the previous ones.

A further target concerns probably one of the most relevant manifestations of technological development and the cyberspace becoming more and more physical and less cyber: the so-called 'modern' or 'smart living'. Domotics, a term deriving from the combination of the words 'domestic robots', also known with the expression 'smart house', is a core example of what is meant by smart living. In this case, security threats that might emerge are linked to the fact that domotics allows to remotely control several aspects of a house, from the use of the electronic devices inside it, to its temperature, lightening, air-conditioning and circulation, the locking of doors and windows and so on[117]. Needless to say that the wide number of possibilities offered by domotics, corresponds to a wide number of possible scenarios that might be put in place by cyberterrorists. Another pivotal example of a manifestation of smart living is self-driving cars[118]. Fully automatic vehicles are not available on the market yet, but prototypes are being tested by car companies like Tesla. As a matter of fact, they plan to finalise their products by the current year and as a consequence the next step in the field of technology seems to be approaching faster and faster. When it comes to self-driving cars, these vehicles are classified on the basis of their level of automation; ranking from 0, which corresponds to the absence of driving automation, to 5, corresponding to full driving automation. As preannounced, Tesla intends to make level 5 self-driving cars available this year, but level 4 vehicles, which are characterised by a considerable level of connectedness and interconnectedness, and as a consequence by a considerable level of vulnerability, are already sold by Ford[119]. A fully self-driving car, if hacked, would

[116] Brenner, S. W. (2007) *"AT LIGHT SPEED": ATTRIBUTION AND RESPONSE TO CYBERCRIME/TERRORISM/WARFARE*, Journal of Criminal Law & Criminology 379, Northwestern University, School of Law.
[117] Luiijf, E. (2014) *New and emerging threats of cyber crime and terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 19-28.
[118] Balough, C. D., &. Balough, R. C (2013) *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, Business Law Today, Business Law Section, available at https://www.balough.com/wp-content/uploads/2013/12/Cyberterrorism-on-Wheels_-Are-Today%e2%80%99s-Cars-Vulnerable-to-Attack_-_-Business-Law-Section.pdf.
[119] Vellinga, N. E. (2017) *From the testing to the deployment of self-driving cars: Legal challenges to policymakers on the road ahead*, Computer Law & Security Review 33, pp. 847-863.

offer cyberterrorists the possibility to have complete control of the vehicle and dispose of it as they please.

Military facilities should be included in the list of the ideal targets for cyberterrorists. However, there are several stages of security to be breached in order to actually carry out a successful attack against IT infrastructures linked to military facilities, just like in the case of aviation[120]. Nonetheless, as the CoE pointed out already in 2007, the military sector relies more and more on remote controlling in order to safeguard the lives of soldiers. Such a use of computer technology creates a condition of interconnectedness, which, as we have previously explained, implies a considerable degree of vulnerability. In addition, civilian technology is deployed in the military sphere as well, including the flaws in security that pertain the computer technology used in everyday life in a much more delicate field[121].

1.5 Cyberterrorism: a problematic definition

After providing an overview of the ways in which cyberterrorism is expected to concretise and manifest itself, we will now move on to the theoretical aspect related to this topic. As anticipated in the introduction of this chapter, despite the fact that cyberterrorism has been recognised as a concrete threat to society as whole by academics and international institutions, to date there is no widely accepted definition of it. Such a lacuna renders the criminalisation and prosecution of cyberterrorism an even more arduous task[122]. In addition, the lack of a definition of cyberterrorism can mainly be ascribed to the fact that the two constitutive elements of this term, *cyberspace* and *terrorism*, are debated terms themselves, of which a universally accepted definition is still missing as well.

In the light of this acknowledgement, we will now examine the controversies concerning the definition of cyberspace and terrorism, making reference both to the most prominent academic contributions on this topic and to international legal instruments. Finally, we will address the matter of the definition of cyberterrorism per se, providing an overview of the mainstream definition that have been outlined so far.

[120] Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, pp. 139-192.
[121] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[122] *Supra, 116.*

1.5.1 Defining *cyberspace*

The term *cyberspace* is the first element that constitutes the concept of cyberterrorism, together with the term *terrorism*. For this precise reason, taking into consideration the most prominent definitions provided by experts of the filed and the definitions that have been adopted by legal texts, is a basic step towards the definition of cyberterrorism itself. As a matter of fact, as Rain Ottis and Peeter Lorents from the Cooperative Cyber Defence Centre of Excellence highlighted, "a good definition for cyberspace" is needed in order not to have several "meaningless or flawed" derived terms[123], among which cyberterrorism is included.

As stated in the beginning of this section, there is no consensus definition of the term cyberspace and this is one of the difficulties currently hindering the outlining of a globally accepted definition for cyberterrorism. The birth of the term *cyberspace* is ascribed to William Gibson and it dates back to 1982, just a few years before Barry Collin coined and first defined the term cyberterrorism. Gibson however is no ITC expert nor an academic, indeed he is a Canadian science fiction writer[124]. Due to his field of expertise, the definition he gave of cyberspace[125] is unfit for the purposes of international law.

Moving on from 1982 to the recent years, we can observe how the prefix *–cyber* of which the term at stake is composed, is popularly related to the broad field of computers, virtual dimension, information and communication technology (ICT), the World Wide Web and so on[126]. Indeed, the contemporary point of view over the issue is that:

> "The word with prefix 'cyber-', or 'cyber', means an online activity. In other words, a modem or networking must be involved.' Besides being a prefix, it is also a verb, not a noun. It is an activity unique to the Information or Knowledge Age[127]."

[123] Lorents, P., & Ottis, R. (2011) *Cyberspace :Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, p. 1, available at https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf.
[124] Fenz, S. (2005) *Cyberspace Security: a Definition and a Description of Remaining Problems*, University Vienna - Institute of Government & European Studies.
[125] Christensson, P. (2006) *Cyberspace Definition*. Retrieved 2020, Mar 4, from https://techterms.com.
[126] Douglas, C. A. *et al.* (2019) *Towards Creating a New Research Tool: Operationally Defining Cybeterrorism*, Augusta University.
[127] Iqbal, M. (2004) *Defining Cyberterrorism*, in The John Marshall Journal of Information Technology & Kenney, M. (2015) *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, Vol. 59, Issue 1, pp. 111-128.

Nevertheless, this prefix' origins are related to the ancient Greek word κυβερνήτης (*kybernetes)*, which literally refers to *the actor who governs a process* [128]. This misinterpretation of the etymology of the term cyberspace, is reflected in the vagueness and inaccuracy of most popular definitions, such as the one that is given by the Cambridge Dictionary: "an electronic system that allows computer users around the world to communicate with each other or to access information for any purpose[129]."

However, academics and experts necessarily need to take a different approach and have therefore given several and different definitions for cyberspace.

A first example of academic definition of cyberspace was given by Barry Collin, the expert who coined the word cyberterrorism, who stated that this "virtual world" is "symbolic – true, false, binary, metaphoric representations of information- that place in which computer programs function and data moves[130]". It is evident how this definition is still too vague to be of use for international law. Moreover, many years have passed from this definition and as consequence it results to be out of date, due to the fact technology has considerably developed in the last years.

A more recent academic definition was outlined by Daniel T. Kuehl in 2009, who affirmed that the cyberspace is:

> "An operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and internetted information systems and their associated structures[131]."

This academic definition has an interesting feature: the fact that it includes the expression 'exploit information'. It is possible that the choice of such a wording was a reference to the inherent vulnerability of the cyberspace, which we have dealt with in the opening of the chapter. As a matter of fact, this kind of definition contemplates the

[128] Vassilys, F. (2004) *What is 'Cyberspace'?*, available at https://www.researchgate.net/publication/328928631_What_is_'cyberspace'#:~:text=is%20'cyberspace'%3F-,Vassilys%20Fourkas,use%20in%20Gibson's%20novel%20Neuromancer.
[129] Cambridge dictionary, *Cyberspace*, last accessed 26th February 2020, stable URL: https://dictionary.cambridge.org/it/dizionario/inglese/cyberspace.
[130] Collin, B. (1997) *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, Crime and Justice International, Vol.13, Issue 2, available at http://www.crime-research.org/library/Cyberter.htm.
[131] Kramer, F. D. (2009) *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in Franklin D. Kramer, S. Starr and L. K. Wentz, eds., *Cyberpower and National Security*, Washington DC: National Defence University, p. 4.

possibility that information can not only be created and shared, but used in a malicious way as well.

The next academic definition seems to build upon the aforementioned one, but it makes some relevant changes:

> "Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources.
>
> Cyberspace includes: a) physical infrastructures and telecommunications devices that allow for the connection of technological and communication system networks, understood in the broadest sense (SCADA devices, smartphones/tablets, computers, servers, etc.); b) computer systems (see point a) and the related (sometimes embedded) software that guarantee the domain's basic operational functioning and connectivity; c) networks between computer systems; d) networks of networks that connect computer systems (the distinction between networks and networks of networks is mainly organizational); e) the access nodes of users and intermediaries routing nodes; f) constituent data (or resident data)[132]".

Contrary to the previous definition, the aforementioned one admits the fact that the cyberspace is not static; quite on the contrary it is described as constantly changing. In addition, it examines in more depth the technical aspects of the issue, providing a detailed list of the elements that should be considered as an integral part of the cyberspace itself.

Despite the fact that there is a wide range of definitions that have been outlined so far and that they all differ among themselves in some way, most experts agree on the distinctive elements of cyberspace. As a matter of fact, nowadays there is a tendency to agree on the fact that a definition of cyberspace should include the following elements: the cyberspace as a worldwide network of hardware, software and data; human beings have the possibility to interface such network and when they do so, they become part of the cyberspace itself[133]. The last core point results to be crucial in our field of analysis. Indeed, human presence and its activities in the cyberspace cannot be neglected,

[132] Mayer, M., Martino, L., Mazurier, P., & Tzvetkova, G. (2014) *How would you define Cyberspace?*, Pisa, p.2, available at https://www.academia.edu/7097256/How_would_you_define_Cyberspace.
[133] Lorents, P., & Ottis, R. (2011) *Cyberspace :Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

considering the fact that they are not only mere users of a network. Quite on the contrary, if human beings had not realised this artificial space for their purposes, it would not even exist; and if human beings ceased to be active users of cyberspace, it would at least stall, if not completely stop[134].

This emphasis on the relevance of human action in this artificial and virtual space is no negligible detail, rather it plays a fundamental role in the study of cyberterrorism. That is why Rain Ottis and Peeter Lorents, two Cooperative Cyber Defence Centre of Excellence experts, proposed a new definition, which explicitly includes the presence of an active human presence in this space: "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems[135]". Evidently, we are not dealing with a technically detailed definition, like the one provided above, but the inclusion of the relevance of human action inside the cyberspace renders this definition noteworthy for the purposes of our analysis.

We will now move on to the definition that international institutions adopted for the drafting of their legal instruments. It is important to anticipate that there is no consensus definition of cyberspace among international institutions and they all differ from one another, despite having some elements in common. Furthermore, it can be noted how some of the distinctive elements of the aforementioned academic definitions have been included in the following legal definitions.

The United Nations define cyberspace as:

> "The technological substrate of modern societies made up of several interconnected layers—physical, syntactic, semantic, and pragmatic, with the physical and pragmatic layers subject to certain sovereign governmental jurisdiction and controls. Framed by the use of electronics and the electromagnetic spectrum, cyberspace enables "the creation, storage, modification, exchange and exploitation of information via interdependent and interconnected networks using information communication technologies[136]".

A particularly noteworthy aspect of this definition is that it includes one of the academic definitions that we analysed before, more precisely the one that contemplates the

[134] Ibid.
[135] Ibid.
[136] Kavanagh, C. (2017) *The United Nations*, *Cyberspace and International Peace and Security Responding to Complexity in the 21st Century*, UNIDIR Resources, p. 7, available at https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

malicious use of the cyberspace, envisaging the exploitation of the information that can be created, stored, modified and exchanged by means of it.

The European Commission decided to adopt a much more synthetic definition of cyberspace, which reads as follows: "the virtual space in which the electronic data of worldwide PCs circulate[137]". In this brief definition cyberspace is depicted as a 'virtual space', thus not a physical dimension, that extends worldwide. In this space, electronic data stored in physical computers all over the world enjoy free movement. Thus, the technological aspect is restricted to the movement of data among personal computers. Moreover there is no reference to the human component[138].

The European Union Agency for Cybersecurity (ENISA), just like the European Commission, provides us a brief definition of cyberspace, which is the following: "cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information[139]". In this case, the cyberspace is depicted as a net of 'tangible and intangible assets', through which electronic information can be either stored or transferred. A noteworthy element of this definition is the fact that time-dependence is highlighted. Acknowledging this feature implies acknowledging that the cyberspace cannot be conceived as a static space and that drastic changes can happen in extremely little time in such an environment[140]. Once again, we note how an element highlighted by an academic in his definition, is included in the outlining of a definition aimed at executing the purposes of international law.

This brief overview of both definitions that have given by experts and academics and ones that have been adopted in legal texts by international institutions, demonstrates how they can range from broad to narrow, how they can differentiate in some aspects, but also how some elements tend to be recurring ones. As a matter of fact, despite the differences in the number of definitions of cyberspace that can be found, some implications result to be evident: being the cyberspace a space that disregards physical

[137] Lorents, P., & Ottis, R. (2011) *Cyberspace :Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, p. 2.
[138] Ibid.
[139] Helmbrecht, U. (2017) *ENISA overview of cybersecurity and related terminology*, version 1, European Union Agency for Network and Information Security, p.6, available at https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.
[140] Lorents, P., & Ottis, R. (2011) *Cyberspace :Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, p. 3.

borders, aggressions by means of the cyberspace or in the cyberspace can be perpetrated anytime and anywhere. The viscosity of such space guarantees no involvement in physical confrontation and an easily obtainable anonymity. These core elements of the cyberspace, renders the task of international law to address cybercrime much more arduous and, as anticipated, renders the cyberspace a particularly attractive frontier for terrorist actors.

1.5.2 Defining *terrorism*

The second term, of which cyberterrorism is composed, is self-evidently the word *terrorism*. When it comes to this issue, we are once again facing the same problem we have just analysed while dealing with cyberspace. As a matter of fact, the term terrorism is just as difficult to define, if not more, as it is to define cyberspace. Doubtless, the most noteworthy evidence of this statement is the fact that a decades-long international debate about the definition of international terrorism has not led to a consensus definition of it yet[141]

If on one side terrorism has been condemned from both political and moral point of view for a considerably long time, one the other we see how only in the 1930s the need to define this issue in the legal context emerged. Since then there have been years of animated debate, not only in the field of international law, but also in fields like political science, security studies, psychology and so on. However, defining terrorism in the domain of international law results to be particularly problematic because it brings with itself a wide number of implications, which need to be taken into consideration[142]. Proof of such difficulties, is the fact that after almost a century no unifying definition for terrorism has been outlined. A good explanation for this complicated dynamic was given by Professor Ben Saul, who stated that:

> "The struggle to define terrorism also reflects genuine normative differences (ideological, philosophical, political, religious or moral) over when violence should be regarded as licit or illicit, justified or unjustified, or legitimate or illegitimate[143]."

[141] De Vido, S. (2017) *The future of the draft UN Convention on international terrorism*, Journal of Criminological Research Policy and Practice, Vol. 3, Issue 3, pp. 233-247, available at https://doi.org/10.1108/JCRPP-09-2016-0020.
[142] Hirsh-Hoefler, S., Pedahzur, A., & Weinberg, L (2004) *The Challenges of Conceptualizing Terrorism*, in Terrorism and Political Violence, Vol. 16, No. 4.
[143] Saul, B. (2015) *Defining Terrorism: a Conceptual Minefield*, Sydney Law School, Legal Studies Research Paper, No. 15/84, p. 1.

In saying so, Professor Saul is referring to the conceptual impasse created by the difficulties in drawing a line between terrorism and other forms of violence, such as guerrilla warfare, national liberation violence or self-determination movements[144]. Richard Garnett and Paul Clarke reiterated this point in stating that:

> "One reason why it has been difficult to secure a universally accepted definition of terrorism has been that some States, primarily from the developing world, have sought to resist condemnation of practices and activities which they may have resorted to in their acquiring of independence, particularly during colonization. Moreover, terrorism has been described as having uniquely "political" and "socio-psychological" aspects which make it difficult to regulate with universal and coherent laws[145]".

This contentious issue has been the *leitmotiv* for most of the years in which the definition of terrorism has been debated, leading more and more States to believe that this issue had to be dealt in the field of national prosecution, instead of the international one. As a matter of fact, from the 1960s on, the cases of terrorism started to multiply and a considerable number of these acts were perpetrated by liberation movements struggling against colonial powers[146].

However, the aforementioned rise in terrorist attacks led the international community to face the deadlock in the debate about a universally accepted definition of terrorism in an indirect way; that is by adopting "sectoral treaties". These covenants dealt with specific terrorist acts and not with terrorism as a unitary threat to civil society. Most of the times, treaties reacted to a specific terrorist attack, criminalising the illicit acts that had been deployed to carry out the attack[147]. For this precise reason, from 1963 on, we have witnessed the enactment of 19 international legal instruments aimed at preventing a series of terrorist acts[148]. These international legal instruments constitute a legal framework[149] tackle instances regarding civilian aviation, protection of international

[144] Hirsh-Hoefler, S., Pedahzur, A., & Weinberg, L (2004) *The Challenges of Conceptualizing Terrorism*, in Terrorism and Political Violence, Vol. 16, No. 4.
[145] Clarke, P., & Garnett, R. (2005) *Cyberterrorism : A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, p. 466.
[146] Saul, B. (2015) *Defining Terrorism: a Conceptual Minefield*, Sydney Law School, Legal Studies Research Paper, No. 15/84.
[147] De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova, Cedam, vol. 7, pp. 2-10.
[148] Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, pp. 139-192.
[149] De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova, Cedam, vol. 7, pp. 2-10.

staff, taking of hostages, nuclear material, maritime navigation, explosive materials, terrorist bombing, financing of terrorism and nuclear terrorism[150].

This pragmatic approach allowed the international community to momentarily overcome the deadlock of terrorism definition that was caused by several reasons, among which the disagreement on the legitimacy of the use of violence by liberation movements was included. This strategy led to the development of a legal framework pragmatically aimed at addressing the several manifestations of terrorism, despite lacking of a definition of the phenomenon per se. However, being these international legal instruments *ad hoc* instruments, they left the core issue unsolved. Indeed, in none of the 19 aforementioned legal instruments a general crime for terrorism is established. Nonetheless, it is custom in treaty-making for international legal instruments to determine the obligation for contracting parties to criminalise the illicit conduct at stake, to establish extraterritorial jurisdiction and to respect the *aut dedere aut judicare* principle, referring to the obligation to either adjudicate or extradite the perpetrator of the crime[151]. However, it needs to be highlighted that another reason why it is generally avoided to give a definition in these treaties is the willingness not to hinder ratification by contracting parties, in such a way to achieve the largest number of ratifications possible and at least an indirect criminalisation of terrorism. Still, this strategy does not enjoy absolute approval in the international community. As a matter of fact, some argue that this approach led States to "define terrorism to suit their own political purposes or to camouflage assaults on fundamental civil and political rights[152]".

After acknowledging the lack of a globally accepted definition of terrorism and the main controversies characterising an issue that is certainly too wide to be exhaustively examined in a paragraph of this dissertation, we will now provide an overview on the most prominent definitions of terrorism that have been outlined in the academic field so far.

The first academic definition we chose to analyse dates back to 1988 and was outlined by Alex P. Schmid, researcher of the International Research Centre for Counter-Terrorism - The Hague (ICCT) and director of the Terrorism Research Initiative (TRI)

[150] See https://www.un.org/sc/ctc/resources/international-legal-instruments/ to access the list and full text of the aforementioned international legal texts. Last accessed 9 March 2020.
[151] Saul, B. (2015) *Defining Terrorism: a Conceptual Minefield*, Sydney Law School, Legal Studies Research Paper, No. 15/84.
[152] Ibid, p. 9.

and Albert Jongman. Their definition results to be of particular interest due to the methodology that they applied to reach their conclusion. As a matter of fact, Schmid based his work on 109 definitions by other scholars and identified 22 "definitional elements[153]", which were recurring in most of those definitions. Subsequently, these criteria were ranked on descending order, from the element that appeared with the highest frequency, to the one that appeared the least among the 109 academic definitions. Finally, Schmid and Jongman elaborated a comprehensive definition on the basis of their study and outlined their own definition, which contains 16 out of the 22 "definitional elements"[154]. The definition reads as follows:

> "Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group, or state actors, for idiosyncratic, criminal, or political reasons, whereby—in contrast to assassination—the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat—and violence—based communication processes between terrorist (organization), (imperiled) victims, and main target (audiences(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought[155]".

It is important to notice that this definition assumes that the goal that terrorist aim at achieving by means of their acts is not violence per se, but rather the coercive power that committing this kind of violent acts can confer to them.

Some years later, precisely in 2011, he updated his definition as following:

> "Terrorism refers, on the one hand, to a doctrine about the presumed effectiveness of a special form or tactic of fear generating, coercive political violence and, on the other hand, to a conspiratorial practice of calculated, demonstrative, direct violent action

[153] The definitional elements listed in Schmid and Jongman's order are: Violence; Political; Fear, terror; Threat; Psychological effects; Victim-target differentiation; Purposive and planned; Method of combat/strategy;
Extranormality, in breach of accepted rules; Coercion/extortion; Publicity; Arbitrariness; Civilians, non-combatants; Intimidation; Innocence of victims; Group/movements; Symbolism; Unpredictability; Covert; Repetitiveness; Criminal; Third party demands.
List available in Hirsh-Hoefler, S., Pedahzur, A., & Weinberg, L (2004) *The Challenges of Conceptualizing Terrorism*, in Terrorism and Political Violence, Vol. 16, No. 4, p. 781.
[154] Hirsh-Hoefler, S., Pedahzur, A., & Weinberg, L (2004) *The Challenges of Conceptualizing Terrorism*, in Terrorism and Political Violence, Vol. 16, No. 4, pp. 777-794.
[155] Jongman, A., Schmid, A. *et al* (1988) *Political Terrorism: A New Guide To Actors, Authors, Concepts, Data Bases, Theories, And Literature*, Transactions Publishers, p. 28.

> without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties[156]".

In the updated version on this definition we can note that the core element highlighted above is maintained, but there is an important addition to it. As a matter of fact, it is made clear that for a criminal act to be a terrorist one, targeted individuals need to be "civilians and non-combatants"[157], thus excluding acts of violence against individuals involved in an armed conflict.

The political analyst Bruce Hoffman described this phenomenon as:

> "[...] terrorism is violence, or the threat of violence, calculated to create an atmosphere of fear and alarm. These acts are designed to coerce others into taking actions they would otherwise not undertake or to refrain from taking actions that they desire to take. All terrorist acts are crimes. Many would also be violations of the rules of war, if a state of war existed. This violence or threat of violence is generally directed against civilian targets. The motives of all terrorists are political, and terrorist actions are generally carried out in a way that will achieve maximum publicity. The perpetrators are members of an organized group, and, unlike other criminals, they often claim credit for their acts. Finally, terrorist acts are intended to produce effects beyond the immediate physical damage they cause by having long-term psychological repercussions on a particular target audience [..][158]".

This definition is in line with the previous statement about the aims of terrorism being broader than violence per se, being it intended to exploit the sense of fear that the use of or the threat to violence generates in the society. The need for the target to be civilian population is maintained as well. However, a new element is added: the fact that terrorist actors, unlike other criminal, tend to "claim credit for their acts[159]".

The Global Terrorism Database (GTD), provided in 2017 the following definition:

---

[156] Douglas, C. A., Griffith, C.,. Murray, G. R, Heslen, J. J., Davies, K. L., Hunter, Y., Jilani-Hyler, N., & Ratan, S. (2019) *Towards Creating a New Research Tool: Operationally Defining Cybeterrorism*, Augusta University, p. 10.
[157] Ibid.
[158] Hoffman, B., & Riley, K. J. (1995) *Domestic Terrorism: A National Assessment of State and Local Preparedness*, supported by the National Institute of Justice, US Department of Justice, RAND, p. 3, available at https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR505.pdf.
[159] Ibid.

> "The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation including two of the following three criteria: (1) The act must be aimed at attaining a political, economic, religious, or social goal; (2) There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims; and (3) The action must be outside the context of legitimate warfare activities[160]".

Also in this case the two core elements of the willingness to exploit the coercive power arising from the spread of fear and the intention to strike against civilian population are included in the definition of terrorism. In addition to these two elements, it is specified that the coercive power needs to be used in order to achieve a a political, economic, religious or social change.

It shall be noted that despite the small differences that characterise these examples of academic definitions, there are certain recurring elements: the illicit use of violence or the threat to use violence in an illicit way; the intent to generate fear among the population and the aim to achieve a social or a political change. When shifting the focus to the definitions of terrorism that have been adopted in international legal instruments, it can be noted that the aforementioned recurring elements are maintained in the following definitions. Thus, it can be claimed that despite the lack of a globally accepted definition, there is at least a convergence of opinions in between international institutions and academics studying the issue on the core aspects of it. We will now take into consideration the most relevant examples provided in legal texts by international institutions:

In 1995, the United Nations General Assembly stated that:

> "Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them[161]".

This statement, despite not being an explicit definition, but rather a conviction of an illicit behaviour, is noteworthy because it makes explicit which intent should be

[160] START (2019) *Global Terrorism Database. Codebook: inclusion criteria and variables*, p. 11, available at https://www.start.umd.edu/gtd/downloads/Codebook.pdf.
[161] UN General Assembly (17 February 1995) *A/RES/49/60 Measures to Eliminate International Terrorism*, forty-ninth session, agenda item 142, p. 4, available at https://undocs.org/en/A/RES/49/60.

underlying an act, in order to consider it as terrorist. Thus, this statement better explains one of the recurring elements that we have just labelled as recurring among academic definition. In other words, the *actues reus*, meaning the illicit act, per se is not enough to trigger the definition of terrorism. Indeed, it needs to be combined with the *mens rea*, which means the intention underlying the act itself, to "provoke a state of terror"[162]. For this precise reason, for one of the acts mentioned inside the aforementioned international legal framework, just like for any other possible manifestation of terrorism that is not included in it, to be classified as a terrorist act, the *mens rea* needs to be the intent to intimidate civil population[163], spreading a sense of fear and terror.

Contrary to the previous Resolution, the International Convention for the Suppression of the Financing of Terrorism of 1999 provides us with a definition of terrorism, which reads as follows:

> "Any 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[164]."

This definition confirms the need for the *mens rea* to be the spread of terrors among civil population, but adds as underlying indentation the willingness to cause death or serious harm to individuals. Most important, article 2 of the Convention clarifies that, for an act to be classified as terrorism, the targeted individuals must not be involved in "in the hostilities in a situation of armed conflict"[165]; in other words the victims need to be civilians.

The next definition provided by Article 2 of the United Nations *Draft comprehensive convention on international terrorism* definition of 2000[166] and it reads as follows:

---

[162] Ibid.
[163] De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova, Cedam, vol. 7, pp. 2-10.
[164] UN General Assembly (December 1999) *International Convention for the Suppression of the Financing of Terrorism*, in resolution 54/109, art. 2.1(b), available at https://www.un.org/law/cod/finterr.htm.
[165] Ibid.
[166] The effort to draft a Comprehensive Convention on International Terrorism started in 1996 in the framework of the United Nations. To date no agreement on this legal instrument and on a globally accepted definition of terrorism has been achieved, despite the fact that most of the international community recognises the benefits that an internationally agreed framework would imply in the fight against terrorism. One of the main obstacles are once again the different approaches to peoples' right to self-determination. For instance, in November 2014 the Organisation of Islamic Cooperation requested to

> "1. Any person commits an offence within the meaning of this Convention if that person, by any means, unlawfully and intentionally, does an act intended to cause: (a) Death or serious bodily injury to any person; or (b) Serious damage to a State or government facility, a public transportation system, communication system or infrastructure facility with the intent to cause extensive destruction of such a place, facility or system, or where such destruction results or is likely to result in major economic loss; 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 abstain from doing any act. (2). Any person also commits an offence if that person attempts to commit an offence or participates as an accomplice in an offence as set forth in paragraph 1. (3). Any person also commits an offence if that person: (a) Organizes, directs or instigates others to commit an offence as set forth in paragraph 1 or 2; or (b) Aids, abets, facilitates or counsels the commission of such an offence; or (c) In any other way contributes to the commission of one or more offences referred to in paragraphs 1, 2 or 3 (a) by a group of persons acting with a common purpose; such contribution shall be intentional and either be made with the aim of furthering the general criminal activity or purpose of the group or be made in the knowledge of the intention of the group to commit the offence or offences concerned[167]".

Despite still being part of a Draft Convention and not of a convention that entered into force, this definition is particularly noteworthy because it is considered to be "consolidated"[168]. On top of that, it is true that the deadlock in the drafting process was caused, among other reasons, by the disagreements on one of the recitals of the preamble and Article 3[169] of the draft[170]; on the other hand, it is also true that High

---

differentiate terrorist acts and 'the legitimate struggle of peoples under foreign occupation and colonial or alien domination in the exercise of their right to self-determination in accordance with the principles of international law'.

[167] UN General Assembly (2000) *Draft comprehensive convention on international terrorism*, fifty-fifth session, agenda item 166, p.3, available at https://digitallibrary.un.org/record/422477#record-files-collapse-header.

[168] De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova: Cedam, vol. 7, pp. 2-10.

[169] "2. The activities of armed forces during an armed conflict, as those terms are understood under international humanitarian law, which are governed by that law, are not governed by the present Convention. 3. The activities undertaken by the military forces of a State in the exercise of their official duties, inasmuch as they are governed by other rules of international law, are not governed by the present Convention. 4. Nothing in the present article condones or makes lawful otherwise unlawful acts, nor precludes prosecution under other laws; acts which would amount to an offence as defined in article 2 of the present Convention remain punishable under such laws. 5. The present Convention is without prejudice to the rules of international law applicable in armed conflict, in particular those rules applicable to acts lawful under international humanitarian law."
United Nations (2013) *Report of the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996*, art. 3 [18], p. 16, available at https://undocs.org/A/68/37.

Contracting Parties have the possibility to ratify a treaty with reservations [171]. Furthermore, this definition establishes that the intention underlying the act needs to be to cause death or serious harm of individual or serious damage of State's infrastructures resulting into a considerable economic harm. These acts shall be characterised by the aim to spread fear among population or to compel a government to act in a specific way.

As confirm to the fact that the definition we have just analysed is deemed to be consolidated, we can note how, in the following statement of the United Nations Security Council Resolution S/RES/1566 of 2004, most of the aforementioned categories are included:

> "[..]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, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature [..][172]".

Moving on to the European Union, the Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism[173] of 2001 states that:

> "Terrorist offences are defined as acts committed with the aim of 'seriously intimidating a population', 'unduly compelling a government or international organisation to perform or abstain from performing any act', or 'seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation'[174]".

---

[170] De Vido, S. (2017) *The future of the draft UN Convention on international terrorism*, Journal of Criminological Research Policy and Practice, Vol. 3, Issue 3, pp. 233-247, available at https://doi.org/10.1108/JCRPP-09-2016-0020.
[171] See Cassese, A. (2013) *Diritto internazionale*, Bologna: Il Mulino.
[172] UN Security Council (2004) *Resolution S/RES/1566*, p.2, available at https://www.un.org/ruleoflaw/files/n0454282.pdf.
[173] Council of the European Union (2001) *Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism*, Official Journal of the European Communities, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0093:0096:EN:PDF.
[174] European Parliament (2015) *Understanding definitions of terrorism*, Briefing European Parliamentary Research Service, p.2, available at https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS_ATA(2015)571320_EN.pdf.

Also this definition includes most of the categories included in the definition provided by the Draft Comprehensive Convention on International Terrorism, such as: the intent to spread fear among society, the willingness to coerce a government to behave in a specific way and the aim to bring havoc in the "political, constitutional, economic or social" order, whether it is national or international[175].

Article 1 of the Council Framework Decision 2002/475/JHA on combating terrorism[176] of 2002 harmonises the different definitions of terrorism at the European level and defines terrorist acts as:

> "Offences under national law, which, given their nature and context, may seriously damage a country or an international organization where committed with the aim of: (1) seriously intimidating a population, or (2) unduly compelling a Government or international organization to perform or abstain from performing any act, or (3) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or international organization[177]".

This definition mirrors the previous one and as a consequence includes the categories that emerged from the definition by the Draft Comprehensive Convention on International Terrorism.

To conclude, we can state that despite the lack of a universally recognised definition of terrorism, academic definitions just like the ones adopted in legal texts highlight the same elements of a constitutive value when it comes to defining terrorist acts. In addition, the new wave of terrorism that characterised the last years starting with the tragic attacks of 2015 and 2016 proved that the current debate on terrorism is characterised by a higher degree of agreements among States. As a matter of fact, as emerged from the discussion at UN level, there seems to be a tendency to indubitably label at terrorists some entities, like Al-Quaida and Da'esh; for their praxis has

---

[175] Ibid.

[176] Council of the European Union (2002) *Council Framework Decision 2002/475/JHA on combating terrorism*, Official Journal of the European Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN.

[177] Casale, D. (2008) *EU Institutional and Legal Counter-Terrorism framework*, Defence against Terrorism Review, Vol. 1, No. 1, p. 62, available at https://www.tmmm.tsk.tr/publication/datr/volume1/04-EU_Institutional_and_Legal_Counter-terrorism_Framework.pdf.
This decision was mentioned for the purpose of this chapter, however it is no longer in force. See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=en for the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

consolidated as a conduct that shall be regarded as terrorism. On the light of this acknowledgement, it can be claimed that it is reasonable to believe that the deadlock on the matter of the definition of terrorism could finally be heading towards a solution.

1.5.3 The birth of the concept of *cyberterrorism* and the road to its definition

After analysing the issue of the still debated definitions of the two constitutive elements of cyberterrorism, namely cyberspace and terrorism, we will now take into consideration the derived term; both taking into account how it was born as a concept and the direction that the road to its definition has followed and is currently following.

The idea of cyberterrorism was first publicly assumed in 1977 by Robert Kupper, who at that time was the Chief Scientist of the US Arms Control and Disarmament Agency. On this issue he declared:

> "Commercial aircraft, natural gas pipelines, the electric power grid, offshore oil rigs, and computers storing government and corporate records are examples of sabotage-prone targets whose destruction would have derivative effects of far higher intensity than their primary losses would suggest. Thirty years ago terrorists could not have obtained extraordinary leverage. Today, however, the foci of communications, production and distribution are relatively small in number and highly vulnerable[178]".

This statement lets us understand how, even though technology was not as advanced as it is nowadays yet, it was already a source of concern. More precisely, the concern arose from the inherent vulnerability of such technology and from the fact that it has a link to the physical world; allowing the harm caused on the cyberspace to have severe consequences of the tangible one.

On the other hand, after this statement a further step was taken and as anticipated at the end of paragraph 1.1, the actual term *cyberterrorism* was first introduced by the California's Institute for Security and Intelligence researcher Barry Collin in mid-1980s[179], in order to refer to all those security threats caused by illicit actions perpetrated by means of networked computers. At that time, Collin's definition for

[178] Conway, M. (2004) *Cyberterrorism: Academic Perspectives*, 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, p. 42.
[179] Purdy, E. R. (2019) *Cyberterrorism*, Salem Press Encyclopedia.

cyber terror was "the convergence of cybernetics and terrorism"[180], a rather synthetic and not exhaustive one.

Despite this lack of exhaustiveness, this first definition of cyberterrorism spurred an animated debate among experts, resulting in the development of two different approaches to this subject. The first school of thought in this field makes reference to Dorothy Denning, a renowned Professor of computer science and information security expert. Professor Denning claimed that cyberterrorism should not be defined in broad terms, quite on the contrary, she defined it as "illegal and highly damaging attacks that target computers, networks, and digitally stored information for the purpose of causing harm to people or property or generating fear[181]". An expert who shares Professor Denning's approach to defining cyberterrorism in narrow terms is Mark. M. Pollitt. He affirmed that a definition for such an issue needs to be "[..] necessarily narrow. For cyberterrorism to have any meaning, we must be able to differentiate it from other kinds of computer abuse [..][182]". Indeed, those academics and experts who share this point of view, do so because they affirm that a too broad definition of cyberterrorism would cause an overlap of the issue at stake with other ones, such as *hacktivism* and *cracking*. In 2015 Professor Michael Kenney reiterated this crucial point and stated that cyberterrorism belongs to the same 'genus' of other cyberattacks, such as cyber-war or hacktivism; still, despite sharing the same 'genus' it is characterised by 'essential differences'[183].

Even though there is no unifying definition for the aforementioned terms either, the former, which is the combination of the terms 'hacking' and 'activism', is commonly referred to as:

> "Intentional access to systems, websites, and/or data without authorization or having exceeded authorized access, and/or the intentional interference with the functioning

[180] Luiijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 11.
[181] Purdy, E. R. (2019) *Cyberterrorism*, Salem Press Encyclopedia.
[182] Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, pp. 8-10.
[183] Kenney, M. (2015) *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, Vol. 59, Issue 1, p. 112.

> and/or accessibility of systems, websites, and data without authorization or having exceeded authorized access, in order to effect social or political change[184]".

Therefore, we can infer that cyberterrorism and hacktivism might share some features, such as the means through which these crimes are perpetrated on the cyberspace or the intent to reach a social or political change. However, hacktivism lacks of the core elements that are needed to classify a phenomenon as terrorism, such as the explicit intent to instil fear and the use or threat to use violence to reach its goals[185]. Indeed, the underlying intention of hacktivists is a political one aimed at drawing the attention needed to reach the desired change and therefore there is no intent per se to cause severe harm to people or their property or to spread fear among civilian population.

Cracking differs from cyberterrorism as well, as it consists on the act of hacking with criminal intents, mainly in order to alter data or to have an economic gain. As a consequence we can make the same argumentation we made while comparing cyberterrorism and hacktivism, underlining the fact that the underlying intent is crucially different. Indeed, one of the definitions that are currently used for cracking is:

> "Gaining unauthorized access to computer systems to commit a crime, such as digging into the code to make a copy-protected program run and flooding Internet sites, thus denying service to legitimate users. During a cracking exploit, important information can be erased or corrupted. Websites can be deliberately defaced. Unauthorized access is typically done by decrypting a password or bypassing a copy-protection scheme[186]".

On the other hand, the second school of thought on cyberterrorism, which is composed by actors like governmental and military officials, believes that a broader definition than Professor Denning's one is needed in order to properly deal with cyberterrorism. As a consequence, these experts are not concerned with the possibility that a wider definition might cause the overlapping of different categories and they believe that this is the most effective way to tackle the issue of cyberterrorism. That is why they classify as cyberterrorism "virtually any cyberattack that threatens computers and networks[187]".

---

[184] UN Office on Drugs and Crimes (2019) *Hacktivism*, stable URL: https://www.unodc.org/dohadeclaration/index.html, last accessed 20 July 2020.
[185] Office of the United Nations High Commissioner for Human Rights, (2008) *Human Rights, Terrorism and Counter-terrorism*, Geneva, pp. 3-7, available at https://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf.
[186] Martin, C., & Schell, B. (2006) *Websters' New World Hackers Dictionary*, Wiley Publishing Inc., p. 73.
[187] Purdy, E. R. (2019) Cyberterrorism, Salem Press Encyclopedia., p. 2.

The advent of the new decade added a new problematic element to the situation shaped by Collin's definition of cyberterrorism. Indeed, the 1990s were the years during which the development of personal computing allowed individuals to access to World Wide Web from all over the world[188]. The developments in this field had such an impact on our society, that it was perceived as a "cyber revolution, the next wave after the industrial revolution[189]". These technological achievements made a huge number of new possibilities available to individuals all over the world, but at the same time it created a new crime frontier[190], offering a new transnational arena and new tools to any kind of malicious actor[191], including terrorist ones[192]. This idea was reiterated in 2007 by the Council of Europe, which underlined the fact that all actors enjoy the right to access when it comes to information and communication technology (ICT), whether it is a regular citizen with no malicious intention or a terrorist organisation aiming at exploiting this resource for their purposes. Moreover, they make that case that criminal acts perpetrated with the help of computing systems have occurred since the advent of ICT itself. On top of that, information on how to exploit computer networks are spread all over the web and are easily accessible by all users. That is why it is neither unrealistic nor unreal to expect that terrorists will exploit this new crime frontier[193].

The concerns that had started to rise in the '90s about the terrorist use of the cyberspace, did not quiet down by the beginning of the new century. Quite on the contrary, the turmoil continued due to the widening spectre of possibilities offered by cybertechnology, but also to the dramatic events of the 9/11 which shaped a new way of conceiving national and international security[194]. As a consequence, the topic of cyberterrorism was no longer just a debated subject, but it became an element of interest and research for experts from different fields. Press started to pay growing attention to

[188] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, pp. 57-118.
[189] Luiijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 11.
[190] Hunt, J. (2011) *The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them*, Information & Communications Technology Law, Vol. 20, No. 2, pp. 133-152.
[191] *Supra*, 184.
[192] Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, pp. 8-10.
[193] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[194] Weimann, G. *www.terror.net* - *How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report, available at https://www.usip.org/sites/default/files/sr116.pdf.

this potential threat, actually causing further difficulties in agreeing on a common definition by creating an imprecise and misleading image of the issue[195]. Furthermore, more and more governments started including the study of cyberterrorism to their national security agenda[196] and soon it became clear to many that, as Lieutenant General Keith Alexander states, cyberspace is the new national security frontier[197].

Moreover, international institutions started expressing their concerns about cyberterrorism as well, some in explicit ways, others in indirect way. The first international organisation to tackle this issue was the United Nations, when on 16th January 1997, with the General Assembly Resolution 51/210 it was recognised the need:

> "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[198]".

The European Union expressed its concerns on the matter in the 19th September 2001 Commission's Explanatory Memorandum of the proposal for a Council Framework Decision on combating terrorism, with which it recognised the rise of 'new forms of terrorism'. On top of that, instances of international tensions culminating in attacks against ICT are acknowledged in this text, just like the risk to witness in the near future more harmful attacks, destined to lead to the loss of human lives. Furthermore, it was pointed out that "the profound changes in the nature of terrorist offences highlight the inadequacy of traditional forms of judicial and police cooperation in combating it", forcing policymakers to address the lacunae that characterise the existing international legal framework[199]." Finally, the Council of Europe's Committee of Experts on

[195] Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, pp. 8-10.
[196] Purdy, E. R. (2019) Cyberterrorism, Salem Press Encyclopedia.
[197] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, p. 76.
[198] UN General Assembly (1997) *Measures to eliminate international terrorism: resolution / adopted by the General Assembly A/RES/51/210*, 51st Session, available at https://www.refworld.org/docid/49997ae127.html.
[199] European Union (2001) *Proposal for a Council framework Decision on combating terrorism*, Official Journal 332 E, p.1, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52001PC0521:EN:HTML.

Terrorism (CODEXTER[200]) realised a whole report on the issue of cyberterrorism[201], which will be the guideline for the second chapter of this dissertation.

However, despite the concerns that such threat was and is still causing to governments, international institutions, experts and civil society, at the moment there is no consensus definition of cyberterrorism[202] yet. Experts and scholars call for a definition of cyberterrorism, not only for their research studies, but because it is deemed to be fundamental in the drafting process of an international legal framework[203]. This point results to be crucial, because the elaboration of a universally recognised definition of cyberterrorism, does not only serve merely descriptive purposes, but on the contrary:

> "[...] a common definition is required for two reasons: firstly, to definitively determine the status of customary law pertaining to the use of force in relation to acts of terror; and secondly, to criminalize such acts, i.e. to prevent terrorism, to condemn it, and to punish it. Worth noting is also that international demand to extradite a terrorist offender far exceeds pressure to extradite a common criminal[204]".

Therefore, it is evident how defining the object at stake is fundamental not just to know how to label a phenomenon, but most of all to know how to prevent it, criminalise it and punish the perpetrators of it.

The complexity of the reasons underlying the lack of a unifying definition cannot be exhaustively depicted in this dissertation, however two main reasons emerge among those factors that render this task arduous to solve.

First of all, cyberterrorism can be referred to as a new form of terrorism and therefore it inherits from it the aims and goals. As a matter of fact, cyberterrorism just like traditional terrorism, acts upon and exploits the human feeling of fear; thus, implying

---

[200] From 2018, with the expiry of the mandate of CODEXTER, the committee changed its name into Council of Europe Committee on Counter-Terrorism (CDCT). The three funding principles of the new mandate are prevention, prosecution and protection.
For further information on the updated mandate of the CDCT see Council of Europe, *Council of Europe Committee on Counter-Terrorism*, stable URL https://www.coe.int/en/web/counter-terrorism/cdct.
[201] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[202] Brickey, J. (August 2012) *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, CTC Sentinel, Vol. 5, Issue 8, available at https://www.researchgate.net/publication/235782714_Defining_Cyberterrorism_Capturing_a_Broad_Range_of_Activities_in_Cyberspace.
[203] Chen, T., Jarvis, L., & McDonald, S. (2014) *Cyberterrorism- Understanding, Assessment and Response*, New York: Springer.
[204] Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1,p. 142.

that the extent to which it is actually perceived as a threat varies from actor to actor. These contrasting perceptions lead to a situation in which there is even no agreement on the actual imminence of this threat or on the severity of the damages that it might caused by it. On the light of this, it can be claimed that the ongoing debate on cyberterrorism is even more complex than the one regarding traditional forms of terrorism. As a matter of fact, in the latter case of discussion the issue at stake is how to define and properly tackle terrorism; while in the former case the scepticism on the issue expressed by some actors in the discussion proves that it is still some steps behind, compared to the discussion on terrorism. As a matter of fact, some claim that cyberterrorism has already occurred in our history, while others argue that we have not witnessed such a thing yet[205]. These differences of perception are led by several and diversified reasons, however, there seems to be a high degree of agreement among experts on one particular reason. As a matter of fact, it has been acknowledged that the more aspects of a society are controlled by computer systems or at least are connected to it, the more cyberterrorism becomes a consistent terrorist threat to that society. To put it in other words and to quote what Richard Clarke said already in 1999 "if you are connected you are vulnerable[206]". As a consequence, it is evident how the degree of risk to which a society is exposed when it comes to cyberterrorism, is proportional to its level of dependence on technology and computer networks. Nowadays, most of the so-called *developed societies* depend on infrastructures, which are controlled by computer networks and subsequently they belong to the group of actors who perceive cyberterrorism as a concrete and imminent threat. On the other hand, those societies whose core infrastructures are not imbedded in technological control systems are not concerned about this topic with the same level of severity[207].

On top of that, as explained in the two previous sections, a further cause for the difficulties in agreeing on a globally recognised definition for cyberterrorism, or at least a considerable delay in establishing it, is due to the fact that this term is the combination of two concepts, which are extremely difficult to define per se: *cyberspace* and

[205] Ibid.
[206] Cohen, D. (2014) *Cyber terrorism: case studies*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 8.
[207] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, pp. 57-118.

terrorism[208]. Indeed, these two elements result to be constitutive for the issue at stake: the cyberspace is the spatial coordinate indicating where the crimes are to take place; while terrorism is the coordinate clarifying which of the several crimes occurring in the cyberspace are to be kept into consideration. Subsequently, building the concept of cyberterrorism upon two still debated issues, outlining a generally recognised definition of the issue at stake could only imply a problematic and long process.

Despite the complexity of the debate surrounding the issue of cyberterrorism, some attempts to define it have emerged so far in the academic field; while, as far as international institutions are concerned, there is no evidence of a definition yet, despite the fact cyberterrorism as concept and threat to society has already been recognised. For this precise reason, we will now provide an overview of the most relevant definitions of cyberterrorism that have been outlined so far.

As explained at the beginning of the chapter, the very first definition of cyberterrorism is ascribed to the California's Institute for Security and Intelligence researcher who coined the term itself: Barry Collins. His definition is extremely concise and left most of the problematic issues about this topic unsolved: "the convergence of cybernetics and terrorism"[209]. However, we need to consider the fact that this definition dates back to the mid-1980s and that the events and technological developments of the following years served as a catalyst[210] for the development of more accurate definitions.

In 1997, the former Director of the FBI's Regional Computer Forensic Laboratory Program Mark M. Pollitt combined the definition of cyberspace by Barry Collin[211] with

---

[208] Douglas, C. A. *et al.* (2019) Towards Creating a New Research Tool: Operationally Defining Cybeterrorism, Augusta University.

[209] Collin, B. (1997) *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, Crime and Justice International, Vol.13, Issue 2, available at http://www.crime-research.org/library/Cyberter.htm.

[210] It is generally recognised that the tragic events of 9/11 had a considerable impact on the field of national and international security related to the problem of terrorism, even though 13 of the 19 international instruments aimed at facing the threat of terrorism already existed before 2001.
See Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, p. 140.
Moreover, on 6th August 1991 the World Wide Web was born and, at least theoretically for those years, it was available to everyone. The downside of this innovation was the concern about the vulnerability, which would be caused by the dependence on ICT. As Mark M. Pollitt stated in *Cyberterrorism- Fact or Fancy?*: "The combination of two of the great fears of the late 20th century are combined in the term 'cyberterrorism'.
See Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, p. 8.

[211] "Symbolic – true, false, binary, metaphoric representations of information- that place in which computer programs function and data moves", *Supra* note 37.

the definition of terrorism provided by the US Department of State[212] to draft a working definition of cyberterrorism. This definition found a considerable level of approval at the time and it was adopted by the FBI and it reads as follows:

> "Cyberterrorism is the premeditated, politically motive attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents[213]."

In this case, it is important to note how some of those elements characterising the several definition of terrorism that we have labelled as "recurring" are included in this definition of cyberterrorism. As a matter of fact, it is described as something "premeditated", meaning that the crime needs to be committed intentionally. However, this definition does not clarify what kind of intention needs to underlie the terrorist act. Moreover, the definition also includes the fact that, for an act to be classified as cyberterrorism, it needs to target the civilian population.

The FBI later dismissed this definition of cyberterrorism and updated it in 2004 with:

> "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda[214]".

It is evident how the gap about the *mens rea* of cyberterrorism was filled with this updated version of the definition. As a matter of fact, the intention needs to be the instillation of fear in civil society, in order to compel a government or a society to enact a certain political, social or economic change.

In December 1999 Bill Nelson outlined a definition for the Centre for the Study of Terrorism and Irregular Warfare, Monterey, CA, which reads as follows: "cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies on the pursuit of goals that are political

[212] "Premeditated, politically motivated violence perpetrated against non-combatant targets by sub national groups or clandestine agents", as quoted in Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, p. 9.
[213] Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, p. 9.
[214] Luiijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p.12.

religious or ideological[215]". This definition lacks of some of the core elements that characterise terrorism, such as the use or threat to use violence. This is plausibly due to the fact that this is one of the first attempts of definition and it dates back to 1999, when the possibilities offered by the cyberspace to perpetrate a terrorist act were still limited and the technical ability of the users were much lower compared to the ones that can be acquired in the recent days.

As we have already seen at the beginning of the chapter, in 2000 also Professor Dorothy Denning gave her contribution to this field. As we previously explained, she is the spokesperson of the school of thought that affirms that cyberterrorism should be defined in narrow terms and she defined the issue as "illegal and highly damaging attacks that target computers, networks, and digitally stored information for the purpose of causing harm to people or property or generating fear[216]". This definition seems to be a combination of the definition of cybercrime and the consensus *mens rea* necessary to label an act as a terrorist act; still, most of the recurring elements that we have spotted in the examples of definitions of terrorism are not included. However, after 9/11 she re-elaborated her definition, getting to the following result:

> "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not[217]".

Contrary to the first one, the updated version on the definition does include the aforementioned recurring elements. As a matter of fact, the underlying intent to generate fear in order to coerce a government or a society to carry out a political and social change is included; just like the fact that this coercive power generated by the spread of fear needs to be reached by means of violence or the threat to use it. A further

[215] Nelson B. *et al*, (1999) *Cyberterror: Prospects and Implications*, Centre for the Study of Terrorism and Irregular Warfare, Monterey, CA, available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a393147.pdf.
[216] Purdy, E. R. (2019) Cyberterrorism, Salem Press Encyclopedia.
[217] Conway, M. (2004) *Cyberterrorism: Academic Perspectives*, 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, p. 43.

noteworthy aspect of this definition is the fact that it includes a reformulation of the very first definition of cyberterrorism, that is the one by Berry Collins[218].

Another major contribution of the year 2000 was the one given in the *Proposal for an International Convention on Cyber Crime and Terrorism*, also known as the *Stanford Draft*. This draft of a legal text aimed at directly approaching the threat of cyberterrorism will be analysed in detail in the second chapter. For now, it is relevant to underline that this draft was spurred by the Council of Europe Convention on Cybercrime, which was recognised as a major step forward in this field by scholars, experts and other actors of the international community. Indeed, the Stanford Draft builds upon the Budapest Convention by the Council of Europe and tries to propose a legal instrument to deal with cyberterrorism explicitly[219]. The definition provided by the Stanford Draft reads as follows:

> "Cyber terrorism" means intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm[220]."

Also in this case intentionality is deemed to be necessary in order to label an act as terrorist. The consequences of the act against cyber systems need to result in harm to individuals or their physical property, to the order of a society or to its economy. It shall be noted that some core aspects are not tackled by this definition, such as the requirement for the target to be a civilian one.

In 2012 the computer science expert Jonalan Brickey outlined another definition of cyberterrorism:

---

[218] "The convergence of cybernetics and terrorism". As quoted in Luiijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 11.
[219] Cohen, A. (2010) *Cyberterrorism: Are We Legally Ready?*, Journal of International Business and Law, Vol. 9, No. 1, pp. 1-40.
[220] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, p. 1, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf.

> "Cyberterrorism is the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change[221]."

This definition does include the *mens rea* established by the consolidated definition provided by the Draft Comprehensive Convention on International Terrorism, but just like the previous definition omits the fact that the attack needs to be directed against civil targets. In addition to that, only the aim to achieve a political change is contemplated, while we have seen that in the recent doctrine there is the tendency to include other changes, such as social and economic ones.

In the same year another academic definition was proposed:

> "The use of electronic networks taking the form of a cyber-attack to commit a) a substantive act criminalized by the existing legal instruments prohibiting terrorism, or b) an act of terrorism under international customary law[222]."

Thus, this definition avoids the impasse of the controversial definition of terrorism by making reference to the existing international legal framework criminalising terrorism and to international customary law. In doing so, it avoids facing one of the major problems in the process of defining cyberterrorism and the question of the definition of terrorism is left unsolved.

Contrary to this example, the following one does not disregard the issue of the definition of the two constitutive elements of cyberterrorism. As a matter of fact, Eric Luiijf derived a definition of cyberterrorism from the combination of his own academic definition of terrorism and cybercrime:

> "The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organisation; made for the purposes of advancing a political, religious, racial or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorised actions affecting

[221] Brickey, J. (August 2012) *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, CTC Sentinel, Vol. 5, Issue 8, p. 6, available at https://www.researchgate.net/publication/235782714_Defining_Cyberterrorism_Capturing_a_Broad_Range_of_Activities_in_Cyberspace.

[222] Shiryaev, Y. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, p. 149.

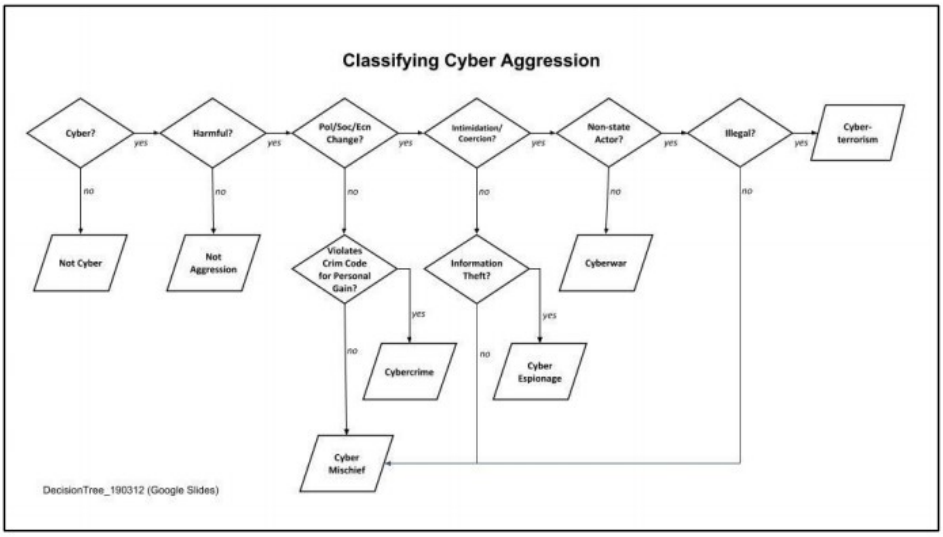
> information and communication technology based control of real-world physical processes; and it involves or causes: violence to, suffering of, serious injuries to, or the death of (a) persons(s); serious damage to a property; a serious risk to the health and safety of the public; a serious economic loss; a serious breach of ecological safety; a serious breach of the social and political stability and cohesion of a nation[223]".

It can be claimed that this definition is the most exhaustive one we have examined so far, as it includes all the recurring elements that are contained in the mainstream definitions of terrorism that have been provided by academic and included in international legal instruments. Moreover, it also faces the topic of in which extent the cyber dimension needs to be involved and it lists the consequences that such acts need to cause for an act to be classified as a cyberterrorist stack.

Finally, one of the most recent definitions was outlined in March 2019 and it reads as follows:

> "A threatened or actual computer-mediated act consequentially conducted through electronic networks by subnational actors to intimidate or coerce governments or people in order to achieve the perpetrator's political, economic, or social objectives[224]".

This definition was supplanted with a graph, which renders it far more thorough.



225

[223] Luijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, p. 16.
[224] Douglas, C. A., Griffith, C.,. Murray, G. R, Heslen, J. J., Davies, K. L., Hunter, Y., Jilani-Hyler, N., & Ratan, S. (2019) *Towards Creating a New Research Tool: Operationally Defining Cybeterrorism*, Augusta University, p. 14.

According to this graph, in order to classify a cyberaggression as cyberterrorism, there needs to be the pivotal presence of the cyber element; the committed act needs to be harmful; its goal needs to be a political, social or economic change; there needs to be the underlying intention to intimidate or coerce a government or a society; it needs to be perpetrated by non-state actors and finally it needs to be an illegal act. Thus, this definition, if considered with its explicative graph, includes all the recurring elements that form the consolidated definition of terrorism and combines it with the pivotal role that the cyber dimension needs to play in an instance of cyberterrorism.

1.6 The choice of the Council of Europe as framework of analysis

So far we have been providing a general overview of the issue of cyberterrorism, first focusing on the concrete ways in which it can manifest itself and then analysing how it can be defined both from an academic point of view and from the point of view of international law. This was a necessary premise to introduce and batter understand the issue at stake. However, the aim of our dissertation is to analyse the issue of cyberterrorism in the framework of the Council of Europe and we will now proceed to give an explanation for such a choice.

The choice of the Council of Europe legal framework as field of analysis was driven by several reasons. First of all, on the light of the lack of an international legal instrument directly addressing cyberterrorism, a viable strategy to tackle this issue could be the combination of the international legal instruments addressing the two constitutive elements of cyberterrorism. In the case of the Council of Europe three Conventions result to be relevant and they are the Convention on Cybercrime, also known as the Budapest Convention[226], the European Convention on the Suppression of Terrorism[227] and the Convention on the Prevention of Terrorism[228]. Among these three international legal instruments, the Budapest Convention is doubtlessly the one that enjoys the highest degree of approval in the international community. As a matter of fact, it is

[225] Douglas, C. A., Griffith, C.,. Murray, G. R, Heslen, J. J., Davies, K. L., Hunter, Y., Jilani-Hyler, N., & Ratan, S. (2019) *Towards Creating a New Research Tool: Operationally Defining Cybeterrorism*, Augusta University, p. 40.
[226] Council of Europe, (2004) *Convention on Cybercrime ETS No. 185*, Budapest, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[227] Council of Europe (1978) *European Convention of the Suppression of Terrorism*, ETS No. 90, art. 1, p. 1, Strasbourg, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800771b2.
[228] Council of Europe (2007) *Convention on the Prevention of Terrorism CETS No. 196*, Warsaw, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.

deemed to be a major achievement in the field of cybercrime, as it is the first Treaty addressing "crimes committed via Internet and other computer networks[229]".

Moreover, what distinguishes the Budapest Convention from other legal texts dealing with the cyberspace and cybercrime and therefore that makes it worth of this analysis, is the fact that this legal text is designed in such a way to tackle the issue of conduct, rather than the issue of technology itself[230]. This feature allows to overcome a long-standing problem: the fact that technology develops at an extremely quick pace, much quicker than the way in which law changes. Therefore, by addressing the conduct instead of technology, it is guaranteed that the legal text won't result to be obsolete after a few years with the development of new technologies. To put it in the words of the drafters of the Convention themselves, the language used in the Budapest Convention is indeed "technology neutral[231]".

Furthermore, as Draetta highlighted, the CoE Convention on Cybercrime includes in its provisions crimes against the integrity of computer data and network and such a precondition would allow to tackle cyberterrorism, even though dealing with a legal instrument not explicitly outlined for that[232]. On top of that, the Convention is supplemented by a Protocol on Xenophobia and Racism, which might result to be of use in using the Budapest Convention to tackle cases of cyberterrorism[233].

These three legal instruments will be analysed into detail in the following chapter, but for now it is relevant to underline the fact that the combination of these legal texts creates a legal framework of binding nature for the High Contracting Parties. As a matter of fact, the international instruments of the Council of Europe enjoy a binding legal nature for their High Contracting Parties. This feature plays a crucial role as it allows to guarantee a higher degree of implementation, due to the fact that those States

[229] Council of Europe, *Details of Treaty No. 185 – Convention on Cybercrime*, last accessed 15th April 2020, stable URL https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[230] Council of Europe, *Council of Europe action against Cybercrime*, stable URL https://www.coe.int/en/web/portal/coe-action-against-cybercrime, last accessed 24th January 2020.
[231] Council of Europe (2004), *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, available at https://rm.coe.int/16800cce5b.
[232] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 453-464.
[233] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, Strasbourg, art. 2, p. 2, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

that decided to ratify a CoE treaty are bound to respect and fulfil the provisions included in it[234].

A further relevant feature of the Council of Europe is its willingness to strike a fair balance between protecting human rights and guaranteeing affective prosecution of crimes. A concrete example can be found in one the recitals of the preamble of the CoE Convention on Cybercrime, which reads as follows:

> "Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy[235]".

Moreover, article 15 of the CoE Convention on Cybercrime requires those States who ratified this legal instrument to establish measure aimed at preventing the abuse of law enforcement and at protecting human rights[236]. Therefore, it can be claimed that violations of human rights are at least harder to commit under the protection of such framework. The human rights that might be invoked in this circumstance and that are protected by the European Convention on Human Rights[237] include rights like right to respect for private and family life; right to freedom of thought, conscience and religion; right to liberty and security; right to freedom of expression; right to freedom of assembly and association. In order to better understand the reasoning that is followed when having to strike a fair balance between human rights and effective prosecution, we could mention a case that was taken in front of the European Court of Human Rights of Strasbourg. As a matter of fact, it has been claimed that the tendency of the Council of

[234] Leach, P. (2017) *Taking a Case to the European Court of Human Rights*, Oxford, fourth edition, student version.
[235] Council of Europe, (2004) *Convention on Cybercrime ETS No. 185*, Budapest, p. 2, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[236] Seger, A. (2012) *The Budapest Convention 10 years on: lessons learnt*, in Cybercriminality: finding a balance between freedom and security, ISPAC International Scientific and Professional, Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, edited by S. Manacorda.
[237] Council of Europe (1953) *European Convention on Human Rights*, Rome, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.

Europe can be inferred by some decisions by the ECHR[238] decisions, like in the case of *Zaoui V. Switzerland*. On 18th January 2001, the Court decided that this recourse was not admissible and that Switzerland had acted legitimately to protect the national security in confiscating Mr. Zaoui's computer. Indeed, Swiss police did so due to the applicant's propaganda online activity in favour of the Algerian Islamic Front[239]. In general, according to the ECHR the matter of security prevails on the protection of the human rights listed above, if the measures taken by the State to preserve national security are provided by domestic law, their the aim is legitimate and necessary in a democratic society[240].

Contrary to our belief that analysing the issue of cyberterrorism in the framework of the Council of Europe, some might argue that the choice of a regional international institution is unfit for the analysis of a topic that is characterised by such a transnational nature. However, accession to the aforementioned international legal instruments is not limited to the 47 member States of the Council of Europe. On the contrary, they are opened for ratification by non-member States as well[241], considerably enlarging the effects that they can have on the topic at stake, where international cooperation plays such a crucial role. As a matter of fact, these treaties have actually been ratified by some non-member States so far and this phenomenon testifies the approval by the international community towards these Conventions. Moreover, also experts and academics express their support to these legal instruments, though stressing their flaws at the same time, and illustrate how they can be a good provisional way to address cyberterrorism in the wait for a specific legal instrument[242]. This is particularly true for the Budapest Convention, which is recognised as a major step in a field still lacking of a well-established legal framework[243]. As a matter of fact, it is regarded at international level, as a guideline for those States that, at national level, have not implemented any kind of legislation aimed at tackling the issue of cybercrime.

---

[238] The Court was established with art. 19 of the European Convention on Human Rights of 1950, *supra* note 227.
[239] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 453-464.
[240] Leach, P. (2017) *Taking a Case to the European Court of Human Rights*, Oxford, fourth edition, student version.
[241] Council of Europe (1949) *Statute of the Council of Europe*, London, available at https://rm.coe.int/1680306052.
[242] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 453-464.
[243] Hopkins, S. L. (2003) *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, Journal of High Technology Law, Vol. 2, No. 1, pp. 101-122.

In addition to that, the Council of Europe's Committee of Experts on Terrorism realised, between the years 2006 and 2007, an analytical report on the issue of cyberterrorism and the terrorist use of the Internet[244]. It can doubtlessly be claimed that this analytical report is one of the most relevant contribution in this field. Indeed, the report seeks to provide a comprehensive overview of the phenomenon bypassing the deadlock over the issue of cyberterrorism definition. The report provides us with an explanation of the possible manifestations of cyberterrorism, which was used to realise this first chapter; but also it provides us with an analysis of how existing legal instruments could be used to tackle this phenomenon. Thus rendering the Council of Europe the only international institution having analysed the existing international legal framework on both cybercrime and terrorism and having outlined an analysis on how it could apply to instances of cyberterrorism. According to our opinion, this unique project is the decisive element to choose the Council of Europe as framework of reference for the analysis of the issue of cyberterrorism.

1.6.1 The lack of a Council of Europe definition of cyberterrorism

After justifying our choice of the Council of Europe as framework of analysis for our dissertation; it is necessary to take a step back to paragraph 1.5.3 and to analyse the issue of the lack of a CoE definition of cyberterrorism.

Until today the Council of Europe, whose legal framework will be our framework of analysis from the next chapter onwards, has not established a comprehensive definition of cyberterrorism yet. The lack of a definition, however, must not be intended as a lack of concern towards this issue. Indeed, as previously anticipated the Council of Europe's Committee of Experts on Terrorism (CODEXTER) started a study in 2006 on the issue of cyberterrorism, which resulted in the explanatory report *Cyberterrorism: the use of internet for terrorist purposes*. At the time of the publishing of the volume in the following year, the then-Secretary General of the Council of Europe Terry Davis stated:

> "The threat of cyberterrorism and the misuse of the Internet for terrorist purposes is particularly alarming because our society is so dependent on computer systems and the Internet.

[244] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

> While it is true that the threat may be exaggerated, it cannot be denied or ignored. The increasing visibility of terrorism has led to these unconventional weapons being harnessed by a new computer-savvy generation of terrorism.
>
> The Council of Europe's Cybercrime Convention (2001) and the Convention on the Prevention of Terrorism (2005) provide a legal response which is consistent with the protection of human rights and the individual freedoms. These innovative and unique treaties have created a new dynamic at international level, fostered by the ever-increasing need for international cooperation[245]".

This statement acknowledges the threat that cyberterrorism poses to civil society and it can also be interpreted as a commitment to address the issue. The last part of this statement both mirrors the reasoning we have followed while analysing the issue of the definition of cyberterrorism, as the two CoE Conventions related to the crimes committed in the cyberspace[246] and to terrorism[247] are mentioned as reference legal instruments; and it also confirmed the assumption we made in the previous paragraph, when affirming that the relevant existing CoE international legal instruments con be interpreted in order to tackle the issue of cyberterrorism, at least as long as more suitable legal instruments will be outlined.

It is true that not only the CoE did not provide a definition of cyberterrorism, neither of cyberspace or terrorism. However, this deadlock did not hinder the drafting of instruments related to these topics, thus guaranteeing at least a partial coverage of them. Indeed, the CoE Convention on Cybercrime is aimed at addressing the jurisdictional issue, which was framed by the evolution of ITC and therefore focuses on harmonizing cybercrime laws and guaranteeing the presence of procedural mechanisms in order to achieve the successful prosecution of cybercriminals[248]. However, the Explanatory Report to the Convention on Cybercrime hints at a definition of cyberspace when reporting:

---

[245] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.p.7.
[246] Council of Europe, (2004) *Convention on Cybercrime ETS No. 185*, Budapest, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[247] Council of Europe (2007) *Convention on the Prevention of Terrorism CETS No. 196*, Warsaw, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.
[248] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425, available at https://btlj.org/?s=The+Council+of+Europe%27s+Convention+on+Cybercrime&submit=Search.

> "The fast developments in the field of information technology have a direct bearing on all sections of modern society. The integration of telecommunication and information systems, enabling the storage and transmission, regardless of distance, of all kinds of communication opens a whole range of new possibilities. These developments were boosted by the emergence of information super-highways and networks, including the Internet, through which virtually anybody will be able to have access to any electronic information service irrespective of where in the world he is located. By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse[249]".

Though this statement cannot be taken as definition, it is noteworthy that is includes an element that we have noticed in some of the definitions we took into consideration in paragraph 1.5.1; that is the recognition that such a space is liable to exploitation by individuals with malicious intents.

On the other hand, when dealing with the definition of terrorism, the CoE does not provide its own definition, but rather states in article 1 of the Convention on the Prevention of terrorism that:

> "(1.) For the purposes of this Convention, "terrorist offence" means any of the offences within the scope of and as defined in one of the treaties listed in the Appendix. (2.) On depositing its instrument of ratification, acceptance, approval or accession, a State or the European Community which is not a party to a treaty listed in the Appendix may declare that, in the application of this Convention to the Party concerned, that treaty shall be deemed not to be included in the Appendix. This declaration shall cease to have effect as soon as the treaty enters into force for the Party having made such a declaration, which shall notify the Secretary General of the Council of Europe of this entry into force[250]".

In doing so, the choice of the Council of Europe for the purposes of its Convention, just like it has already happened in other cases, is to make reference to the existing international legal framework that uses the sectoral approach to terrorism, about which we have argued in the previous section.

---

[249] Council of Europe (2004), *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, p. 2, available at https://rm.coe.int/16800cce5b.

[250] Council of Europe (2007) *Convention on the Prevention of Terrorism CETS No. 196*, Warsaw, art, 1, p. 2, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.

However, the CODEXTER made a clarification to this issue in its analytical report on cyberterrorism, stating that:

> "In this report, the term "terrorism" is understood in a broad sense in order to enable a comprehensive examination of possible use of the Internet for terrorist purposes. It includes the elements of violence or the threat to use violence, psychological impact (such as the increase in fear), political goal(s), and the unlawfulness of the committed acts[251]".

Therefore the choice of the CoE is to make reference to the aforementioned framework, but to widen its range of analysis to other aspects that might be implied in the commission of a terrorist act.

To conclude, it shall be noted how the CoE seeks to provide a legal framework for both fields, despite not having found a consensus definition for them yet. In doing so, the controversies that most of the times lead to deadlocks in the shaping of an international framework causing the emergence of a gap in international law, are avoided.

Conclusions

This first chapter opened with an overview of the ways in which cyberterrorism is likely thought to be perpetrated. We highlighted how the perpetration of cyberterrorism is actually incentivised by a series of factors, such as the possibility to efficiently preserve anonymity, the quickness that the cyberspace guarantees, the disregard for territorial borders and so on; which terrorist actors seem to be aware of. A proof of this was found in the files contained in some seized computers belonging to al-Qaeda, such as engineering and structural features of digital switches of dams, power, water, transportation and communication grids[252]. Moreover, the latest generation of terrorists belongs to the so-called digital world, allowing them to have a greater familiarity with cybertechnology and cyberspace in general[253]. Based on these preconditions, the exploitation of the cyberspace by terrorist actors cannot be neglected, in none of its manifestations, whether it is in the form of pure cyberterrorism, of cyberterror support or the broad use of internet for terrorist purposes.

---

[251] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.p. 14.
[252] Weimann, G. *www.terror.net* - *How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report, available at https://www.usip.org/sites/default/files/sr116.pdf.
[253] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

After the overview on the forms that might be taken by cyberterrorism, we moved on to the definitional aspect of the issue. After taking into consideration the controversies regarding the two constitutive elements of cyberterrorism, cyberspace and terrorism, and their definition; we moved to the definitional issue of cyberterrorism per se. From our analysis it emerged that the doubt whether cyberterrorism should be defined in narrow or in broad terms remains unsolved. Each side believes that its definition is the most suitable one to face this issue: on the one side, those who claim a narrow definition do so, as we have already said, to avoid an overlap of cyberterrorism with other forms of cybercrime; on the other side, those who claim a broad definition, do so in view of a potential international legal instrument, in such a way that a too strict definition would never be the cause of a lack of ratification and national implementation.

Despite the wide array of possible definitions of cyberterrorism, it is self-evident how certain elements are a constant inside each of them. First of all cybertechnology needs to play a pivotal role in this issue; indeed the cyberspace can either be the target of the attack per se, or the means through which it is perpetrated[254]. To quote the clarification on this aspect, given by one of the authors of the aforementioned definition:

> "Cyber must play a consequential or essential role in the act such that the act exists only or primarily because of its cyber nature or that the conduct of the act requires expertise in cybertechnology beyond that of the typical user of cybertechnology[255]".

Moreover, a hypothetical cyberterrorist act needs to be intentional and needs to be premeditated in order to reach a social, political or economic change. The means through which these goals are to be reached is violence or the threat to use violence against non-combatants[256]. This violence needs to result in either fear or harm towards non-combatants or their property. To put it in the words of Professor Kenney:

> "These four elements—computer generation, political motivation, physical violence, and psychological coercion—are the essential attributes of cyber-terrorism. To qualify as cyber-terrorism, an act must contain all four properties, the combination of which

[254] Luiijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, pp. 11-17.
[255] Douglas, C. A., Griffith, C.,. Murray, G. R, Heslen, J. J., Davies, K. L., Hunter, Y., Jilani-Hyler, N., & Ratan, S. (2019) *Towards Creating a New Research Tool: Operationally Defining Cybeterrorism*, Augusta University, p. 5.
[256] If we were to deal with a cyberattack against combatants, we would enter the domain of cyberwar. According to some scholars, to classify a cyberattack as cyberwar the perpetrator needs to be a State or one of its bodies.

> distinguishes it from its broader genus and other cyber-attack species, such as hacktivism and cyber-warfare[257]".

Nonetheless, despite being these elements almost a constant in the wide range of possible definitions of cyberterrorism, applying these "traditional" categories to a new space and a new phenomenon implies a series of considerations. Indeed, the last two points result to be the most problematic. We have already anticipated that the cyberspace can either be the means of a cyberterrorist act or its target. When it comes to the latter, it is possible that the harmful consequences of the illicit act do not involve the real world and therefore we would be dealing with "virtual violence". To the present days there have been several studies about the wide array of manifestations of violence on several fields of expertise. The same cannot be affirmed for that kind of violence, which takes place in the cyberspace and affects the cyberspace in a way that does not affect the real world[258]. This issue is linked with the last element dealing with the causing of harm towards non-combatants or their property. Indeed, for instance it is widely recognised that destroying someone's computer means harming someone's property; but destroying the information contained in that computer is still a debated issue that the current definitions of cyberterrorism leave unsolved.

The lack of an official definition results to be concerning, considering the fact that several evidences prove cyberterrorism to be an incoming threat. Some scenarios have already concretised, others only partly, while others are alarmingly realistc; both technologically speaking and for their compatibility with the aims of terrorist actors. Despite the imminence of the threat posed by cyberterrorism, there is no legal framework directly addressing this topic. Cyberterrorism has been indirectly included among the provisions of some legal instruments[259] dealing either with terrorism or

---

[257] Kenney, M. (2015) *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, Vol. 59, Issue 1, p. 122, available at https://www.sciencedirect.com/science/article/pii/S0030438714000787.

[258] Conway, M. (2004) *Cyberterrorism: Academic Perspectives*, 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK.

[259] For instance, the UK's Terrorism Act (UK, 2000) defined terrorism as follows:
The use or threat of action designed to influence the government or an international governmental organisation or to intimidate the public, or a section of
the public; made for the purposes of advancing a political, religious, racial or
ideological cause.
It involves or causes:
• serious violence against a person;
• serious damage to a property;
• a threat to a person's life;
• a serious risk to the health and safety of the public; or
• serious interference with or disruption to an electronic system (UK Terrorism Act 2000).

cybercrime and it has been subject of interest for a wide number of scholars and academics; however technology and crime develop at such a high speed that a legislative gap emerged. Nonetheless, three of the Council of Europe's treaties separately and indirectly cover some of the aspects regarding cyberterrorism; that is why they will be taken into account in the next chapter, in order to verify to which extent it can be claimed that the threat of cyberterrorism is covered by already existing international legal instruments in the framework of the Council of Europe.

The last point of the definition shows us how the cyber element is contemplated as a plausible aspect of a terrorist attack.
Luiijf, E. (2014) *Definitions of Cyber Terrorism*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, pp. 11-17.

Chapter 2: Existing international legal instruments relevant for the issue of cyberterrorism

Introduction

The following chapter builds upon the acknowledgment emerged along the previous one, that is the fact that at the moment there is no international legal instruments directly addressing the issue of cyberterrorism. For this precise reason, the aim of this chapter is to take into consideration existing international legal instruments indirectly linked to our field of analysis and try and assess their applicability to it.

Despite the choice of the Council of Europe as framework of analysis, first we will provide a brief overview of the most relevant aspects on the UN framework addressing the issue of international terrorism. As explained in the previous chapter, it is frequent for international institutions to make reference to this framework in their legal texts. This happens also in the case of the CoE instruments addressing terrorism; as a consequence this digression is needed for the purposes of our analysis.

After that, we will proceed to an overview of the possible application of existing CoE instruments to the issue at stake. As a matter of fact, we will depict how despite the lack of an international instrument explicitly outlined for this field, the existing treaties at CoE level can guarantee an indirect and, in some cases, partial coverage of the issue. The analysis of the existing CoE legal instrument will follow the same reasoning that we applied to the analysis of the definition of cyberterrorism: focusing on the two elements that constitute the phenomenon of cyberterrorism, that is cyberspace and terrorism. That is why, the main focus of the chapter will be on the Convention on Cybercrime of the Council of Europe (CETS No. 185)[260], also known as the Budapest Convention and the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196)[261]. Another core topic of this second section will be the so-called Stanford Draft, an academic document, which builds upon the CoE Convention on Cybercrime to try and propose an instrument directly addressing the issue of cyberterrorism[262].

[260] Council of Europe, (2004) *Convention on Cybercrime ETS No. 185*, Budapest, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[261] Council of Europe (2007) *Convention on the Prevention of Terrorism CETS No. 196*, Warsaw, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.
[262] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, pp. 25-45, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf.

2.1 The UN sectoral framework against terrorism: a reference for other international legal instruments

As anticipated above, despite the fact that the purpose of our analysis is to frame the issue of cyberterrorism in the context of the Council of Europe's legal instruments, making a reference to the UN regime addressing terrorism is necessary. As a matter of fact, it is frequent for other treaties to make reference to the UN framework tackling terrorist manifestations; considering the fact that the United Nations is deemed to be the lead international institution in the fight of international terrorism and in the coordination of international cooperation against it[263]. To date, the UN regime counts 13 sectoral Conventions and Protocols addressing possible manifestations of terrorism[264]: Convention on Offenses and Certain Other Acts Committed on Board Aircraft; Convention for the Suppression of Unlawful Seizure of Aircraft; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents; International Convention against the Taking of Hostages; Convention on the Physical Protection of Nuclear Material; Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation; Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf; Convention on the Marking of Plastic Explosives for the Purpose of Detection; International Convention for the Suppression of Terrorist Bombings; Convention on the Suppression of Terrorist Financing and International Convention for the Suppression of Acts of Nuclear Terrorism.

As anticipated in the paragraph 1.5.2 about the definitions of terrorism, in addition to these Conventions and Protocols, the UN Ad Hoc Committee established by the UN General Assembly in 1996 is negotiating a Draft Comprehensive Convention on

[263] Manap, N. A., Taji, H., & Tehrani, P. M. (2013) *Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime*, Computer Law & Security Review, Vol. 29(3), 2013, pp. 207-215.
[264] De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova: Cedam, vol. 7.

International Terrorism in order to establish "an umbrella legal framework[265]" against terrorism.

In the aftermath of 9/11, the UN Security Council decided to take a more vigorous approach to the issue, which resulted into resolution 1373 acting under Chapter VII of the UN Charter[266]. This Resolution declares that international terrorism is "a threat to international peace and security" and it also binds UN Member States to criminalise the "financing of terrorist acts and associated money-laundering" and "recruitment of members of terrorist groups" and to foster "exchange of information on movement of terrorists, forgery and falsification of travel documents, arms trafficking, use of communication technologies, and terrorist threats related to WMD [267] ". The implementation of the aforementioned measures shall be monitored by the Counter-Terrorism Committee established by the Resolution itself[268]. The wording used to criminalise the aforementioned conducts allows for the inclusion of the perpetration of these acts by means of ICT. The UN Security Council reiterated its condemn against these offences preparatory to terrorism in the Resolution 2178 of 2014[269].

However, the presence of such international regime does not imply its immediate application to possible instances of cyberterrorism. Indeed, we need to take into consideration the wording that is used, in order to verify that the provisions can be interpreted in such a way that cyberterrorism can be addressed. The fact that, in order to guarantee a partial coverage of cyberterrorism, it is needed to rely on interpretation; is due to the fact that no provision has criminalised it so far. It shall be noted, that some of the treaties composing the international legal framework on terrorism were drafted in years, in which cyberterrorism was unconceivable; thus rendering the global application of the provisions to cyberterrorism a considerably hard task, if not impossible in some cases [270]. We will now provide an overview of the possible application of the

[265] Hmoud, M. (2006) *Negotiating the Draft Comprehensive Convention on International Terrorism: Major Bones of Contention*, Journal of International Criminal Justice, Vol. 4, Issue 5, pp. 1031–1043, available at https://doi.org/10.1093/jicj/mql081.
[266] Cohen, A. (2010) *Cyberterrorism: Are We Legally Ready?*, Journal of International Business and Law, Vol. 9, No. 1, pp. 1-40.
[267] UN Security Council (2001) *Resolution 1373*, available at https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf.
[268] Cohen, A. (2010) *Cyberterrorism: Are We Legally Ready?*, Journal of International Business and Law, Vol. 9, No. 1, pp. 1-40.
[269] UN Security Council (2014) *Resolution 2178*, available at https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2178.pdf.
[270] Ibid.

aforementioned UN regime addressing terrorism to instances of cyberterrorism, also making reference to some of the scenarios we took into analysis in the first chapter.

The purposes of the Convention for the Suppression of Unlawful Seizure of Aircraft[271], the Convention for the Suppression of Unlawful Acts Against Safety of Civil Aviation[272] and the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation[273] is to guarantee the criminalisation of acts like the seizure of an aircraft, acts of violence against individuals present inside it and the destruction of air navigation facilities. A possible scenario that would require the triggering of these provisions would the instance of an IT-based manipulation of those systems responsible for the control of flights[274]. In such a case, the wording of article 1 of Convention for the Suppression of Unlawful Acts Against the Safety of Civilian Aviation would be suitable to address the matter, as it states that Member States should criminalise the destruction "of an aircraft in service or causes[ing of] damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight"; such condition applies to "air navigation facilities" and the interference with them as well. In addition to that, the communication of false information with the aim of "endangering the safety of an aircraft in flight" is contemplated as well[275]. The fact that the wording does not specify the means through which the aforementioned acts shall be perpetrated allows the inclusion of IT-based perpetration.

The framework created by the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation[276] exactly mirrors the situation depicted above. An instance that might require the triggering of the provisions of this Convention

[271] United Nations (1970) *Convention for the Suppression of Unlawful Seizure of Aircraft*, The Hague, , available at https://treaties.un.org/doc/db/Terrorism/Conv2-english.pdf.
[272] United Nations (1971) *Convention for the suppression of unlawful acts against the safety of civil aviation*, Montreal, available at https://treaties.un.org/doc/Publication/UNTS/Volume%20974/volume-974-I-14118-English.pdf.
[273] United Nations (1988) *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*, Montreal, available at https://treaties.un.org/doc/db/Terrorism/Conv7-english.pdf.
[274] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[275] United Nations (1971) *Convention for the suppression of unlawful acts against the safety of civil aviation*, Montreal, available at https://treaties.un.org/doc/Publication/UNTS/Volume%20974/volume-974-I-14118-English.pdf.
[276] United Nations (1988) *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, Rome, available at https://treaties.un.org/doc/db/Terrorism/Conv8-english.pdf.

could be the IT-based manipulation of the computer systems controlling a ship[277]. The same can be claimed for instances related to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf. In this case, the seizure or exercise of control by means of force or threat to use it, is criminalised by the Convention, together with the destruction of the platform with the aim of compelling a third party to behave in a specific way[278]. The wording of the Convention does not hinder the possibility to apply it to instances of destruction of fixed platform carried out by means of IT-interference against the security control system[279]

The Convention on the Prevention and Punishment of Crimes Against Internationally protected Persons, including diplomatic agents sets forth the criminalisation of certain acts against representatives of States, such as murder, kidnapping, certain violent attacks, but also the attempt and threat to commit such acts[280]. Also in this case, the wording does not specify the means through which the aforementioned acts shall be carried out; allowing to cover their perpetration by means of computer systems. The most plausible case of IT-based commission of one of the aforementioned acts is the threat to commit violent acts. However, more dramatic instances cannot be excluded, such as the manipulation of the computer system of a hospital in order to interfere with vital data of the targeted person[281].

The International Convention Against the Taking of Hostages criminalises the actions of "any person who seizes or detains and threatens to kill, to injure or to continue to detain another person" with the aim of compelling a third party to act in a specific way[282]. Also in this case the exploitation of computer systems is not excluded by the

[277] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[278] United Nations (1999) *Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf*, New York, available at https://treaties.un.org/doc/Publication/UNTS/Volume%201678/v1678.pdf.
[279] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[280] United Nations (1973) *Convention on the Prevention and Punishment of Crimes Against Internationally protected Persons, including Diplomatic Agents*, art. 2, available at https://legal.un.org/ilc/texts/instruments/english/conventions/9_4_1973.pdf.
[281] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[282] United Nations (1979) *International Convention Against the Taking of Hostages*, art. 1, available at https://treaties.un.org/doc/db/terrorism/english-18-5.pdf.

wording. A plausible instance would be the manipulation of a computer system controlling elevators[283] or the demand of ransom by means of ICT[284].

One of the Convention on the Physical Protection of Nuclear Material's goals is to prevent the "loss, theft, misuse or damage of nuclear material[285]". The threat to commit one of these acts is also criminalised by the Convention, precisely by article 6. Just like in the previous case, threat to use nuclear material for the purpose of striking a terrorist attack can be carried out by means of ICT and the wording does not hinder the triggering of article 6. However, most harmful instances are possible as well, such as the manipulation of the computer system controlling a nuclear power plant, in order to scatter nuclear material. Such instance could be covered, as there is no clause on how such "misuse" should be carried out[286].

The International Convention for the Suppression of Terrorist Bombing criminalises the intentional and unlawful delivery, placing, discharging or detonation of an explosive or lethal device in or against a place of public use, a State or government facility, a public transport system or an infrastructure facility[287]. Due to the wording of this article, the hypothetical triggering of a bomb by means of a computer system can be covered[288].

2.2 An overview of the Council of Europe Convention on Cybercrime – CETS No. 185

As previously stated, in the light of the lack of an international legal instrument addressing the threat of cyberterrorism, an alternative way to try and guarantee at least a partial cover of the issue is separately tackling the two constitutive elements of the topic. We will now proceed with an overview of the most relevant instrument for crimes related to the cyberspace: the CoE Convention on Cybercrime.

---

[283] United Nations (1982) *Convention on the Physical Protection of Nuclear Material*, art. 3, Vienna available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub615web.pdf. pp. 139-192.
[284] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[285] United Nations (1982) *Convention on the Physical Protection of Nuclear Material*, art. 3, Vienna available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub615web.pdf.
[286] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[287] United Nations, *International Convention for the Suppression of Terrorist Bombing*, art. 2, 15th December 1997, available at https://treaties.un.org/doc/Treaties/1997/12/19971215%2007-07%20AM/ch_XVIII_9p.pdf.
[288] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

The CoE Convention on Cybercrime, or Budapest Convention, is considered to be particularly noteworthy because it is the first international legal instruments dealing with criminal actions perpetrated by means of the Internet[289] and, at the moment, it is the only instrument dealing with this issue and having a binding nature[290]. For this precise reason it is of particular relevance for the purposes of our analysis as it addresses the field in which cyberterrorism is included.

This treaty stemmed from the need to find an instrument, which would have been suitable to address the new crimes or the new ways of committing already existing crimes, that emerged alongside pivotal technological developments, such as the Internet[291]. The fact that the need for such a convention is linked to these events implicates that this legal instrument has a long history. Indeed, The Budapest Convention was the first international legal instrument dealing with crimes committed by means of the Internet and computer networks in general. Already in 1989 the CoE Recommendation No. R. (89) 9[292] of the Committee of Ministers to Member States on Computer-related Crime dealt with the need to establish new substantive laws, in order to criminalise the illicit conduct carried out by means of computer networks[293]. The treaty per se roots in November 1996, when the European Committee on Crime Problems (CDPC)[294] first expressed its belief, that the Council of Europe needed to establish a committee of experts on cybercrime. Such committee was instituted on the basis of the following acknowledgment:

---

[289] Cohen, A. (2010) *Cyberterrorism: Are We Legally Ready?*, Journal of International Business and Law, Vol. 9, No. 1, p. 8.

[290] Council of Europe, *Budapest Convention and related standards*, last accessed 26th July 2020, stable URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[291] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425, available at https://btlj.org/?s=The+Council+of+Europe%27s+Convention+on+Cybercrime&submit=Search.

[292] Council of Europe Committee of Ministers (1989) *Recommendation No. R. (89) 9 on Computer-related Crime*, available at https://dig.watch/instruments/recommendation-no-r-89-9-committee-ministers-member-states-computer-related-crimes.

[293] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425, available at https://btlj.org/?s=The+Council+of+Europe%27s+Convention+on+Cybercrime&submit=Search.

[294] Council of Europe, *European Committee on Crime Problems*, last accessed 10th July 2020, stable URL: https://www.coe.int/en/web/cdpc/home:
Set up in 1958, the European Committee on Crime Problems (CDPC) was entrusted by the Committee of Ministers the responsibility for overseeing and coordinating the Council of Europe's activities in the field of crime prevention and crime control. The CDPC meets at the headquarters of the Council of Europe in Strasbourg (France).
The CDPC identifies priorities for intergovernmental legal co-operation, makes proposals to the Committee of Ministers on activities in the fields of criminal law and procedure, criminology and penology, and implements these activities.
The CDPC elaborates conventions, recommendations and reports. It organises criminological research conferences and criminological colloquia, conferences of directors of prison administration.

> "By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities. [..] The criminal law must therefore keep abreast of these technological developments which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse[295]".

This statements proves how, despite the fact that the technology of those years had not reached the potential that is available to us all nowadays, the pivotal issue about cybercrime in general was already clear to the Council of Europe: its 'transborder character'. This awareness was a constant in the drafting process of the Budapest Convention and it is reflected in the core aims of the Convention, which includes international cooperation[296]. For the purposes of our analysis, this focus on international cooperation results to play a pivotal role. Thus, as we have already highlighted, such an approach is required in order to tackle such a transnational issue like cyberterrorism.

The effort to outline the Budapest Convention lasted over 12 years and in that period, several soft-law recommendations helped opening the road to this covenant and its goals[297], but the need for a Convention and its binding legal nature was strongly felt by experts. As a matter of fact, Professor Dr. H.W.K. Kaspersen, the author of the report on the matter at stake on behalf of the CDPC, openly stressed the need for an actual convention and stated that such international legal instruments should deal with

[295] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, p. 2, available at https://rm.coe.int/16800cce5b.
[296] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[297] Seger, A. (2012) *The Budapest Convention 10 years on: lessons learnt*, in Cybercriminality: finding a balance between freedom and security, ISPAC International Scientific and Professional, Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, edited by S. Manacorda.

"criminal substantive law matters, but also with criminal procedural questions as well as with international criminal law procedures and agreements[298]".

In addition to the measures taken by the CDPC, on 4th February 1997 the Committee of Experts on Crime in Cyber-space (PC-CY) was set up by the Committee of Ministers with the decision No. CM/Del/Dec(97)583[299]. The role of this committee results to be pivotal in the history of the Budapest Convention, as it was the body that was appointed to draft an "international convention of cybercrime[300]". Two years later, on 27th May 1999, when the Budapest Convention was still a draft, it obtained the support of another international institution: the European Union. As a matter of fact, on that occasion the European Union required in its joint position that "Member States shall support the drawing up of the Council of Europe's draft Convention on Cyber Crime[301]".

One of the peculiar aspects about the drafting and negotiation process of the Budapest Convention, is the fact that not only CoE member States took part to it. Indeed, Canada, Japan, South Africa and United States participated in the negotiations as observers. However, the US observer state was merely formal. Indeed, they actively contributed to the drafting and the plenary sessions that led to the Budapest Convention. Experts report that such a behaviour was due to their longstanding experience in the field of cybercrime and its positions towards the issue deriving from such experience[302].

The treaty was to be finished and opened for signature by December of that same year, however negotiations were not concluded yet and that is why the mandate of the committee was postponed to 31st December 2000. Nonetheless, the extended term expired as well and the Draft Convention was submitted during the Plenary Assembly of October 2000 and it was finally adopted in April 2001, during the second part of the plenary session[303]. Before opening the treaty for signature, the Committee PC-CY decided to release the draft in April 2000, in order to allow the States that took part to

[298] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, pp. 56-59.
[299] Council of Europe Ministers' Deputies, *Decision No. CM/Del/Dec(97)583*, Strasbourg, 4th February 1997 https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168062dc73.
[300] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, p. 3, available at https://rm.coe.int/16800cce5b.
[301] Council of the European Union (1999), *Common Position 1999/364/JHA*, Official Journal of the European Communities, p. 1, available at https://op.europa.eu/en/publication-detail/-/publication/42be716f-31a9-444f-afe0-56c6929f78b3.
[302] Vatis, M. A. (2010) *The Council of Europe Convention on Cybercrime*, available at http://www.nap.edu/catalog/12997.html.
[303] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, available at https://rm.coe.int/16800cce5b.

the negotiation to consult with third parties that might be involved[304]. The last step of the drafting process took place during the 50th plenary session of the CDPC, with the submission of the draft of the Budapest Convention to the Committee of Ministers and finally the opening for signature of the legal instrument[305].

Ratification of the Budapest Convention is governed by articles 36 and 37 that open the fourth chapter of the Convention, which deals with miscellaneous provisions[306]. These two articles establish that the Budapest Convention can be ratified only by member States and non-member States could ratify it on condition that they had participated in the negotiation and drafting process[307]. However, this condition was to be in force only until the entry into force of the Convention, which was bound to five ratifications, of which at least three should be by member States[308]. As a matter of fact, from entry into force of the CoE Convention on Cybercrime, which occurred on 1st July 2004 with the ratification by Lithuania, this legal text can be accessed by non-member States that did not take part in the negotiation process as well. 'Accession' refers to those cases, in which a State is invited to become part of a treaty and accepts to be bound to it; therefore accession implies the same legal effects of ratification[309]. Such a decision, results to be pivotal in the field of cybercrime, just like in the field of cyberterrorism. This is because of the strong transnational character of the issue at stake, which we have already highlighted and which has been taken into consideration by the Council of Europe since the very first steps towards the Budapest Convention. As stressed in the first chapter, cyberspace is not only hard to define, but it is even harder to locate in space. Indeed, it has no well defined borders and as a consequence, the crimes that are committed against or through it, inherit the same trans-border character of cyberspace itself. For this precise reason, an international legal instrument that can be accessed solely by the members of a regional international organisation[310] would doubtlessly

[304] Ibid.
[305] Ibid.
[306] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425, available at https://btlj.org/?s=The+Council+of+Europe%27s+Convention+on+Cybercrime&submit=Search.
[307] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 36, par. 1, Budapest.
[308] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 36, par. 3, Budapest.
[309] To consult an official definition of 'accession' see United Nations Treaty Collection, *Glossary*, stable URL https://treaties.un.org/Pages/Overview.aspx?path=overview/glossary/page1_en.xml#:~:text=of%20Treaties%201969%5D-,Accession,treaty%20has%20entered%20into%20force, last accessed 18th July 2020.
[310] Membership to the Council of Europe is governed by Chapter 2 of the Statute of the Council of Europe. Articles 4 and 5 openly refer, as admissible members, to 'any European State' or 'European country' and they read as follows:

have limited effectiveness. However, as anticipated above, this is not the case of the Budapest Convention, since its entry into force. Indeed, from the year 2004 this legal instrument is no longer limited to a regional area, but potentially it can extend its value worldwide[311].

At the moment, the CoE Convention on Cybercrime has been ratified by 65 States. 44 of the States party to the Convention are members of the Council of Europe[312]. Two Coe Member States, Ireland and Sweden are not party to the treaty, but signatories, meaning that they agree on the content of the Convention and are committed to work towards its implementation, but they are not legally bound to it yet. On the other hand, the Russian Federation is neither party nor signatory to the Budapest Convention, despite admitting its concerns about terrorist, criminal and military-political threats that might arise in the field of cybersecurity[313]. This choice was due to the conviction that being bound to the Budapest Convention would undermine Russian sovereignty[314]. In addition to CoE member States that ratified the Budapest Convention, currently 21 non-

---

Article 4

Any European State which is deemed to be able and willing to fulfil the provisions of Article 3 may be invited to become a member of the Council of Europe by the Committee of Ministers. Any State so invited shall become a member on the deposit on its behalf with the Secretary General of an instrument of accession to the present Statute.

Article 5

a In special circumstances, a European country which is deemed to be able and willing to fulfil the provisions of Article 3 may be invited by the Committee of Ministers to become an associate member of the Council of Europe. Any country so invited shall become an associate member on the deposit on its behalf with the Secretary General of an instrument accepting the present Statute. An associate member shall be entitled to be represented in the Consultative Assembly only.

b The expression "member" in this Statute includes an associate member except when used in connexion with representation on the Committee of Ministers.

Council of Europe, *Statute of the Council of Europe*, art. 4 and 5, London, 5th May 1949, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680935bd0.

[311] Austin, G., & Gady, F. S. (2010) *Russia, the United States and Cyber Diplomacy: Opening the Doors*, East West Institute, available at https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

[312] The 65 High Contracting Parties include: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Switzerland, Turkey, Ukraine and United Kingdom.
Status as of 27th July 2020, Council Of Europe, *Chart of signatures and ratifications of Treaty 185*, stable URL https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=f1bIKBSP, last accessed 29th July 2020.

[313] Jerome, O. U. (2012) *Russia and the Council of Europe Convention on Cybercrime*, Computer and Telecommunication Law Review, pp. 16-17, available at https://www.researchgate.net/publication/322083052_Russia_and_the_Council_of_Europe_Convention_on_Cybercrime.

[314] Austin, G., & Gady, F. S. (2010) *Russia, the United States and Cyber Diplomacy: Opening the Doors*, East West Institute, available at https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

member States have ratified the Budapest Convention and[315] one non-member State, South Africa, is signatory to the Convention[316].

The Budapest Convention is classified as a criminal justice treaty and it "establishes criminal law measures based on rule of law and human rights principles[317]". The preamble states as a priority for the Convention the establishments of a common criminal policy, which is aimed at protecting society from crimes committed by means of and in the cyberspace[318], among which cyberterrorism is included. Such common policy shall be based on "appropriate legislation" and "international co-operation"[319]. In addition to that, the Convention aims at harmonising cybercrime legislation, establishing suitable mechanisms suitable to the cyber-environment and its peculiarities and guaranteeing prosecution of cybercriminals[320]

The Convention established substantive criminal law obligations as well as criminal procedure obligations, in addition to those regarding international cooperation. The convention includes 48 articles and it is divided into four chapters and this division mirrors the three main fields of action of the Budapest Convention.

The first chapter of the Convention, *Use of terms*[321], includes a relatively restricted number of definitions, which are considered to be particularly relevant for the ends of the Convention per se. The four definitions that are given in the first chapter are the ones of: computer system[322], computer data[323], service provider[324] and traffic data[325].

---

[315] The non-member States that ratified the Convention include: Argentina, Australia, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Israel, Japan, Mauritius, Morocco, Panama, Paraguay, Peru, Philippines, Senegal, Sri Lanka, Tonga and United States.
Status as of 27th July 2020, Council Of Europe, *Chart of signatures and ratifications of Treaty 185*, stable URL https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=f1bIKBSP, last accessed 29th July 2020.

[316] Ibid.

[317] Seger, A. (2012) *The Budapest Convention 10 years on: lessons learnt*, in Cybercriminality: finding a balance between freedom and security, ISPAC International Scientific and Professional, Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, edited by S. Manacorda, p. 168.

[318] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425, available at https://btlj.org/?s=The+Council+of+Europe%27s+Convention+on+Cybercrime&submit=Search.

[319] Council of Europe (2004) *Convention on Cybercrime – No. 185*, preamble, Budapest, p. 2, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[320] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425.

[321] Council of Europe (2004) *Convention on Cybercrime – No. 185*, chapter I – Use of terms, Budapest, p. 4.

[322] "'computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;" as stated in Council of Europe (2004) *Convention on Cybercrime – No. 185*, preamble, art. 1(a), Budapest, p. 4.

These definitions were selected on the basis of their utility with respect to the scope of the Convention and the fact that the CoE decided to limit the list of definitions to those that are considered to be essential for the purposes of this international legal instrument, might be attributed to the willingness to avoid a low rate of ratification, due to dissenting opinions on definitions.

The provisions of the second chapter, *Measures to be taken at national level*[326], deal with the measures that High Contracting Parties are required to implement in at domestic level, in order to comply with the Convention they ratified. That is why, the basic need for prosecution of a crime, is the presence of adequate substantive criminal law in the domestic system of all those States that arte party to the Convention[327]. This chapter is subdivided into three further sections, covering the topics of substantive criminal law, procedural law and jurisdiction.

Section I of chapter two provides member States with a list of conducts, which need to be considered as criminal offences under the domestic law of the High Contracting Parties. The offences are governed by articles from 2 to 10 and they comprehend: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to the infringements of copyright and related rights[328]. The offences covered by articles from 2 to 6 are classifies as "offences against confidentiality, integrity and availability of computer data and systems"; these provisions were outlined in order to prevent infringements of confidentiality, integrity or availability and they

---

[323]" "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;" as stated in Council of Europe (2004) *Convention on Cybercrime – No. 185*, preamble, art. 1(b), Budapest, p. 4.

[324] ""service provider" means:
i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;" as stated in Council of Europe (2004) *Convention on Cybercrime – No. 185*, preamble, art. 1(c), p. 4, Budapest.

[325] ""traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service." As stated in Council of Europe (2004) *Convention on Cybercrime – No. 185*, preamble, art. 1(d), Budapest, p. 4, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[326] Council of Europe (2004) *Convention on Cybercrime – No. 185*, chapter II – Measures to be taken at national level, Budapest, pp. 4-14.

[327] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

[328] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 2 through 10, Budapest.

shall not criminalise any of the legitimate actions that are related to this field[329]. Articles from 7 to 10 deal with computer-related offences. These offences are ordinary crimes that are committed with the aid of computer systems; meaning that despite the fact that there is no indispensable need for the use of ICT technology, they were still carried out by means of it. Such a situation implies the fact that most of the time member States already criminalise these conducts at domestic level; however, High Contracting Parties are required to verify if pre-existing provisions are suitable to deal with those cases, in which computer systems play a role in the perpetration of the crime[330]. Article 11 establishes that an individual can be held responsible for the aforementioned criminal offences only if the conduct was carried out intentionally or if an individual aided or abetted the commission of one of the aforementioned criminal offences[331]. In order to tackle the crimes established by articles 2 though 11, article 13 requires States to adopt "legislative and other measures" and specifies that these measure need to be based on the principles of effectiveness, proportionality and dissuasiveness[332].

Section II of the second chapter comprehends articles 14 to 21, which regulate procedural law, meaning that they establish how High Contracting Parties are bound to enforce the aforementioned articles and how to provide redress in case of infringement of one of them[333]. Article 14 opens this section outlining the scope of procedural provisions contained in the Convention and according to it, the first procedural obligation for member States is therefore to institute the powers and procedures that are needed to execute criminal investigations and proceedings. The aforementioned powers and procedures are not only to be adopted with respect to all those crimes covered by articles 2 to 11, but also with other criminal offences, provided that a computer system was deployed in commission of the illicit conduct[334]. Paragraph 2 b of article 14, therefore plays a pivotal role in our analysis. As a matter of fact, despite the lack of a broadly accepted definition of cyberterrorism, it has been recognised that the deployment of a computer system needs to be involved in the perpetration of the terrorist act in order to label it as cyberterrorism. For this precise reason, this paragraph

[329] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 43, Budapest, available at https://rm.coe.int/16800cce5b.
[330] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 79, Budapest.
[331] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 11, Budapest.
[332] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 13, Budapest, p. 8.
[333] Merriam-Webster, *Legal Definition of Procedural Law*, stable URL: https://www.merriam-webster.com/legal/procedural%20law, last accessed 11th August 2020.
[334] Council of Europe, (2004) *Convention on Cybercrime – No. 185*, art. 14, Budapest, pp. 8-9.

might allow the application of article 14 of the Budapest Convention to cyberterrorism. This issue will be further dealt with later on in this chapter. With respect to the powers and procedures that are to be established, implemented and applied according to article 14, article 15 clarifies that they must not prejudice the protection of human rights and liberties[335] and the principle of proportionality. Parties shall consider as common standard or minimum safeguard human rights included in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms[336] and its additional protocols No. 1, 4, 6, 7 and 12[337], the 1966 United Nations International Covenant on Civil and Political Rights[338] and other regional legal instruments regarding human rights[339]. The willingness to strike a fair balance between the protection of human rights and the measures that need to be taken to tackle the issue at stake[340], is thus once again highlighted.

According to the drafters, the framework for investigation and prosecution needs to take into consideration the ever-developing nature characterising the cyberspace and the volatility of whatever circulates inside it[341]. For this precise reason provisions 16 through 21 provide for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of stored computer data, real-time collection of traffic data and interception of content data[342]; in order to set a provisional framework that can be suitable for the peculiarities of the cyberspace compared to any other physical space. High Contracting Parties are required to establish the aforementioned procedures in order to render the process of investigation and prosecution more effective, considering the strong volatility of evidences in this field[343]. These mechanisms are to be applied to the cybercrime

[335] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 14, Budapest, p. 9.
[336] Council of Europe (1950) *Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.
[337] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 145, Budapest, p. 23.
[338] UN Genral Assembly (1996) *International Covenant on Civil and Political Rights*, available at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[339] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 145, Budapest, p. 23.
[340] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[341] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 134, Budapest, p. 21, available at https://rm.coe.int/16800cce5b.
[342] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art 16 through. 21, Budapest.
[343] Moise, A. C. (2017) *A few comments on the Council of Europe Convention on Cybercrime*, Journal of Law and Administrative Sciences, No. 8/2017.

offences included in the Convention, to any other crime committed by means of a computer system and to those cases in which evidence needs to be collected via ICT[344].

This section of the Convention aims at harmonising the investigative mechanism and the criminal proceeding in the field of cybercrime. Harmonisation results to play a crucial role when dealing with an issue, which is characterised by such a transnational nature. As a matter of fact, the accomplishment of an effective harmonisation would avoid the creation of the so-called 'safe heavens'. In the absence of harmonisation, some countries might decide not to criminalise certain conducts, inducing criminals to perpetrate their criminal acts there, simply by exploiting the fact that cybercrimes can be committed everywhere, disregard of the physical location of the perpetrator. Secondly, harmonisation allows for a better international cooperation, which is one of the pillars of this international legal instrument[345]. Moreover, the Budapest Convention executes the role of guideline for those States that are still outlining their national legislation in order to deal with cybercrime[346] and might need to look up for a concrete example of legislation.

The third and last section of chapter two establishes a loose set of rules[347], with which Parties are expected to assess jurisdiction over crimes committed in the cyberspace. However, the arduous topic of cyber-jurisdiction will be the object of the third and last chapter of this dissertation.

The third chapter of the Budapest Convention sets forth the framework for international cooperation. As previously anticipated, international cooperation and harmonisation of substantive and procedural law, are considered to be the most efficient way to tackle such a transnational phenomenon as cybercrime and, for the specific purposes of our analysis, cyberterrorism as well. The compelling need for international cooperation when facing the transnational threat of cybercrime and cyberterrorism was reiterated by the Council of Europe in its report on cyberterrorism, which stated:

[344] Vatis, M. A. (2010) *The Council of Europe Convention on Cybercrime*, available at http://www.nap.edu/catalog/12997.html.
[345] Clough, J. (2014) *A world of difference: the Budapest Convention on cybercrime and the challenges of harmonisation*, Monash University Law Review, Vol. 40, No. 3, available at https://www.researchgate.net/publication/277892666_A_World_of_Difference_The_Budapest_Convention_On_Cybercrime_And_The_Challenges_Of_Harmonisation.
[346] Ibid.
[347] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425.

> "The investigation and prosecution of most of these crimes is complex and challenging due to the technical nature of the Internet. Investigation and prosecution in this area require both adequate substantive criminal law provisions as well as adequate procedural capabilities[..]. In many cases, these phenomena have an international dimension, which may require concerted investigation in numerous countries. As a consequence, the prosecution and prevention of terrorist activities on the Internet depend to a great extent on the existence of appropriate international conventions and other instruments of international cooperation. These instruments must address the specific legal and forensic challenges posed by the Internet, they must make use of new Internet-based investigation techniques, and, at the same time, they must balance the need for effective prosecution against the obligation to protect citizens' civil liberties[348]".

As a matter of fact, international cooperation obligations are one of the three main branches that are covered by the provisions of the Convention, together with substantive criminal law obligations and criminal procedure obligations[349]. The need to guarantee efficient and effective international cooperation stems, once again, from the transnational nature of the crimes at stake. This peculiar nature implies the fact that a jurisdictional issue, which will be the object of the next and final chapter, needs to be faced and the solution that is provided by the Council of Europe with the Budapest Convention is precisely international cooperation.

When it comes to the specific instance of cyberterrorism, international cooperation, if possible, becomes even more crucial. As a matter of fact, as we have already highlighted, cyberterrorism combines two strongly transnational fields and, for this precise reason, the international cooperation obligations of the Budapest Convention might play a crucial role in the fight against cyberterrorism. To put it in the words of the CODEXTER, "the global cyber space provides a unique environment in which to carry out cyberterrorism and to pursue other international terrorist goals[350]".

Section I of the third chapter opens with article 23, addressing "general principles relating to international co-operation", which establishes that Parties shall cooperate in accordance with the provisions set by the Budapest Convention, "relevant international instruments on international cooperation in criminal matters, arrangements agreed on

[348] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing. p. 48.
[349] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[350] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, p. 47.

the basis of uniform or reciprocal legislation, and domestic laws[351]". Such cooperation shall be exerted "to the widest extent possible", for the processes of investigation and prosecution[352].

Article 24 regulates the matter of extradition and sets forth that an individual, who committed one of the crimes described in articles 2-11, can be extradited between States that are party to the convention; but only provided that the aforementioned crimes "are punishable under the law of both parties concerned by the deprivation of liberty for a maximum period of at least one year, or by a more severe penalty[353]". The drafters of the Convention decided to set this condition, because the illicit behaviours covered by articles 2 through 11 were not considered to be extraditable *per se*. For this precise reason, extradition can be demanded only for those crimes that can be punished with a maximum punishment of at least one year of deprivation of liberty[354].

A further aspect included in the framework for international cooperation is mutual assistance. High Contracting Parties "shall afford one another mutual assistance to the widest extent possible", when it comes to investigation, proceedings or collection of evidence. In the spirit of mutual assistance, States party to the Budapest Convention are allowed and encouraged to share information they have collected through their investigation with other High Contracting Parties[355].

Section two of the third chapter addresses specific provisions related to international cooperation, in order "to provide for specific mechanisms in order to take effective and concerted international action in cases involving computer-related offences and evidence in electronic form[356]". As a matter of fact, articles 29 through 35 regulate: the expedited preservation of stored computer data, the expedited disclosure of preserved traffic data, mutual assistance regarding accessing of stored computer data, trans-border access to stored computer data with consent or where publicly available, mutual assistance in real-time collection of traffic data, mutual assistance regarding the interception of content data and the so-called '24/7 Network'[357]; which consist on a

[351] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 23, Budapest, p. 14.
[352] Ibid.
[353] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 24, Budapest, p. 14.
[354] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 245, Budapest, p. 42, available at https://rm.coe.int/16800cce5b.
[355] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 26, Budapest, p. 16.
[356] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 281, p. 50, Budapest.
[357] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 29 through 35.

contact point that needs to be always available, in order to provide immediate assistance to other Parties. The measures set forth by these provisions play a pivotal role in the fight against cybercrime in general, and cyberterrorism in our specific case. That is why, as anticipated above, cyberspace is probably the most volatile environment at the moment and, for this precise reason, new measures that take into consideration this peculiar feature need to be established[358].

The last chapter of the CoE Convention on Cybercrime consists of miscellaneous provisions that are usually part of all CoE legal instruments[359].

2.3 Assessing the applicability of the Council of Europe Convention on Cybercrime – CETS No. 185 to cyberterrorism

After providing an overview of the CoE Convention on Cybercrime, focusing on its drafting process, its goals and its structure, we will now go more into depth analysing how existing legal instruments can be applied to the field of cyberterrorism. We will evaluate how an international legal instrument, that was outlined to address the broad problematic of cybercrime, could be used to tackle cases of cyberterrorism and to which extent it can actually be of use.

The experts of CODEXTER analysed in their report on cyberterrorism and the use of internet for terrorist purposes, which we have already mentioned along this dissertation, how already existing international legal instruments could be used to tackle cases of cyberterrorism.

First of all, it can be claimed that the very first prerequisite for an effective prosecution of cyberterrorism is the presence, at national level, of suitable substantive criminal law provisions. These provisions need to be able to cover the possible acts that might be involved in the case of a cyberterrorist attack[360]. Though we have already stated that, at the moment, there is no international legal instrument addressing cyberterrorism, a part of the criminal behaviours that could be used to carry out such attacks are contemplated by the CoE Convention on Cybercrime.

[358] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art 16 through. 21.
[359] Council of Europe, (2004) *Convention on Cybercrime – No. 185*, art. 36 through 48, Budapest, p. 25.
[360] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

In the light of this acknowledgment a pattern was developed by CODEXTER in order to analyse how to apply already existing provisions to possible cases of cyberterrorist attacks. The pattern assumes that the results of a hypothetical attack could be classified in three different levels. The primary results regard the mere interference with data, which is considered to be the prerequisite for all kinds of attacks in the cyberspace. It can either consist on circumvention of integrity, confidentiality or availability of computer systems or data. The secondary results can be split into two sub-categories: the first one is digital damage, and it comprehends those cases in which the damages or destruction happen on the cyberspace; while the second one is physical damage, and it includes all those cases in which the target in the cyberspace had any kind of link to the physical world (for examples of the most plausible scenarios, see par. 1.1(d)). The third result refers to the terrorist intention per se, in other words the *mens rea* underlying the attack. As it emerged from the analysis of the first chapter there is no universally agreed definition of terrorism, but there seems to be a considerable degree of consensus on what constitutes a terrorist intent: the willingness to achieve a political, social or economic change, by means of violence and the spread of fear[361].

On the basis of this analytical pattern, the CODEXTER concluded that instances ranging from primary results to the first category of secondary results, which is digital damage, can be tackles using IT-based regulations, such as the CoE Convention on Cybercrime. On the other hand, for those offences that are included in the second category of the secondary results, which is physical damage, and the third result terrorist-specific legal instruments can be triggered as well. Thus, a dual approach can be used: IT-based approach for those cases in which the focus is on the harm to data; and "corporeal damage approach" or "terrorist-specific" approach for those cases in which the focus is on the physical harm and intent[362]. An instance of the application of this approach is the reasoning we followed in the brief overview of the UN framework to counter terrorism, outlined at the beginning of this chapter. For this precise reason, conceiving the application of pre-existing international legal instruments to cases of cyberterrorism is possible, though the evaluation on whether they can suffice or not will take place on the conclusion of this chapter.

[361] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.
[362] Ibid.

After demonstrating the conceivability of the application of existing CoE instruments to cases of cyberterrorism, we will now proceed to an analysis of the articles of the Budapest Convention that result to be the most relevant for the purpose of tackling the threat at stake.

As illustrated in the previous paragraph, articles 2 through 13 constitute the substantive criminal law provisions of the Convention and cyberterrorism is clearly not included among them[363]. However, these provisions include criminal behaviours that are considered to be prerequisites for a terrorist attack carried out by means of ICT.

Article 2 of the Convention addresses illegal access and criminalises the intentional "access to the whole or any part of a computer system without right[364]". With the expression "without right" the Treaty makes reference "to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law[365]". This illicit behaviour needs to be perpetrated with the intent to obtain "computer data or other dishonest intent[366]". It can be claimed that this requirement is in line with the aims pursued by cyberterrorists, that can be included under the wording "other dishonest intent". Cyberterrorists are expected to use illegal access, which generally takes the form of hacking as explained in the first chapter, to overcome security measures put in place in order to protect a computer system. For this precise reason, article 2 of the Budapest Convention can be applied to one of the preparatory actions to the commitment of a cyberterrorist attack[367].

A further act, which is considered to be preparatory to the striking of a cyberterrorist attack, is illegal interception. This conduct is criminalised by article 3 of the Convention, that classifies interceptions as illegal when it is executed "without right, made by technical means, of non-public transmission of computer data to, from or within a computer system[368]". In this case, the underlying intention needs to be exactly

[363] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 453-464.
[364] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 2, Budapest, p.4.
[365] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 38, Budapest, p. 8.
[366] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 2, Budapest, p.4.
[367] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, pp. 52-55.
[368] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 3, Budapest.

the same one of art. 2 and, as a consequence the abovementioned reasoning applies to this article as well. Illegal interception, just like illegal access, belongs to the illicit acts that constitute the early stages of the commission of a cyberterrorist attack and that are considered to be preparatory to it[369]. As a consequence, it can be claimed that articles 2 and 3 of the Convention would apply to cases of cyberterrorism and, despite not including in their wording the terrorist *mens rea*, they still grant coverage to the preparatory acts of an attack.

Moving on from the preparatory acts to the acts that constitute a "prerequisite for terrorist attacks on computer systems carried out by means of internet[370]", it can be claimed that articles 4, 5 and 6 address this more advanced stage of the cyberterrorist attack. As a matter of fact, article 4 of the Budapest Convention criminalises data interference, which is defined as "the damaging, deletion, deterioration, alteration or suppression of computer data without right[371]". Clearly, all the operations contemplated by article 4 result to be of use for commission of one of the scenarios depicted in the first chapter. Most important, article 5 on system interference extends the purposes of the previous article by criminalising system interference as well. By system interference it is meant "the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data[372]". Therefore article 5 plays a crucial role in our analysis, because it allows to cover not only those IT-based attacks directed against computer systems, but also interferences targeting "infrastructures, physical property, life or well-being of persons[373]". As a matter of fact, the wording of article 5 is "neutral", precisely in order to protect "all kinds of function[374]". In the light of this acknowledgment it can be claimed that "all types of terrorist attacks against computer systems fall under articles 4

[369] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, pp. 52-55.
[370] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, p. 52.
[371] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 4, Budapest, p.5
[372] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 5, Budapest, p. 5.
[373] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, p. 52.
[374] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, note 65, Budapest, p. 12.

and 5[375]". The acts preparatory to the intrusion addressed by articles 4 and 5 are covered by article 6 on misuse of devices. This provision sets forth the criminalisation of:

> "[..] the production, sale, procurement for use, import, distribution or otherwise making available of (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent the it be used for the purpose of committing any of the offences established in Article 2 through 5[..][376]".

To recall the scenarios we analysed in the first chapter and to mention a concrete instance, we can note how in case of the deployment of a DDoS in the commission of a cyberterrorist attack, article 6 can be triggered, as the a computer program aimed at the perpetration of crimes set forth by articles 2 through 5 is involved. In addition to that, the possession of the aforementioned devices or computer password with the intent to use them for the carrying out of one of the conducts criminalised by article 2 through 5 constitutes an offence under article 6 as well[377]. In the light of that, we can conclude that articles 4, 5 and 6 could be applied to cases of cyberterrorism and that the offences that they set forth address those conducts that constitute the preliminary stages of a cyberterrorist attack, meaning that in the absence of these passages no attack would be possible.

The aforementioned provisions are extended in scope by articles 11 and 13. According to article 11, an individual can be convicted of the infringement of articles 2 through 10 of the Convention also in case of "aiding or abetting" and attempting the commission of such crimes[378]. This article is relevant because it allows to condemn individual who contributed to the striking of a cyberterrorist attack, but also it allows the conviction of individuals responsible for failed attempts. Considering that we are dealing with terrorist actors, who might be working in the framework of a terrorist organisation, this provision plays a crucial role. As a matter of fact, it would allow to plea as guilty also those individuals that were connected in some way to the perpetration of the cyberterrorist attack, for example by being part of the same terrorist organisation.

[375] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, p. 53.
[376] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 6, par. 1(a), Budapest, p. 5.
[377] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 6, par. 1(b), Budapest.
[378] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 11, Budapest, pp. 6-7.

Article 13, the last of the substantive provision of the Convention, requires High Contracting Parties to establish sanctions to punish conducts set forth by articles 2 through 11, provided that these sanctions are based on the principles of effectiveness, proportionality and dissuasiveness. Sanctions contemplated by article 13 include both monetary sanctions and the deprivation of liberty[379]. The principles that are set forth as the basis for the sanctioning of crimes can be considered as suitable for the issue at stake. As a matter of fact, effectiveness, proportionality and especially dissuasiveness would play a crucial role in the fight against cyberterrorism. Proportionality can be granted also in the case of the extension of the Budapest Convention to cyberterrorism, due to the fact that deprivation on liberty is contemplated as sanction.

In addition to the substantive criminal law provisions analysed so far, there other two relevant articles, namely art. 7 and 8, which address computer-related forgery and fraud. As a consequence, they could apply to all those scenarios depicted in chapter one in paragraph 1.2 (d). As a matter of fact, the articles at stake obviously refer to forgery and fraud carried out by a cyber means and therefore they result to be relevant for the matter at stake. In the opening of our analysis of the field of cyberterrorism, we referred to these illicit acts as "cyberterrorist support", as they are considered to be predicate offences to the commission of a cyberterrorist act. Article 7 establishes that if the "input, alteration, deletion or suppression of computer data" perpetrated without right results into "inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic[380]", such conduct constitutes the crime of computer-related forgery. As far as computer-related fraud is regarded, article 8 sets forth the criminalisation of "(a) any input, alteration, deletion or suppression of computer data; (b) any interference with the functioning of computer system, with fraudulent or dishonest intent of producing, without right, an economic benefit for oneself or for another person[381]". The wording used in this article allows to tackle those cases in which cyberfraud is used for the purposes of financing a cyberterrorist attack, both if committed by an individual or by a terrorist organisation.

Moving on to the procedural law provisions of the Convention (Art. 14-21), it can be noted that they have a broad scope and, for this precise reason, cyberterrorism is potentially covered by them. Most important, as previously anticipated, article 14 states

[379] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 13, Budapest, p. 8.
[380] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 7, Budapest, p. 6.
[381] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 8, Budapest, p. 6.

in paragraph 2 that the powers and procedures that High Contracting Parties are required to establish in order to guarantee effective criminal investigation and proceeding apply to "(a) the criminal offences established in accordance with Articles 2 through 11 of this Convention; (b) other criminal offences committed by means of a computer system; and (c) the collection of evidence in electronic form of a criminal offence.[382]" Thus, as anticipated, the wording of paragraph 2 (b) allows for an interpretation of procedural law provisions of the Budapest Convention that enables the inclusion of cyberterrorism[383], as it belongs to offences committed by means of computer systems.

Finally, the same reasoning can be followed for the third chapter of the Convention, which establishes the framework for international cooperation. As a matter of fact, article 23 sets forth that States party to the Treaty "shall co-operate with each other [..] to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence[384]". This wording allows to apply article 23 to any kind of criminal offences involving computer systems and data, among which cyberterrorism is included[385]; thus allowing to apply the entire framework for international cooperation to cases of cyberterrorism.

2.4 An overview of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – ETS No. 189

On 21st January 2003, the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of racist and xenophobic nature committed through computer systems was opened to signature in Strasbourg. It entered into force 3 years later on 1st March 2006, when the clause of a minimum of 5 ratifications was fulfilled. To date[386], 29 CoE Member States have ratified the Additional Protocol[387].

[382] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art.14, Budapest, pp. 8-9.
[383] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 453-464.
[384] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 23, Budapest, p. 14.
[385] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 453-464.
[386] Council of Europe, *Chart of signatures and ratifications of Treaty 189*, stable URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=Q8wGkgaa, last accessed 10th August 2020.

Needless to highlight that the Additional Protocol to the Convention of Cybercrime has a lower rate of ratification that the Convention per se. As far as non-Member States are concerned, the Additional Protocol No. 189 counts 3 ratifications, indeed by Morocco, Paraguay and Senegal; while Canada and South Africa are signatories to the protocol[388].

The Additional Protocol was drafted due to the fact that "[…] the emergence of international communication networks like the Internet provide certain persons with modern and powerful means to support racism and xenophobia and enables them to disseminate easily and widely expressions containing such ideas[389]".

The choice to address such an issue in a separate protocol and not to include it in the text of the Budapest Convention was taken due to disagreements among the Parties on the criminalisation of racist and xenophobic acts[390]. The scope of the Additional Protocol is "to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as "the Convention"), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems[391]".

The Additional Protocol is based on all the provisions of the Budapest Convention, maintaining its framework for substantive and procedural law and international cooperation. However, it aims at widening the Convention's purpose to the spread of racist and xenophobic material. The definition of "racist and xenophobic material" is

---

[387] The member States that ratified the Convention include: Albania, Andorra, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Latvia, Lithuania, Luxembourg, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, San Marino, Serbia, Slovenia, Spain and Ukraine. While 11 of the remaining Member States are signatories to the Additional Protocol and they include: Austria, Belgium, Estonia, Iceland, Italy, Liechtenstein, Malta, Slovak Republic, Sweden, Switzerland and Turkey.
Council of Europe, *Chart of signatures and ratifications of Treaty 189*, stable URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=Q8wGkgaa, last accessed 10th August 2020.

[388] Ibid.

[389] Council of Europe (2006) *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, note 3, Strasbourg, p. 1, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016 80989b1c.

[390] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

[391] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, art. 1, Strasbourg, p. 2, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

provided by article 2 of the Additional Protocol, which, together with article 1, constitutes the first chapter of this legal instrument. The definition is the following:

> "(1) For the purposes of this Protocol: "racist and xenophobic material" means 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[392]".

States that are party to the Additional Protocol are required in chapter two to criminalise at national level the following illicit conducts: dissemination of racist and xenophobic material through computer systems; racist and xenophobic motivated threat; racist and xenophobic motivated insult; denial, gross minimisation, approval or justification of genocide or crimes against humanity and aiding and abetting the commission of the aforementioned crimes[393].

Chapters three and four respectively regulate the relations between the Convention on Cybercrime and its protocol and miscellaneous provisions common to most CoE treaties.

2.5 Assessing the applicability of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – ETS No. 189 to cyberterrorism

After taking into consideration the cyberterrorist financing by means of cyberfraud in the previous section, the evaluation on the applicability of the Additional Protocol to the Convention on Cybercrime takes us back to another support activity that has been taken into consideration during the first chapter: propaganda and threats (see par. 1.2 (b)). As far as this phenomenon is concerned, the CODEXTER affirmed that:

> "With respect to terrorism, the provisions of this Protocol are relevant to threats and insults committed with the intent to incite conflicts and violence between groups distinguished by race, colour, or national or ethnic origin. The provisions are directed at

[392] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, art. 2, Strasbourg, p. 2
[393] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, art. 3-7, Strasbourg.

> IT-based content and are therefore also applicable to the use of the Internet for terrorist purposes[394]".

Article 3 criminalises the dissemination of racist and xenophobic material by means of computer systems[395]. This is an article suitable to address the cyberterrorist support activity of propaganda; while article 4 on racist and xenophobic motivated threat committed through computer systems[396] and article 5 on It-based racist and xenophobic motivated insult[397] can be triggered in the instance of the diffusion of threats. As a matter of fact, article 4 sets forth that the message conveyed by means of ICT needs to be the threat of "the commission of a serious criminal offence", among which cyberterrorism could be included. We say "could be included" because article 4 also specifies "as defined under its domestic law", referring to the fact that such "serious criminal offence" should be criminalised at national level. Therefore, article 4 could be triggered solely in two cases: either cyberterrorism is considered as a manifestation of terrorism and therefore included in the broad criminalisation of it; or the crime of cyberterrorism is specifically established. To date there is no solution to this situation, only the development of this doctrine will allow us to solve this issue.

2.6 An overview of the Council of Europe Convention on the Prevention of Terrorism – CETS No. 196

The second pillar, which cyberterrorism builds upon is clearly terrorism. The CoE international legal instrument addressing terrorisms that results to be the most relevant for the purposes of our analysis is the European Convention on the Prevention of Terrorism (CECPT). We will now proceed to an overview of the Convention and subsequently, we will take into account the possible application of this Treaty to instances of cyberterrorism.

In the aftermath of the 11th September 2001 terrorist attack in New York, the international community felt the need to question the effectiveness of the international

[394] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, p. 70.
[395] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, art. 3, Strasbourg, pp. 2-3.
[396] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, art. 4, Strasbourg, p. 3.
[397] Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, art. 5, Strasbourg, p. 3.

legal instruments dealing with terrorism that were available at the moment[398]. The opinion of the Council of Europe Committee of Experts on Terrorism on this matter was that "an instrument, or instruments, with limited scope, dealing with the prevention of terrorism and covering existing lacunae in international law or action, would bring added value[399]" to the already existing international framework addressing terrorism. For this precise reason, the CECPT was drafted and opened for signature on 16th May 2005 by Member States, the European Union, non-Member States that took part in its elaboration and it was opened for accession by non-Member States. The CECPT entered into force on 1st June 2007, when the condition set forth by article 23 was fulfilled reaching the threshold of six ratifications, four of which needed to be by Member States. To date the Convention counts 39 ratifications by Member States 8 signatures by Member States: Belgium, Georgia, Greece, Iceland, Ireland, San Marino, Switzerland and United Kingdom; and the ratification of the European Union[400].

The CECPT does not provide a definition of terrorism; but rather article 1 makes reference to the UN sectoral instruments addressing the manifestations of terrorism, stating that ""terrorist offence" means any of the offences within the scope of and as defined[401]" in one of these international legal instruments[402].

---

[398] Hunt, A. (2007) *The Council of Europe Convention on the Prevention of Terrorism*, European Public Law 603, Vol. 12, No. 4, available at https://www.researchgate.net/publication/228209564_The_Council_of_Europe_Convention_on_the_Prevention_of_Terrorism.

[399] Council of Europe (2007) *Explanatory Report to the Convention on the Prevention of Terrorism – CETS No. 196*, note 11, Warsaw, p. 2.

[400] The member States that ratified the Convention are: Albania, Andorra, Armenia, Austria, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, Russian Federation, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Turkey and Ukraine.
Council of Europe, *Chart of signatures and ratifications of Treaty 196*, last accessed 22nd August 2020, stable URL https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196/signatures?p_auth=AbrF0dEE.

[401] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 1, Warsaw, p. 2.

[402] The CECPT precisely makes reference to: Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on 16 December 1970; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, concluded at Montreal on 23 September 1971; Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, adopted in New York on 14 December 1973; International Convention Against the Taking of Hostages, adopted in New York on
17 December 1979; Convention on the Physical Protection of Nuclear Material, adopted in Vienna on 3 March
1980; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, done at Montreal on 24 February 1988; Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, done at Rome on 10 March 1988; Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf,

Unlike the previous CoE instrument addressing terrorism, the European Convention on the Suppression of Terrorism[403], the CECPT is remarkably outlined on a preventive level, criminalising those behaviours that facilitate and are preparatory to the strike of a terrorist attack[404]. As a matter of fact, "The Convention does not define new terrorist offences in addition to those included in the existing conventions against terrorism. [..] However, it creates three new offences which may lead to the terrorist offences as defined in those treaties[405]".

The purpose of the Convention is "to enhance the efforts of Parties in preventing terrorism and its negative effects on the full enjoyment of human rights, in particular the right to life[406]" and such aim should be reached both by the implementation at national level of the provisions included in the Convention and by enforcing effective international cooperation among States party to this international legal instrument.

Once again we can notice how international cooperation is deemed to be necessary when dealing with a transnational issue; as a matter of fact it is considered to be pivotal in order to better achieve effective prevention of terrorism; just like it was deemed to be pivotal in order to tackle cybercrime. As a matter of fact, the framework for international cooperation is laid down by article 4, which requires Parties to "assist and support each other with a view to enhancing their capacity to prevent the commission of

---

done at Rome on 10 March 1988; International Convention for the Suppression of Terrorist Bombings, adopted in New York on 15 December 1997; International Convention for the Suppression of the Financing of Terrorism, adopted in New York on 9 December 1999; International Convention for the Suppression of Acts of Nuclear Terrorism, adopted in New
York on 13 April 2005 (*).
Council of Europe, (2007) *Appendix – Council of Europe Convention on the Prevention of Terrorism*, Warsaw, available at https://rm.coe.int/168008371b.

[403] Council of Europe (1978), *European Convention of the Suppression of Terrorism*, ETS No. 90, Strasbourg, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800771b2.

[404] Hunt, A. (2006) *The Council of Europe Convention on the Prevention of Terrorism*, European Public Law 603, Vol. 12, No. 4, available at https://www.researchgate.net/publication/228209564_The_Council_of_Europe_Convention_on_the_Prevention_of_Terrorism.

[405] Council of Europe (2007) *Explanatory Report to the Convention on the Prevention of Terrorism – CETS No. 196*, Warsaw, note 32, p. 5, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3811.

[406] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 2, Warsaw, p. 2.

terrorist offences, including through exchange of information and best practices, as well as through training and other joint efforts of a preventive character[407]".

Articles 5 though 7 constitute the core substantive criminal law provision of the Convention and they create the three new offences mentioned in the Explanatory Report, which are considered to be criminal behaviours that facilitate and lead to the commission of terrorist acts. The new offences introduced by the CECPT are public provocation to commit a terrorist offence, recruitment for terrorism and training for terrorism[408]. We will proceed to their detailed analysis in the next paragraph.

Articles 11 through 13 constitute the procedural law provisions of the Convention, requiring High Contracting Parties to establish "effective, proportionate and dissuasive measures" to counter the criminal conducts set forth by articles 5 through 7[409]; provided that the criminalisation of conducts under articles 5, 6, 7 and 9 does not hinder the respect of human rights obligations[410]. Finally, article 13 requires High Contracting Parties to protect, compensate and support victims of terrorism and their close relatives. It is a State's responsibility to fulfil the previous requirement when the terrorist attack was committed inside its territory[411].

Jurisdiction over the crimes laid down by the CECPT is addressed by article 14, while one of the aspects of due diligence is addressed by article 15, setting forth that High Contracting Parties have the obligation to investigate facts, once informed that an individual inside their territory has been alleged of one or more offences under articles 5 though 7[412]. The framework for international cooperation is regulated by articles 17, 18, 19 and 22 respectively addressing international co-operation in criminal matters, extradition or prosecution, extradition and spontaneous information[413]. Articles 20 and

terrorist offences and offences set forth in this Convention." See Council of Europe, (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 3, Warsaw, p. 2.

[407] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 4, Warsaw, p. 2.

[408] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 7, Warsaw, p. 3.

[409] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 11, Warsaw, p. 4.

[410] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 12, Warsaw, p. 4.

[411] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 13, Warsaw, p. 5.

[412] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 15, Warsaw, p. 6.

[413] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 17, 18, 19 and 22, Warsaw.

21 on the exclusion of the political exception clause and the discrimination clause are aimed at widening and updating the scope of the European Convention on the Suppression of Terrorism, due to the differences between the current historical context and 1977, the year in which the Convention was opened for signature. Finally, articles 23 though 32 cover miscellaneous provisions common to most CoE treaties.

2.7 Assessing the applicability of the Council of Europe Convention on the Prevention of Terrorism – CETS No. 196 to Cyberterrorism

The new offences established by the CECPT, just like the ones we have analysed so far, have an effect on the second category of cyberterrorism we analysed during the first chapter: the one that is referred to by academics as cyberterrorist support activities (see par. 1.2). The cyberterrorist activities that are covered respectively by articles 5, 6 and 7 of the present Convention are provocation to commit a terrorist offence, recruitment and training for terrorism (see par. 1.2 (b – c)).

According to the analytical report by the CODEXTER in the case of the commission of a cyberterrorist support act, the aforementioned article contained in the CECPT could be trigger. The wording of these provisions does not require that public provocation, recruitment and training are committed by means of ordinary ways, such as documents or personal contact.

As a matter of fact, article 5 criminalised 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, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed[414]". As anticipated, there is no reference to the fact that the process of "distribution, or otherwise making available" should be carried out in a specific way. Thus, the instances related to propaganda and threat we analysed in the first chapter are covered by article 5 of the CECPT, due to the fact that the wording of the article at stake does not hinder its application to conducts carried out in the cyberspace.

As far as recruitment of new terrorist actors is regarded, article 6 requires High Contracting Parties to criminalise the conduct aimed at soliciting "another person to commit or participate in the commission of a terrorist offence, or to join an association

[414] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 5, Warsaw, p. 3.

or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group[415]". Also in this case there is no condition on the means through which the act of soliciting should take place, in order to trigger article 6. Thus, it can be claimed that the cyberterrorist support activity of IT-based recruitment is covered by the CECPT as well, allowing to use the Budapest Convention in order to address this activity of support to cyberterrorism.

Finally, by "training for terrorism" article 7 means "to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose[416]". Also the wording of this article does not hinder its application to instances in which the instructions are provided by means of computer systems. In addition to that, due to the expression "other specific methods or techniques", it can be claimed that instructions on how to exploit the cyberspace in order to commit a cyberterrorist attack are contemplated by article 7, together with traditional methods, such as "explosives, firearms or other weapons".

For this precise reason, it can be claimed that all the substantive criminal law provision of the CECPT are suitable to cover the illicit activities that "lead to terrorist offences[417]", also in those cases in which the offences are committed by means of computer systems[418].

Furthermore, the substantive criminal law provisions are extended in their purpose by the following articles. Article 8 on the 'Irrelevance of the commission of a terrorist act' establishes that for an individual to be convicted of the aforementioned offences, there is no need for the actual commission of any terrorist act[419]. This means that there is no need for the actual cyberterrorist attack to take place, its planning is considered to be

[415] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 6, Warsaw, p. 3.
[416] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 7, Warsaw, p. 3.
[417] Council of Europe (2007) *Explanatory Report to the Convention on the Suppression of Terrorism – CETS No. 196*, Warsaw, note 32, p. 5, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3811.
[418] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing, p. 70.
[419] Council of Europe (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 8, Warsaw, p. 3.

enough in order to trigger article 8. Such a provision plays a pivotal role in the field of cyberterrorism, due to the fact that it allows a preventive approach to the matter. Considering the highly detrimental effects that could be brought by a cyberterrorist attack, such an approach would be the most suitable one to the issue. On top of that, article 9 on 'Ancillary offences' widens the previous provision to those individuals who intentionally participated, organised or directed others and contributed to the offences set forth by articles 5 through 7[420]. Once again, the convention does not specify the means through which such participation, organisation or direction shall take place; thus, the instances in which they are carried out by means of ICT can be included.

2.8 The Stanford Draft: "A Proposal for an International Convention on Cyber Crime and Terrorism"

After analysing the two most relevant CoE international legal instruments for the purpose of evaluating their applicability to instances of cyberterrorism, we will now proceed to the presentation of a Draft of International Convention outlined to explicitly address cyberterrorism.

In August 2000, when the CoE Convention on Cybercrime was on its final drafting stages, "A Proposal for an International Convention on Cyber Crime and Terrorism" was outlined by a group of experts of Stanford University. This academic text is also known as the "Stanford Draft" and builds upon the Budapest Convention. However, it differs from it due to the fact that its aim is to specifically address cyberterrorism and not to tackle the broad field of cybercrime[421].

During a meeting organised by the Hoover Institution, in collaboration with the Consortium for Research on Information Security and Policy (CRISP) and the Center for International Security and Cooperation (CISAC) held on 6th and 7th December 1999 at Stanford University, known as the "Stanford Conference", the aforementioned group of experts agreed on the fact that terrorists have taken a lot of steps forward in the exploitation of the cyberspace for their ends; while law has neglected these

[420] Council of Europe, (2007) *Convention on the Prevention of Terrorism – CETS No. 196*, art. 9, Warsaw, pp. 3-4.
[421] Cohen, A. (2010) *Cyberterrorism: Are We Legally Ready?*, Journal of International Business and Law, Vol. 9, No. 1, pp. 34-35.

developments[422]. This was the purpose underlying this academic project, which is made explicit in the very beginning of the Draft. This academic text never converted into a legal instrument, still it is an important example of the perspective of those academics believing that existing legal instruments are not sufficient to tackle the issue of cyberterrorism.

The group of experts who outlined the Stanford Draft justify the choice of a multilateral approach on the basis of a few acknowledgments. First of all, as previously stated in this dissertation, it is acknowledged that cyberterrorism is a transnational issue and therefore needs to be dealt with international legal instruments; tackling it exclusively at national level would result into a pointless struggle. On top of that, the possibility for criminals to exploit the legislative gaps of some countries exposes the entire international community to the threat of cyberterrorism. Such condition is a further justification for the choice of the international approach towards the tackling of cyberterrorism. Moreover, as ICT becomes more and more complex, prearranged and effective solutions are more and more needed. In the light of this acknowledgment, the Stanford Draft proposes the institution of an international agency that should serve as international forum aimed at discussion among Parties, in order to allow them to deal with tackle technological development and afford each other mutual assistance in real-time[423].

Contrary to the cases we have taken into analysis so far, the Stanford Draft provides us with a definition of cyberterrorism. Such definition, which we have already analysed in the first chapter, is contained in Article 1. This article includes several definitions, some of which are included in existing international legal instruments, while others, such as *cyberterrorism* or *critical infrastructures* are not. The Draft states that it should be criminalised as cyberterrorism the "intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic

[422] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, pp. 25-45, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf.
[423] Ibid.

harm;[424]". Though in a synthetic way, we can note that the core elements of the definition of terrorism given by the UN Draft Comprehensive Convention on International Terrorism, which is considered to be a "consolidated" one, are included. However, it needs to be pointed out that it is not made explicit that "death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm[425]" needs to be caused with the aim to intimidate a population or compel a Government to act in a specific way.

Among the other definitions provided by the Stanford Draft, the definition of "critical infrastructures" results to be of particular interest for the purposes of our analysis. As a matter of fact, as it emerged from the analysis of the first chapter, the kind of cyberterrorist attack that is likely to produce the most harm to society is precisely the one that targets IT infrastructures that control the so-called "critical infrastructures". According to this Proposal for an International Convention:

> "critical infrastructures" are the interconnected networks of physical devices, pathways, people and computers that provide for timely delivery of government services; medical care; protection of the general population by law enforcement; firefighting; food; water; transportation services, including travel of persons and transport of goods by air, water, rail or road; supply of energy, including electricity, petroleum, oil and gas products; financial and banking services and transactions; and information and communications services;[426]"

What is noteworthy about this definition is the fact that it covers all possible scenarios we described at the beginning of this dissertation. In the light of these acknowledgements, it can be claimed that despite the fact that the text at stake is an academic draft, these two definitions could be considered as a good starting point for the discussions about the drafting of the legal ones.

As previously said, the Stanford Draft was laid down on the basis of the CoE Convention on Cybercrime and that can easily be noted when moving on to its substantive criminal law provisions. As a matter of fact, if we take into analysis article 3, which sets forth the offences that should be criminalised by High Contracting Parties,

[424] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 1, par. 2, p. 26, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf.
[425] Ibid.
[426] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 1, par. 2 and 7, p. 26.

we can infer a correspondence with some of the crimes established by the Budapest Convention. Thus, we will now consider the offences that were outlined on the basis of existing CoE provisions.

First of all, all conducts included in article 3 need to be carried out intentionally and without right in order to be considered as a criminal behaviour. Such condition corresponds with the requirements of the CoE Convention on Cybercrime. Moving on to paragraph (a) of article 3, it is stated that an act should be criminalised when it "creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system[427]" with the aim of hindering the functioning of a cyber system or of forcing it to perform illegal functions disregard of the willingness of its owner. This first offence could be related to articles 4 and 5 of the Budapest Convention on data and system interference. Furthermore, paragraph (c) builds upon article 2 of the Budapest Convention, establishing the offence of illegal access. As far as misuse of devices is concerned, which in the CoE text is governed by article 6, it can be claimed that the same conduct is criminalised in the Draft by paragraph (e), which refers to the manufacturing, selling, use, posting or distributing of devices or programs aimed at the commission of one of the offences set forth by articles 3 and 4. Finally, article 4, just like article 11 of the Budapest Convention, establishes as offence also the attempting, aiding or abetting, and conspiring to commit one of the crimes included in article 3.

In addition to the offences that build upon the ones previously established by the Budapest Convention, the Stanford Draft proposes a set of new offences in order to better address cyberterrorism; which we will now proceed to analyse.

Paragraph (b) of article 3 of the Stanford Draft establishes as an offence the creation, storage, alteration, deletion, transmission, diversion, misrouting, manipulation or interference with data in the cyberspace, when it is intended to provide "false information in order to cause substantial damage to person or property[428]". Such a provision would be relevant in order to prevent the fulfilment of the scenarios depicted in paragraph 1.1 of this dissertation. In addition to that, the Draft criminalises the

[427] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford,. 3 (a), p. 27.
[428] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 3 (b), p. 27.

interference with "tamper-detection or authentication mechanisms[429]". Such provision is less broad than the criminalisation of illegal access, as it specifically addressed to those mechanisms aimed at sensing an active attempt to compromise the device or its data[430]. In addition to that, the Stanford Draft contemplates as offences the deployment of a cyber system "as a material factor" in the commitment of any of the acts criminalised by the following treaties: Convention on Offenses and Certain Other Acts Committed on Board Aircraft; Convention for the Suppression of Unlawful Seizure of Aircraft; Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation; International Convention Against the Taking of Hostages; International Convention for the Suppression of Terrorist Bombings; United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and International Maritime Organization Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation[431]. Finally, according to paragraph (g) the commission of any of the acts included in articles 3 and 4 and directed against the critical infrastructures of a State, whose definition we have previously analysed, is to be criminalised by High Contracting Parties.

This Proposal for an International Convention addressing the issue of cyberterrorism lays down a framework for international cooperation, just like the Budapest Convention does for the broader issue of cybercrime. This choice is due to the same reasons that led the drafters of the CoE Convention on Cybercrime to consider as crucial the role of international cooperation, in order to efficiently deal with such a transitional crime. However, the Stanford Draft proposes the establishment of an agency for information infrastructure protection (AIIP)[432] and the drafting of annual reports by States parties to the Draft[433]. Such proposal can be seen as a step ahead in the field of international cooperation. Such agency should serve as international forum for discussion among

[429] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 3 (d), p. 27.
[430] Elngar, A. (2018) *IT-based Efficient Tamper Detection Mechanism for Healthcare Application*, International Journal of Network Security, Vol.20, No.3, pp. 489-495, available at https://www.researchgate.net/publication/323935849_IoTbased_Efficient_Tamper_Detection_Mechanism_for_Healthcare_Application.
[431] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 3 (f), p. 27.
[432] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 12, pp. 33-35.
[433] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 14, p. 35.

Parties and it could be of particular use for the real-time sharing of useful information on the latest development of the issue at stake.

A part from the substantive matters, the Stanford Draft builds upon the CoE Convention on Cybercrime also for another core issue: the preservation of the fair balance between the protection of human rights and effective prosecution of crimes. This matter is addressed by article 13 of the Draft, according to which it is prohibited "to require an infringement of the privacy or other human rights of any person as defined by the laws of the State Party requested to perform any duty agreed to under this Convention[434]". In addition to that, this article provides for the establishment of "a permanent subcommittee of experts [..] to evaluate and comment upon the manner in which the Convention is being implemented with regard to the protection of privacy and other human rights[435]". Considering the fact that this matter is deemed to be of major importance in the opinion of the Council of Europe, such proposal could be considered for implementation.

To conclude, we should stress once again that the Stanford Draft remained an academic text and did not develop into an international legal instruments. There is no certain explanation for that, however some academics advocated for the fact that the entry into force of the CoE Convention on Cybercrime, which addresses the broader aspects regarding cybercrime and outlines a framework for international cooperation, rendered a considerable part of the Draft a duplication of an already existing legal instrument[436].

Conclusions

In this chapter we briefly took into consideration the counter-terrorism regime established by UN international legal instruments with regard to its application to cyberterrorism. Subsequently we analysed the existing CoE framework that is linked to the issue of cyberterrorism, to evaluate whether or not come of the provisions included in it could be triggered by cases of cyberterrorism. It turned out that some provisions could actually cover some aspects of terrorism. Prosecution results to be more effective for the early stages of a cyberterrorist attack, such as all those illicit behaviours that are classified as support activities to cyberterrorism. However, as the CODEXTER affirmed

[434] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 13, p. 35.
[435] Ibid.
[436] Cohen, A. (2010) *Cyberterrorism: Are We Legally Ready?*, Journal of International Business and Law, Vol. 9, No. 1, pp. 34-35.

in its report "prosecution and prevention of terrorist activities on the Internet depend to a great extent on the existence of appropriate international conventions and other instruments of international cooperation[437]". On top of that, some academics argue that despite the fact that existing international legal instruments' wording is broad enough to allow their application in some cases, "it is regrettable that terrorism is not specifically addressed[438]".

For this precise reason, in order to avoid the problem of overlapping with pre-existing international legal instruments, a lesson we learnt from the analysis of the Stanford Draft, a viable option to better tackle the issue of cyberterror to tackle the issue of cyberterrorism could be found in the drafting of a Protocol to the CoE Convention on Cybercrime. Such a choice would allow to insert the aggravating factor of the terrorist *mens rea* to offences already contemplated by the Convention. As a matter of fact, the only requirement set forth by substantive criminal law provisions of the Budapest Convention is that the act is carried out "without right and intentionally". However, there is clearly no reference to the fact that the underlying intention should be the spread of terror in order to coerce a society or a Government to act or refrain from acting in a specific way. The drafting of an additional Protocol would also allow to establish new offences that are not included in the legal text, but that are deemed to be a concrete threat to society; in such a way that criminalisation is guarantee and does no longer depend on the possibility or not to interpret an article in an evolutive way.

[437] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.p. 48.
[438] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, p. 461.

Chapter 3: The concept of jurisdiction applied to the cyberspace

Introduction

It has already been pointed out along this dissertation, that cyberspace has contributed to the erosion of some of the core concepts of international law, such as the concept of border. With its disregard for physical geographical and political division, the possibility to hide ones actual location and identity and a number of other peculiarities strictly related to cyberspace, the latter makes the task of applying traditional concepts to it harder and harder[439]. However, this chapter will focus on one specific concept which is particularly hard to apply to the cyber dimension: jurisdiction.

For the purposes of our dissertation, this chapter will mainly focus on the matter of judicial or adjudicative jurisdiction, which consists on "the legitimate authority of a national court to try crimes under international law which occurred outside its territory[440]. Furthermore, considering the nature of cyberterrorism and the challenges it poses to jurisdiction, the principle of *rationae loci* will be mainly considered in our analysis, referring to "geographic jurisdiction over particular places[441]". Judicial jurisdiction demands particular attention because its assessment is the very basic step in the process of prosecution. If determining jurisdiction over cases of international crimes is no easy task, determining it in the case of cyberterrorism is an even harder one. The analysis we have conducted so far probably leaves no doubt on what are the peculiarities that characterise cyberspace that render the assessment of jurisdiction an arduous task; still, quickly recalling them can be of use.

As a matter of fact, the concept of jurisdiction relies on a series of concepts that have consolidated along the centuries, such as territoriality and sovereignty; which, however were outlined to mirror a context that is very different from the one of cyberspace. As we have seen, the cyber domain knows no borders, disregards geographical and political divisions and the actual location of an individual, just like identity, can be disguised. As

[439] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, pp. 531-573, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-1714.2002.tb00305.x.
[440] Amnesty International (2001) *Universal Jurisdiction: The duty of states to enact and enforce legislation*, p. 1, available at https://www.amnesty.org/download/Documents/128000/ior530032001en.pdf.
[441] Ibid.

far as sovereignty is concerned, at the moment there is no one who can claim to have absolute control, or even the right to exert it, over the cyberspace[442].

3.1 The notion of jurisdiction

The notion of jurisdiction under public international law refers to the authority of sovereign State to regulate, to adjudicate and to enforce[443]. However, despite the core principle in international law of non-intervention, according to which "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State[444]"; jurisdiction does not limit itself to the territorial borders of a nation. As a matter of fact, under some instances the jurisdiction of a State can trespass its national borders, leading to the emergence of the so-called 'extra-territorial jurisdiction'. The most strict interpretation of the extraterritoriality principle would imply the "assertions of jurisdiction over persons, property, or activities which have no territorial nexus whatsoever with the regulating State[445]"; however this expression has consolidated as a "shortcut for "not exclusively territorial"[446]" jurisdiction. Needless to say that such authority to exceed ones national borders is not unlimited. As a matter of fact it is assessed on the basis some principles that have been defined and consolidated with the passing of time[447]. Still, the presence of such principles does not guarantee the absolute avoidance of conflicts of jurisdiction, rendering the jurisdictional issue one of the most controversial fields in international law[448].

Such situation reflects itself in the fact that to date two approaches to the assessment of jurisdiction coexist. On the one hand, the first approach regards the instances in which a State allows another to "exercise jurisdiction as they see fit, unless there is a prohibitive rule to the contrary[449]"; on the other hand, a State can prohibit another to "exercise jurisdiction as they see fit, unless there is a permissive rule to the contrary[450]". The first approach was outlined in the 1927 *Lotus case* decided by the Permanent Court of

[442] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[443] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, available at https://rm.coe.int/16803042b7.
[444] UN General Assembly (1970) *Declaration of principles of International law friendly relations and co-operation among States in accordance with the Charter of the United Nations*, available at https://www.un.org/ruleoflaw/files/3dda1f104.pdf.
[445] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford, p. 7.
[446] Ibid.
[447] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[448] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[449] Ibid, p. 30.
[450] Ibid.

International Justice (PCIJ); while the second approach, the so-called permissive principles approach, has consolidated in costmary international law and has been adopted by the majority of States. According to the second approach, a State can apply its jurisdiction solely if it can prove its right to do so on the basis of one of the permissive principles. Such principles will be analysed later on in this chapter[451], we will now proceed to a brief analysis of the Lotus case with respect to the first approach to jurisdiction.

3.1.1 The Lotus case and its contribution to the assessment of jurisdiction

Taking into consideration the Lotus Case is a useful step towards a better understanding of the issues concerning cyberjurisdiction, precisely for the fact that despite being a decision taken into 1927 it still serves as basic framework for the assessment of jurisdiction under international law. This case is indeed the only instance of a judgement of an international court directly assessing a jurisdictional issue and precisely for this reason, despite being criticised and considered to be obsolete by many, a considerable number of States still makes reference to it[452].

The core facts of the case regard a French steamship colliding with a Turkish collier in the high seas in 1926. The accident resulted in the death of 8 Turkish people and that is why Turkey proceeded with the sentencing of the Lieutenant of the French ship to a 80 day's imprisonment. However, in 1927 the dispute was submitted to the PCIJ[453]. The Court established that Turkey had the right to try the French officer, stating that States are allowed to "set rules for persons, property and acts outside their territory in the absence of a prohibitive rule, provided that they enforce(d) those rules territorially[454]". More precisely, the PCJI ruled that:

> "[..]it is certain that the courts of many countries, even of countries which have given their criminal legislation a strictly territorial character, interpret criminal law in the sense that offences, the authors of which at the moment of commission are in the territory of another State, are nevertheless to be regarded as having been committed in the national

[451] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[452] Ibid.
[453] Permanent Court for International Justice (1927) *The case of the s.s. "Lotus"*, Series A- No. 1, available at https://documents.law.yale.edu/sites/default/files/ss_lotus_-_pcij_-_1927.pdf.
[454] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford, p.32.

> territory, if one of the constituent elements of the offence, and more especially its effects, have taken place there[455]".

This passage results to be pivotal for the purposes of our analysis. As a matter of fact, as we stated above the judgment at stake, though widely criticised, is still used as basic framework for the assessment of jurisdiction. For this precise reason, it can be claimed that the acceptance of the taking place of a constituent element of the offence or the perceiving of its effects as a justification for the assessment of jurisdiction could render the application of an ancient principle, like the one of territoriality, slightly more feasible. As a matter of fact, considering the fact that the framework designed in the Lotus era was thought for the context of 1927, some claim that in order to make it fit for the cyberspace, the principle of territoriality should not be interpreted in a strict way.

The main downside of this kind of approach is the fact that by stating that a State has the right to claim and exert jurisdiction provided that there is no rule prohibiting it. Such condition is destined to create conflicts of jurisdiction, allowing different States to claim jurisdiction, leading to a situation in which they risk to be concurring against each other. Such flaw was partly fixed in 1970 by the International Court of Justice with the *Barcelona Traction Case*, when the Court highlighted the jurisdictional limits and restraint under international law, though not directly referring to specific international norms[456].

3.1.2 The Harvard Draft and the principles of jurisdiction

As previously anticipated, the permissive principles approach to jurisdiction is based on principles that are aimed at justifying the jurisdictional claim of a State and the exerting of jurisdiction by the latter. As a matter of fact, such principles are invoked in order to prove that there is a "sufficiently close connection between the subject matter and the state[457]", allowing that State to override "the interests of a competing state[458]". The following principles were outlined in the 1935 *Harvard Research draft Convention on Jurisdiction with Respect to Crime*. More precisely, the draft identifies 5 different grounds for jurisdiction that still constitute the framework that is used in international

[455] Permanent Court for International Justice (1927) *The case of the s.s. "Lotus"*, Series A- No. 1, p.23, available at https://documents.law.yale.edu/sites/default/files/ss_lotus_-_pcij_-_1927.pdf.
[456] International Criminal Court (1970) Case Concerning *the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain),* available at https://www.icj-cij.org/files/case-related/50/050-19700205-JUD-01-00-EN.pdf.
[457] Aust, A. (2005) *Handbook of International Law*, Cambridge, p. 43.
[458] Ibid.

law[459] for the aforementioned second approach to the assessment of jurisdiction, that is the permissive principles approach. It is important to stress that, just like in the case of the Stanford Draft, the Harvard Draft was never converted into a binding legal instrument; due to the fact that a treaty addressing limitations on State's jurisdiction would address one of the most sensitive issues of international law[460]. The five principles identified by the Harvard Draft are: territoriality principle, nationality principle, protective principle, universality principle and passive personality principle. However, the draft does not consider these principles as equally strong justifications for the claiming of jurisdiction. On the contrary, the territoriality principles is deemed to be "of fundamental importance and of fundamental character[461]", leading to the conclusion that the "other jurisdictional principles merely function as exceptions to the territoriality principle[462]". However, the fact that these principles are triggered only in those cases in which the territorial nexus cannot be invoked, does not imply that they are not a manifestation of States' sovereignty[463]. The prominence conferred to the territoriality principle is one of the reasons of the success of the Harvard Draft, as such choice was in line with the dominant legal and political theories of that period, which mainly focused on the central role of the State[464]. In addition to that, the draft was the result of the effort of top scholars, who succeeded in summarising one of the most complicated issues of international law[465].

We will now proceed to the analysis of these principles, due to the fact that disregard of the unique nature of the cyberspace, no specific principle has been established yet. As consequence, these principles dating back to 1935 are still the main reference for the jurisdictional issue, also when it comes to the matter of international crimes perpetrated via or against the cyberspace.

[459] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[460] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford, p.32.
[461] Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, p. 445, available at https://www.jstor.org/stable/i312472#:~:text=Description%3A,journal%2C%20published%20quarterly%20since%201907.&text=The%20Journal%20also%20contains%20analyses,U.S.%20practice%20in%20international%20law.
[462] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford, p. 34.
[463] Ibid.
[464] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[465] Ibid.

a. The territoriality principle

The principle of territoriality is commonly linked to the concept of sovereignty. As a consequence, according to the "flag principle[466]" territorial jurisdiction extends to ships flying the national flag and aircrafts registered in the territorial State; just like sovereignty extends itself to the territorial sea and the airspace above the territory itself[467]. The latter, together with the related principle of non-intervention, is probably the main reason explaining why this principle is still considered to be the basic step in assessing jurisdiction[468], even though more and more actors are concerned about its actual applicability to contemporary transnational threats. As a matter of fact, this principle is accepted by the international community as a whole. States agreed indeed on the practical advantages of using the territoriality principle, such as the fact that in most cases the victim, witnesses, evidences and suspect are likely to be in the territorial State[469]. On top of that, this principle affords respect for the sovereignty of each State and, as a consequence, reduces the possibility to incur international tensions caused by jurisdictional conflicts. However, this claim is true as long as this principle is not applied to the cyberspace, whose features are extremely different from the ones characterising the territorial organisation of nations[470]. We will address this issue in detail later on in this chapter.

The most basic interpretation of the territoriality principle is the following:

> "A state is free to legislate and enforce that legislation within its territory, the main exception being when that freedom is restricted by treaty. A state is generally free to apply its legislation to any person within its territory, including foreign nationals; and a constructive presence (a certain degree of contact with the territorial state) may be enough, especially for legal persons like corporations[471]".

Which means that the right to legislate and enforce laws inside the borders of a State belongs solely to the territorial State, a part from those cases in which such right is

[466] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, available at https://rm.coe.int/16803042b7.
[467] Cassese, A. (2013) *Diritto internazionale*, Bologna: Il Mulino, p. 107.
[468] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[469] Amnesty International (2001) *Universal Jurisdiction: The duty of states to enact and enforce legislation*, available at https://www.amnesty.org/download/Documents/128000/ior530032001en.pdf.
[470] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268, available at https://law.stanford.edu/wp-content/uploads/2018/03/stocktongoldman.pdf.
[471] Aust, A. (2005) *Handbook of International Law*, Cambridge, p. 44.

limited by a treaty. An example of restriction to territorial jurisdiction established by a treaty is the matter of immunity of foreign diplomats, which, however does not imply that no jurisdiction can be exerted over them, but rather that "it cannot be exercised unless immunity is waived[472]". According to article 3 of the Harvard Draft by "territorial jurisdiction" it is meant that:

> "A State has jurisdiction with respect to any crime committed in whole or in part within its territory. This jurisdiction extends to (a) Any participation outside its territory in a crime committed in whole or in part within its territory; and (b) Any attempt outside its territory to commit a crime in whole or in part within its territory[473]".

First of all, it is affirmed that, in order to claim territorial jurisdiction, it is not necessary that for all the steps of the crime to be committed inside the territory of a State. The "subjective territoriality" doctrine, indeed establishes that a State has jurisdiction over an illicit conduct that has been initiated inside its territory, even though it was finalised outside it[474]. The territoriality principle might also take the form of the "objective territoriality" doctrine, which reverses the previous principle focusing on the *locus delicti* in which the illicit behaviour was finalised, conferring jurisdiction to that State[475].

Second, a foreign subject participating to and attempting to commit a crime or a constitutive part of it inside a State's territory is considered to be enough to legitimately claim territorial jurisdiction[476]. However, this "constituent element approach" or "ubiquity doctrine[477]" results to be controversial under international law; due to the fact that it is up to national law to define which are the constitutive elements of a particular offence. As a consequence, it can be claimed that under international law, in order to claim territorial jurisdiction it is sufficient that a constituent element of a crime has taken place inside the territory of the State. Such an approach does not take into

[472] Ibid.
[473] Dickinson, D. E. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 3, p. 480.
[474] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.
[475] Ibid.
[476] Dickinson, D. E. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 3, p. 480.
[477] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, available at https://rm.coe.int/16803042b7.

consideration the national characterisation of the constituent acts or the effects of the latter[478].

This kind of approach led to the rise of two subcategories of the territoriality principle: the commencement nexus and effect nexus. According to the first subcategories a State is allowed to exert jurisdiction over a crime that was initiated inside the forum's territory, but was finalised outside it. On the other hand, the second nexus confers a State the jurisdictional right over crimes that have been planned abroad, but whose effects have been perceived inside its territory[479]. In addition to the ubiquity doctrine, the effects doctrine allows for the further expansion of the place in which the *locus delicti* can be identified. As a matter of fact, such doctrine establishes that the perception of the effects of an offence inside a State are a sufficient territorial nexus in order to claim jurisdiction on the basis of the territorial principle[480].

Another way in which these two ways of interpreting territoriality is referred is "subjective territoriality" and "objective territoriality". The first case refers to the primary interpretation of the territoriality principle, the one in which the illicit behaviour takes place inside the territory of the forum. On the other hand, objective territoriality refers to the second case, the one in which the criminal act have been perpetrated abroad, but whose effects are significantly perceived in the territory of the forum[481].

These two doctrines allowing to extend the scope of the territoriality principle render the latter on the one hand more suitable for the application to contemporary transnational threats; but on the other hand they increase the risk that more than one State is entitled to claim jurisdiction, leading to conflicts of jurisdiction among the Parties involved[482].

[478] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[479] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, pp. 531-573, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-1714.2002.tb00305.x.
[480] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg.
[481] Menthe, D. C. (1998) *Jurisdiction in Cyberspace: A Theory of International Spaces*, Michigan Telecommunications and Technology Law Review, Vol. 4, Issue 1, 1998, pp. 69-103.
[482] Ibid.

b. The nationality principle: active personality

The active personality principle, or *la compétence personelle active*, is one of those principles that can be invoked in order to claim jurisdiction, when the territorial nexus cannot be used for this purpose. The principle at stake has prevailed over the others for centuries, until the XVII century when territoriality was adopted as the main reference of the jurisdictional framework. However, it is still universally recognised and accepted[483]. It builds upon the concept of State as "a group of persons, wherever located, who are subject to a common authority[484]

According to this principle established by article 5 of the Harvard Draft:

> "A State has jurisdiction with respect to any crime committed outside its territory, (a) By a natural person who was a national of that State when the crime was committed or who is a national of that State when prosecuted or punished; or (b) By a corporation or other juristic person which had the national character of that State when the crime was committed[485]".

Therefore, in this case jurisdiction is assessed on the basis of the nationality of the suspect[486]. The application of this principle allows a State to exercise jurisdiction over its nationals, even though they are not inside the territory of the State, a ship flying national flag or an aircraft registered in the territorial State[487]. Such condition implies that a State is invested with "worldwide jurisdiction over offences committed by its nationals[488]".

Nonetheless, there is a more restrictive version of the active personality principle, which requires the application of the concept of dual criminality in order for it to be applicable. The restrictive version of this nationality principle establishes that "[..]some criminal acts are made applicable to nationals irrespective as to whether the conduct is

[483] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, pp. 531-573, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-1714.2002.tb00305.x.
[484] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[485] Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 5, p. 519.
[486] Amnesty International (2001) *Universal Jurisdiction: The duty of states to enact and enforce legislation*.
[487] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[488] Clarke, P., & Garnett, R. (2005) *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, p. 475.

criminalised under the law of *locus fori*[489]". The above mentioned dual criminality requirement implies that the conduct over which jurisdiction is being claimed is criminalised both in the State where it was carried out and in the State that is claiming jurisdiction[490]. However, this requirement is a peculiarity of the States in continental Europe, whereas it is not that common in the rest of the world[491].

A further restriction to this principle is applied at national level by some States. As a matter of fact, the applicability of the active personality principle might be restricted to "serious crimes". However, precisely due to the fact that there is no official agreement on which offences are to be considered as serious crimes at international level, there is no such requirement under international law[492].

c. The nationality principle: passive personality

The passive personality principle, or *la compétence personelle passive*, mirrors the aforementioned principle, but focuses on the nationality of the victim and not on the one of the suspect or perpetrator[493]. In other words, according to this principle States are allowed to "assert jurisdiction over offences committed against their nationals abroad by whomsoever committed[494]".

In contrast to the previous ones, this principle is not widely accepted by States and it is considered to be controversial by most of them. For instance, France, the United Kingdom and the United States have strongly criticised the principle at stake in several occasions [495]. Opposing States usually claim that this is the most aggressive jurisdictional principle and that it creates a situation in which the perpetrator cannot foresee which laws he will be subject to, considering the fact that it is plausible that the

[489] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg.
[490] Oxford Reference, stable URL https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095728554, last accessed 10th September 2020.
[491] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[492] Ibid.
[493] Amnesty International (2001) *Universal Jurisdiction: The duty of states to enact and enforce legislation*.
[494] E. D. Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, p. 578.
[495] Amnesty International (2001) *Universal Jurisdiction: The duty of states to enact and enforce legislation*, available at https://www.amnesty.org/download/Documents/128000/ior530032001en.pdf.

nationality of the victim is unknown. In such a condition, the main aim of deterrence would be missing[496].

However, there is a case in which the passive personality principle seems to be more widely accepted and, on top of that, it is considered to be a reasonable ground for asserting jurisdiction: the case of international terrorism[497]. This point results to be of particular importance for the purposes of our analysis and that is why we will recall this aspect later on in this chapter, when analysing the application of the principles at stake to the issue of cyberterrorism.

Just like for the previous principle, passive personality can be restricted in scope by the requirement of dual criminality of by allowing its application only to serious crimes.

d. The protective principle

The protective principle, or *compétence réelle* or *compétence du protection*, focuses on the protection of serious national interests[498]. Still, it must be noted that there is no common standard indicating which interests are included in the wording "serious national interests" or in other cases "essential interests"[499]. As a consequence, it can be claimed that this principle roots in the pivotal principles of self-defence and sovereignty[500].

According to article 7 of the Harvard Draft:

> "A State has jurisdiction with respect to any crime committed outside its territory by an alien against the security, territorial integrity or political independence of that State, provided that the act or omission which constitutes the crime was not committed in exercise of a liberty guaranteed the alien by the law of the place where it was committed[501]".

[496] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[497] Ibid.
[498] Amnesty International (2001) *Universal Jurisdiction: The duty of states to enact and enforce legislation*.
[499] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, p. 10, available at https://rm.coe.int/16803042b7.
[500] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268, available at https://law.stanford.edu/wp-content/uploads/2018/03/stocktongoldman.pdf.
[501] Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 7, p. 543.

It can be noted how the protective principle legitimises jurisdictional claims, even though the crime has been perpetrated above, when such offence jeopardises the sovereignty of the targeted State. Such principles results to be widely accepted in the international community and its legality is not questioned[502].

Nonetheless there are some controversies about the principle as well. As a matter of fact, those States that have been recognising the legitimacy of this principle for centuries claim that this principle derives from the inherent right of the State to self-defence. On the other hand, those States whose history is not characterised by the acceptance of the protective principle affirm that such claim risks to politicise this principle and to encourage its abuse. The instances that would be covered by protective principle would indeed be cases of self-defence against a *fait accompli* and not against an offence that is perpetrated in that moment, resulting into a paradoxical situation[503].

In addition to that, contrary to the principles of territoriality and nationality, which are universally accepted, the protective principle tends to prevail in common law countries and is generally refused in civil law countries. Such division is caused by the fact that the former restrict the application of the principle at stake to serious interests, such as national security; while the latter apply this principle "more expansively to include nearly all actions that injure the forum[504]".

e. Universality principle

The term "universality" probably anticipates the fact that this last jurisdictional principle outlined by the Harvard Draft is the most far-reaching. As a matter of fact, under the universality principle the scopes of territoriality and the two nationality principles are combined, without the application of the restrictions imposed by the protective principle[505].

According to article 9 of the Harvard Draft:

[502] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[503] Ibid.
[504] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, pp. 531-573, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-1714.2002.tb00305.x.
[505] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, p. 10, available at https://rm.coe.int/16803042b7.

> "Foreigners who have committed abroad any offence referred to in Article 3, and who are in the territory of a country whose internal legislation recognises as a general rule the principle of the prosecution of offences committed abroad, should be punishable in the same way as if the offence had been committed in the territory of that country[506]".

Under this principle, jurisdiction over an illicit behaviour can be claimed disregard of the presence of a nexus between the State claiming jurisdiction and the offender, provided that the offence can be classified as matter of international public policy[507]. Considering the fact that international law usually "does not establish regulations or criminal sanctions that apply directly to individuals[508]", but rather it addresses the legislative matter among nations, this principle results to be a sort of exception[509]. As a matter of fact, the possibility for a State to assert jurisdiction over a an offence without the need to have a connection to it "sits uneasy with the classical State-centred view of public international law[510]

However, when the Harvard Draft was written, the only crime that was accepted in order to trigger the universality principle was piracy[511], because such a threat was considered to be against the mankind as a whole[512]. Nonetheless this principle became an object of academic discussion in the '90s and its scope has been broadened[513] including other "universal offences", such as drug trafficking, hijacking[514], slave trade, war crimes, genocides and crimes against humanity. In general, the universality principle is considered to be applicable only to "those crimes that are considered to be so egregious as to be of universal concern[515]". However, it needs to be noted that

[506] Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 9, p. 563.
[507] Clarke, P., & Garnett, R. (2005) *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, p. 475.
[508] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, p. 542.
[509] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, pp. 531-573.
[510] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford, p. 126.
[511] Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 9, 1935.
[512] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701, available at https://www.sciencedirect.com/science/article/abs/pii/S0267364913001362.
[513] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[514] Clarke, P., & Garnett, R. (2005) *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, p. 475.
[515] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, p. 542.

despite fact that this principle attracted the attention of the academic fields only in the '90s, the aforementioned list has been changing and expanding since WWII[516]. For this precise reason, it is often claimed that an offence like the one of cyberterrorism could be covered by the universality principle, considering its transnational nature and the threat it poses to international community[517]. We will deepen this aspect later on in this chapter.

In the light of the fact that the aforementioned crimes of universal concern are not established by national law, but rather by international law, each court applying international law can exert jurisdiction over these crime and hear them. No territoriality or nationality nexus with the forum is required; on condition two conditions: first, the offence must be "serious enough to be hazardous to the international community", in other words it needs to be *hostis humani generis*, meaning "the enemy of all mankind[518]; second, "the country which asserts jurisdiction must have the defendant in custody[519]". However, it must be noted that this is the classical understanding of universal jurisdiction; but at the same time there is no treaty formally forbidding the application of the universality principle *in absentia*. Nonetheless, State praxis on this front is still too scarce in order to try and foresee how this aspect might evolve in the future[520].

3.2 The birth and evolution of cyberjurisdiction

With the birth of the cyberspace and the consolidation of its role in our society, the need for regulation could no longer be ignored. The jurisdictional issue was not excluded from the process of regulation, bringing to light a number of problematic. As a matter of fact, if jurisdiction is no easy riddle to solve when it has to be dealt with respect to tangible spaces, the situation can only get more and more complicated when it has to be applied to an intangible and borderless space like the cyberspace.

---

[516] August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, pp. 531-573.
[517] Manap, N. A., Taji, H., & Tehrani, P. M. (2013) *Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime*, Computer Law & Security Review, Vol. 29(3), pp. 207-215.
[518] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, p. 245, available at https://law.stanford.edu/wp-content/uploads/2018/03/stocktongoldman.pdf.
[519] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, p. 695.
[520] Ryngaert, *Jurisdiction in International Law*, 2nd Edition, Oxford, 2015.

The concept of *cyberjurisdiction* stems from the need to extend an ancient principle of international law, jurisdiction, to one of the most recent developments of the contemporary society, the cyberspace and its functions. It can be claimed that by cyberjurisdiction it is merely meant the application of the concept of jurisdiction, which corresponds to the "competence under international law to prosecute and punish for crime[521]", to the field of cyberspace. Being the cyberspace a relatively new domain, the concept at stake is relatively new as well. For this precise reason it has been the object of an animated debate, yet there seems to be no consensus on the steps that need to be taken in order to better define this branch of jurisdiction[522].

The starting point for the discussion on the issue of cyberjurisdiction coincides with the advent of Internet in 1991. Once again, it needs to be stressed that this system relies on a protocol that was not outlined for the use that it is made nowadays if the Internet[523]. In addition to that, "the Internet was not designed with jurisdictional conundrums in mind[524]". During the first years of this decade the cyberspace has been perceived as a *terra nullius*, leading to instances like the 1996 "Declaration of the Independence of Cyberspace[525]". Such declaration was the manifesto of the *cyber-libertarians* political movement, which claimed that governments had no right on the cyberspace, considering its borderless and global nature. On the basis of this assumption, Post and Johnson derived their juridical thesis: activities on the cyberspace cannot be regulated by States, considering the fact that their authority is limited to their national borders; whereas cyberspace and the activities that take place in it extend worldwide[526].

The emergence of such claims led States to feel the need to seriously address the jurisdictional issue for the first time. As a matter of fact, short after the aforementioned declaration, the first decision that related personal jurisdiction to Internet was taken. The case was *Zippo Manufacturing Company V. Zippo Dot Com, Inc.* and it recognised the fact that the claiming of jurisdiction over activities carried out online is legitimate.

[521] Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, p. 467.
[522] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[523] K.E. Gable, *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law 43, no. 10, January 2010, 57-118.
[524] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford, p. 92.
[525] Barlow, J. P. (1996) *A declaration of the Independence of Cyberspace*, available at https://scholarship.law.duke.edu/dltr/vol18/iss1/2/.
[526] Cassese, A. (2013) *Diritto internazionale*, Bologna: Il Mulino.

However, the legitimacy of the claim can be ranked on different degrees, leading to the birth of the expressions "Zippo test" or "Zippo's sliding scale"[527].

With the advent of the new century, a phase of over-regulation on cyberspace began. As a matter of fact, courts and legislators tended to claim jurisdiction over any conduct carried out on the cyberspace that impacted or would impact ones territory or citizens. Being the cyberspace present worldwide and taking into consideration the difficulties in identifying the actual geographical location of an individual using the cyberspace, courts and legislators could virtually claim jurisdiction over any conduct carried out on the cyberspace[528]. The *Yahoo! INC V. La Ligue Contre le Racisme et L'Antisémitisme*[529] case is probably the most emblematic one of this phase in the development of cyberjurisdiction. In accordance to the French Penal Code, La Ligue Contre le Racisme et l'Antisémitisme requested that Yahoo! Removed from its auction service the Nazi material that was circulating. However Yahoo!, a US Internet company, refused to do so. The final decision indeed confirmed that France had the right to regulate the matter taking place in the cyberspace as long as it was limited to French borders, but that French decisions could not be applied in US soil[530].

The time span from 2010 to 2014 is characterised by a tendency contrasting the one we have just mentioned, that is under-regulation. As a matter of fact, the willingness of courts and legislators to avoid the claiming of a too broad jurisdiction led to a lower degree of regulation in this field. A proof of this approach can be found in the cases of *Pammer v Reederei Karl Schlüter GmbH & KG* and *Hotel Alpenhof GesmbH v Oliver Heller* jointly addressed by the European Court of Justice. The latter stated that the mere fact that a website can be accessed from the territory under the jurisdiction of a State does not automatically imply that the activities were directed to that State[531]. This was also the time span in which the topic of cyberjurisdiction became mainstream in the

[527] US District Court for the Western District of Pennsylvania (1997) *Zippo Manufacturing Company V. Zippo Dot Com, Inc*, 952 F. Supp. 1119, available at https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/.
[528] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[529] United States Court of Appeal (2004) *Yahoo! INC V. La Ligue Contre le Racisme et L'Antisémitisme*, No. 01-17424, available at https://caselaw.findlaw.com/us-9th-circuit/1308396.html.
[530] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[531] European Court of Justice, (2010) *Joined Cases C-585/08 and C-144/09*, par. 95, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CA0585.

academic debate. A considerable number of publications and cyberjurisdiction-themed events can be seen as proof of this tendency[532].

The phase that started in 2015 and that we are still living is considered to be another clash with respect to the previous period. As a matter of fact a tendency to hyper-regulation emerged. It can be claimed that in the present context it is no longer of assessing which State's law can be applicable to a case; but rather "which of the many applicable laws actually matter[533]". The instances of these years have proven that, due to the viscosity of the cyberspace, States can exploit several nexus to claim jurisdiction. In addition to that, treaties addressing issues related to cyberspace are now more consolidated tools compared to the time in which the Council of Europe was the first international organisation addressing the matter of crimes perpetrated via and against the cyberspace. The fact that the CoE is currently undertaking an effort to reform the Budapest Convention [534] in order to amplify the role of this international legal instrument is a further proof of the current tendency towards the matter at stake.

3.2 The problematic aspects of cyberjurisdiction with respect to cyberterrorism

As anticipated at the beginning of the previous paragraph, disregard of the peculiarities that characterise and differentiate the cyberspace, and as a consequence the crimes committed through and against it, no jurisdictional principle dedicate to this unique environment has been established yet. As a matter of fact, the five principles of jurisdiction established in the Harvard Draft that serve as reference framework in this field, are applied to the cyberspace as well[535].

The problem is that the main features of the cyberspace render the application of the classical jurisdictional principles to this peculiar environment a particularly complicated task. On top of that, some even doubt the actual effectiveness of such ancient principles when applied to such a modern field[536]. That is why we will now proceed to taking into account each jurisdictional principle and its application to the cyberspace with respect to possible instances of cyberterrorism.

---

[532] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[533] Ibid, p. 107.
[534] Cybercrime Convention Committee (2020) *The Budapest Convention on Cybercrime: benefits and impact in practice*, Strasbourg, available at https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.
[535] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.
[536] Ibid.

3.2.1 Applying the territoriality principle to cyberterrorism

As we have stressed several times so far, the cyberspace disregards the geopolitical division among nations and the crimes that are committed through and against it are characterised by a strongly transnational nature[537]. Despite of that, the territoriality principle is still the prevailing one when it comes to assessing jurisdiction; just like it is the basic principle in all other instances and the other principles are taken into consideration solely when the territorial nexus cannot be invoked[538].

For the territoriality principle to be considered as applicable to cases of cybercrime in general, but also for our specific case of cyberterrorism, a substantial territorial connection between the State claiming jurisdiction and the *locus delciti* needs to be present. Such nexus might be established by the perception of the effects of the attack inside the territory of a State (objective territoriality principle); by the localisation, by means of IP address for example, of the perpetrator's computer inside the territory of the State (substantive territoriality principle); or even if relevant content is stored inside a server based inside the territory of the State[539].

However, the cyberspace implies a series of complication to the application of the territoriality principle to instances of cyberterrorism. As we have seen in the first chapter, cyberterrorism is a transnational crime that does not limits itself to the national borders of a country[540]. Establishing jurisdiction over instances of cyberterrorism relying on the territorial principle might actually be impractical, due to the fact that, contrary to the geopolitical division among States, the cyberspace lacks of borders and simultaneously encompasses all nations[541]. In addition to that, we explained how easy it is for a cyberterrorist to disguise the actual location from which the cyberterrorist attack was launched, for example by using a fake IP. Furthermore, the effect of a single cyberterrorist attack can be perceived in more than one nation, just like the steps that are needed in order to strike the final attack can be perpetrated in more than one country[542].

---

[537] Luiijf, E. (2014) *Cyber Terrorism: Case studies*, in Cyber Crime and Cyber Terrorism Investigator's Handbook, edited by B. Akhagar, A. Staniforth, F. Bosco, pp. 163-174.
[538] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[539] Ibid.
[540] Bogdanoski, M., & Petreski, D. (2013) *CYBER TERRORISM– GLOBAL SECURITY THREAT*, International Scientific Defence, Security and Peace Journal, Vol. 13, Issue 24, pp. 59-73.
[541] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268,
[542] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701.

To recall one of the scenarios we depicted in the first chapter, crucial infrastructures usually rely on SCADA systems and, most of the times, these systems are internationally connected. This condition brings with itself the possibility for cyberterrorists to exploit the flaws of a single system in order to strike against numerous nations[543].

Such a situation is likely to create jurisdictional conflicts. As a matter of fact, the territoriality principle outlined by the Harvard Draft establishes that it is sufficient for a constitutive aspect of the offence to take place inside the territory of the form, to allow the territorial State to claim jurisdiction[544]. According to the subjective territoriality principle a State has jurisdictional right once an illicit action has been initiated inside its territory, but when it comes to cyberterrorists attack such a principle is no guarantee of single jurisdictional claim. As a matter of fact, a cyberterrorist attack can be initiated by a huge number of computers acting simultaneously from all over the world, for instance exploiting the botnet technology[545] we described in the first chapter. In the light of that, considering the aforementioned possibility for a cyberterrorist attack to be constituted by several step that can be carried out anywhere in the world, the emerging of a jurisdictional dispute among several countries is a realistic scenario[546].

The same reasoning can be followed for the objective territoriality principle, which legitimises the exerting of jurisdiction by a State if the effects of an attack have been perceived inside its territory[547]. As a matter of fact the exploitation of ICT allows to expand the effects of an illicit behaviours to an incredibly wide area, technically to each place in the world that is connected to it. As a consequence, once objective territoriality is set forth as main jurisdictional reference, the possibility that the effects of a cyberterrorist attack are perceived in a considerable number of States needs to be taken into consideration[548]. Despite this problematic implication, the effect doctrine seems to be the prevailing approach to instances of jurisdictional issues related to the cyberspace.

[543] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.
[544] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[545] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.
[546] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701.
[547] Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg.
[548] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701.

To briefly mention an example, we could take into account the *R v Waddon*[549] case. The English Court of Appeal allowed for the prosecution of an English resident for the spreading of obscene materials in the UK through a pornographic website. Despite the fact that the offence was carried out by means of a US-based server, on which the website relied, UK gained the right to assert jurisdiction. This is because the Court aimed at protecting "the public in the forum from the *effects* of such material being accessible even though the content was physically located on a computer server outside the forum[550]". Even though this is no example of assessment of jurisdiction over cyberterrorism, it is a good example of how the effect doctrine is applied to the cyberspace and it can be claimed that a Court confronted with an instance of cyberterrorism is likely to act in a seminal way[551].

Despite the problematic scenarios that the application of the territoriality principle to the cyberspace is likely to cause, no formal international protest against this pattern of asserting jurisdiction has taken place in the international community so far[552]. This is probably due to the fact that many focus on the amplification of the scope of the territoriality principle with the application of the ubiquity and effect doctrine, which allows to take a "broad view of harmful effects in the forum so as to capture a wide variety of offences under the territorial principle[553]". However, such an approach does not take into consideration the aforementioned flip side of such a wide applicability of the territoriality principle that is likely to lead to jurisdictional conflicts. Considering the fact that this kind of conflict is considered to be detrimental for the maintaining of good international relations among State, such flips side should not be neglected[554].

3.2.2 Applying the nationality principle to cyberterrorism

The application of the nationality principle, both when for the passive and active personality versions, is not particularly widespread when it comes to cybercrime and, as a consequence, its application to cyberterrorism seems to be unlikely. However, it

[549] English Court of Appeal (2000) *R v Waddon*, available at https://www.lccsa.org.uk/r-v-graham-lester-ian-waddon-2000/.
[550] Clarke, P., & Garnett, R. (2005) *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, p. 475.
[551] Ibid.
[552] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[553] Clarke, P., & Garnett, R. (2005) *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, p. 475.
[554] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.

cannot be categorically excluded from the possible options for a regulation of the jurisdictional issue with respect to cyberterrorism. As a matter of fact, some States like the United States, actually choose to use it despite the lack of broad consensus[555].

The first problematic aspect that might arise is the fact that hiding ones identity, and as a consequence ones nationality, in the cyberspace results extremely easy. In the first chapter we saw how cyberterrorists can use a false identity to perpetrate their acts, can exploit some mechanisms in order to simply hide it or can even commit identity theft and use it to act undercover.

As anticipated, the United States is the main supporter of this approach to jurisdiction and decided to apply it to the cyberspace as well; despite of the important difficulties that are implied in such process and the lack of a broad consensus on this kind of choice. For this precise reason, in order to understand how the nationality principle might be applied to cases of cyberterrorism, we need to rely on the US approach to the matter.

According to the Fourteenth Amendment of the United States Constitution[556], in order to trigger the nationality principle there needs to be a "substantial, systematic and continuous contact with the forum state and even of the conduct is unconnected to the form state[557]". In addition to that, a "minimum contact test" and a "reasonableness prong" are applied to the matter before assessing personal jurisdiction. The minimum contact test simply consists on the collection of evidence that there has actually been a contact between the defendant and the forum[558]. However, while analysing the Budapest Convention we highlighted how the volatility of the cyberspace might actually render the collection of evidence problematic. In the case of the CoE framework related to the topic, as we have seen, provisions providing for the expedited collection of evidence and the exchange of information among High Contracting Parties are included. Such mutual assistance framework established taking into consideration the peculiarities of the cyberspace might be a useful solution to the problems posed by the cyber domain to

[555] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701.
[556] Legal Information Institute, *14th Amendment*, stable URL https://www.law.cornell.edu/constitution/amendmentxiv, last accessed 15th September 2020.
[557] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, p. 693.
[558] Ibid.

the minimum contact test. Once the minimum contact test is exhausted, the reasonableness prong takes place, in which a Court has to:

> "(1) weigh up the burden on the defendant to litigate in the forum state (USA), (2) consider the interest of the forum state (USA) in the matter, (3) ascertain the interest of the plaintiff in obtaining relief, (4) scrutinize the efficiency of the forum state (USA) in dispute settlement, and (5) look over the interests of several states (USA) in furthering certain fundamental social policies[559]".

Finally, in the case of passive personality principle, according to what emerged in the aforementioned *Zippo Case*, the action that are taken against a resident of the forum State need to be taken deliberately[560]. This point might result to be problematic as well. As a matter of fact, if we recall one of the distinctive elements of cyberterrorism we highlighted in the first chapter, it can easily be noted how there can be an *impasse* in the application of this principle. Contrary to the traditional manifestations of international terrorism, it is conceivable that cyberterrorists prefer not to claim responsibility for their actions, in order not to expose the flaws in the system that allows them to perpetrate the act itself[561]. As a consequence, it might be hard to prove the fact that an individual has chosen to act against another one by deliberately taking into account their nationality.

Finally, it needs to be noted that, despite the low level of support that is granted to the passive personality principle in general, in the last decades this principle has been considered as suitable for asserting jurisdiction over cases of international terrorism. However, an extension of the principle to the cyber manifestation of international terrorism would lead to the same *impasse* caused by the effect doctrine of territoriality. As a matter of fact a cyberterrorist attack has the potential to reap victims in multiple States at the same time, leading to concurring jurisdictional claims that would be equally legitimate compared to one another[562].

---

[559] Rahman, M. O. (2008) *Towards Understanding Personal Jurisdiction in Cyberspace*, International Journal of Law and Management, p. 110, available at https://www.emerald.com/insight/content/doi/10.1108/17542430810877445/full/pdf?casa_token=99nCe0YmCPMAAAAA:lSNO0yjT9Y4zU6t-JEX3Rw5JGj4E7U69pvdF0-7swnrFmzbR1cdmG1jD2lg4KKqk13bMhKw9kpd8aeDiUTWwuDQCnkxZJmiI8IvvKzexIaJPHwd39Mo.

[560] Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701.

[561] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

[562] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.

3.3.3 Applying the protective principle to cyberterrorism

At the moment there seems to be no particularly relevant example of praxis in which the protective principle has been applied to instances of cybercrime. In addition to that, there is no agreement on the efficacy of this principle; some claim that its scope is still too vague in order to conceive its application[563], while others claim that it might be a suitable solution considering the peculiarities of cyberterrorism. As a matter of fact, it was claimed that applying this principle to cyberterrorism would allow "to reduce the number of conflicting jurisdictional claims and mitigate international discord[564]".

The application of the protective principle to instances of cyberterrorism would allow States whose security is under threat to exert jurisdiction. In the light of that, some experts claim that the application of the protective principle in this field would allow for the reduction of competing jurisdictional claims. This is because the protective principle is the only jurisdictional nexus under international law authorising the exertion of extraterritorial jurisdiction over crimes that threaten a nation's security. Needless to say that cyberterrorist attacks, in the light of the plausible scenarios we took into account in the first chapter, can endanger national security and therefore trigger the protective principle. This kind of approach would restrict the *locus delicti* that is identified with approaches like the one established by the effect doctrine, which results to be far more far-reaching. As a matter of fact, this principle would circumscribe the legitimate jurisdictional claims to those risen by States in which the effects of the attack have been perceived; but on condition that those effects are serious enough to be considered as a threat to national security[565].

Such an approach would also be a guarantee of reduction of impunity, compared to the application of the territoriality principle for instance. In the possible instance of a cyberterrorist attack, it is logic to expect that the countries in which the effects of the attack produced a threat to the security of the nation would be the most prone to claim jurisdiction over the acts and to undertake the effort of prosecution. It needs to be highlighted that cyberforensic investigation is extremely expensive and complicated and, as a consequence, the mere perception of effects without the endangering of serious

[563] Aust, A. (2005) *Handbook of International Law*, Cambridge, p. 51.
[564] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, p. 249.
[565] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.

national interests could not be enough in order to spur the prosecution of cyberterrorists[566].

Most important, the application of the protective principle to the assertion of jurisdiction over cases of cyberterrorism would allow to take a preventive approach against the matter. Such claim relies on the fact that the principle at stake "is the only jurisdictional basis under international law that authorises extraterritorial jurisdiction over crimes that pose a potential danger to the security of a state[567]". Unfortunately, not all kinds of cyberterrorists attack can be prevented due to the technology they rely on. In the first chapter we mentioned the zero-day exploits technique, which precisely exploits the vulnerability of a system that is still unknown to the developer of the latter[568].

3.3.4 Applying the universality principle to cyberterrorism

As anticipated in the paragraph about the classical application of the universality principle, this jurisdictional basis was born with respect to the offence of piracy[569]. However, during the last decades the international community decided to expand the scope of this principle to other crimes that are considered to be particularly heinous, such as genocide, war crimes and crimes against humanity[570]. On the basis of such evolution, it is more and more often claimed that universal jurisdiction could be applied to cases of cyberterrorism and soma also believe that it would actually be the most suitable way to address this new threat to the international community[571]. As a matter of fact, in the light of the fact that the universality principle does not rely on territorial grounds, just like the cyberspace disregards territorial geopolitical divisions, the universality principle could be a suitable solution in order to face the peculiarities of the cyberspace.

A good instance of the new perceptive that has been taken in the last years towards the matter of the broader application of universal jurisdiction is article 18 of the *Draft Code*

---

[566] Ibid.
[567] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, p. 251.
[568] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.
[569] Dickinson, E. D. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 8, p. 561.
[570] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[571] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, pp. 57-118.

of Crimes against Peace and Security of Mankind. This article, which appears in the draft adopted by the International Law Commission and submitted to the UN General Assembly, seeks to expand the concept of crimes against humanity. As previously explained, these crimes are included in the crimes over which universal jurisdiction can be applied. As a matter of fact, according to the Draft Code of Crimes against Peace and Security of Mankind:

> "A crime against humanity means any of the following acts, when committed in a systematic manner or on a large scale and instigated or directed by a Government or by any organization or group: (a) murder; (b) extermination; (c) torture; (d) enslavement; (e) persecution on political, racial, religious or ethnic grounds; (f) institutionalized discrimination on racial, ethnic or religious grounds involving the violation of fundamental human rights and freedoms and resulting in seriously disadvantaging a part of the population; (g) arbitrary deportation or forcible transfer of population; (h) arbitrary imprisonment; (i) forced disappearance of persons; (j) rape, enforced prostitution and other forms of sexual abuse; (k) other inhumane acts which severely damage physical or mental integrity, health or human dignity, such as mutilation and severe bodily harm[572]".

If such a reform of the conception of crimes against humanity was to enter into force, cyberterrorism could formally be included in the crimes that fall under universal jurisdiction.

In the academic field, there seems to be a stream of experts pushing for the application of the universality principle to instances of cyberterrorism due to a number of reasons. First, the assumption that cyberterrorism needs to be considered as a manifestation of terrorism allows to claimed that the existing international legal framework on terrorism, by extension, can be considered as a basis for extending universal jurisdiction to cyberterrorism. As a matter of fact, the aforementioned framework would serve as a basis in either treaty law or customary international law[573].

On top of that, in order to assess whether or not cyberterrorism should be considered as suitable for the application of the universality principle there are a series of rationales that cyberterrorism is able to fulfil. The first rationale requires that a crime reaches a

[572] International Law Commission (1996) *Draft Code of Crimes against the Peace and Security of Mankind*, art. 18, p. 6, available at https://legal.un.org/ilc/texts/instruments/english/draft_articles/7_4_1996.pdf.

[573] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, No. 10, pp. 57-118.

certain threshold of heinousness in order to be considered as approachable by universal jurisdiction[574]. As a matter of fact, a crime needs to be universally abhorred, monstrous or able to shock human conscience[575]. The instances that we depicted in the first chapter prove that cyberterrorism might actually meet this requirement.

Second, it is claimed that universal jurisdiction can be seen as an extension of the protective principle. Therefore, the basic principle that national interest need to be endangered by the offence remains valid. As we affirmed in the paragraph about the protective principle, the threat of cyberterrorism is in line with such purpose[576].

Third, the "agency rationale" establishes that the State gaining jurisdiction over an offence should be acting as "agent for the international community[577]. As we have said many times by now, cyberterrorism has the potential to strike against more than one State at once and can be classified as a transnational crime. As a consequence, acting against cyberterrorism meets the requirement of acting in favour of the interests of the international community[578].

The fourth rationale focuses on the *locus delicti*, claiming that crimes over which universality can be considered as legitimate are perpetrated in territories that are beyond the sovereignty of nations[579]. This rationale can be fulfilled by cyberterrorism, due to the fact that the cyberspace is considered to be the place where sovereignty is particularly arduous to *establish par excellence*.

Last but not least, as anticipated above some claim that applying the universality principle to cyberterrorism is not only conceivable, but also advisable. As a matter of fact, it is believed that the application of the universality principle to the issue at stake would have the positive implication of deterrence. As a matter of fact, deterrence is reached by means of effective and consistent prosecution and the application of this

[574] Ibid.
[575] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.
[576] Ibid.
[577] Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, pp. 57-118.
[578] Ibid.
[579] Ibid.

approach could be a better guarantee of that, than the application of the other jurisdictional principles[580].

Nonetheless, the issue regarding the matter of the applicability of the universality principle to cyberterrorism is still an animatedly debated one. As a matter of fact some experts argument against some of the previous assumptions. For instance, it has been claimed that at the moment there is no sufficient legal basis in order to extend the universality principle to cyberterrorism. In addition to that, it is doubted that all kinds of cyberterrorist attacks can actually reach the heinousness threshold that is required for the crime to be addressed under universal jurisdiction. Moreover, this academic stream supports the theory that the acknowledgment that there is a "mismatch" between existing international legal instruments and the cyber capabilities that terrorist actors have acquired, is not enough to claim that an actual *opinion juris* on the matter has emerged. Finally, some scholars claim that universal jurisdiction is not the most suitable solution to the jurisdictional issue regarding cyberterrorism because of the fact that it is the most far-reaching among the jurisdictional basis. As a consequence it might be more easily applicable to the matter, but at the same time it is likely that it raises a considerable number of jurisdictional claims, leading to conflicts and tension among countries[581].

3.4 The jurisdictional issue in the Council of Europe framework: art. 22 of the Convention on Cybercrime

In the light of the analysis that we carried out in the second chapter, despite the fact that the CoE Convention on Cybercrime does not include among its offences the crime of cyberterrorism; its provisions result to be an indirect coverage of the matter, due to the fact that they target those offences that are at the basis of a cyberterrorist attack[582]. For this precise reason, it is useful to take a closer look at how the Budapest Convention binds High Contracting Parties to assess jurisdiction over cybercrimes and, by extension, cyberterrorism.

[580] Ibid.
[581] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.
[582] Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

The matter of jurisdiction, as anticipated in the second chapter, is governed by article 22 and it governs the jurisdictional matter of the Additional Protocol to the Convention on Cybercrime as well. The article reads as follows:

> "(1) Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: (a) in its territory; or (b) on board a ship flying the flag of that Party; or (c) on board an aircraft registered under the laws of that Party; or (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. (2) Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. (3) Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. (4) This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. (5) When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution[583]".

The first paragraph of the article 22 makes it clear that the Budapest Convention follows the mainstream approach to cyberjurisdiction, thus choosing to respect the prominence of the territoriality principle even though applied to the cyberspace[584]. As a matter of fact, *littarea* a through c mirror the classical conception of the territoriality principle, according to which a State has jurisdiction over offences that were perpetrated inside its territory, in ships flying the national flag and in aircrafts registered under the national law[585].

Littera d, however, sets forth the application of the nationality principle as well. Under this paragraph, indeed, High Contracting Parties have jurisdiction over their nationals,

[583] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 22, Budapest, pp. 13-14.
[584] P Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701.
[585] Cottim, A. A. (2013) *Cybercrime, Cyberterrorism and Jurisdiction : An Analysis of Article 22 of the COE Convention on Cybercrime*, European Journal of Legal Studies, Vol. 2, No. 3, 2013, pp. 55-79.

even though the illicit behaviour has been carried out outside their territory[586]. States parties to the Convention must prosecute the offences laid down by the Convention that have been committed in the aforementioned way, on condition that the "conduct is also an offence under the law of the State in which it was committed[587]", according to the dual criminality principle that we have previously mentioned in this chapter[588], or on condition that "the conduct has taken place outside the territorial jurisdiction of any State[589]".

Paragraph 2 of art. 22 establishes that Parties are allowed to enter a reservation regarding the matter of jurisdiction solely if it is related to paragraph 1 (b), (c) and (d). On the contrary, no reservation is admitted on the territoriality principle established by paragraph 1 (a) and the obligations under paragraph 3[590].

The third paragraph of this article regulates the jurisdictional aspect with respect to extradition. Article 24 of the Budapest Convention establishes that States parties to the Convention must respect the international customary law principle *aut dedere aut judicare*, either adjudicate or punish[591]. In the case in which the alleged offender should be found in a State different from the one in which the crime was committed and extradition was required and denied by the State where the alleged offender is currently present on the basis of national law constraints; that State has the duty to prosecute the alleged offender, but also to guarantee that it has the legal ability to investigate and proceed the case. The aim of this clause is to make sure that impunity is avoided[592], thus conferring added value to the Budapest Convention.

It is true that the main jurisdictional grounds established by the Budapest Convention are territoriality and nationality; however, paragraph 4 of article 22 sets forth the possibility for High Contracting Parties to apply other jurisdictional grounds, provided that they are in conformity with their domestic law. Such provision *de facto* allows

---

[586] Ibid.
[587] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, p. 41, available at https://rm.coe.int/16800cce5b.
[588] Ryngaert, C. (2015) *Jurisdiction in International Law*, Second Ed., Oxford.
[589] Council of Europe (2004) *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, p. 41, available at https://rm.coe.int/16800cce5b.
[590] Ibid.
[591] Council of Europe (2004) *Convention on Cybercrime – No. 185*, art. 24, Budapest, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.
[592] Cottim, A. A. (2013) *Cybercrime, Cyberterrorism and Jurisdiction : An Analysis of Article 22 of the COE Convention on Cybercrime*, European Journal of Legal Studies, Vol. 2, No. 3, 2013, pp. 55-79.

States to apply the jurisdictional ground they prefer to adopt[593]; leading to the fact that, if confronted with instances of cyberterrorism States might decide to apply other jurisdictional principles than territoriality and nationality.

Finally, paragraph 5 of art. 22 provides for a solution to one of the main concerns regarding cyberjurisdiction. As a matter of fact, it emerged from the analysis of the application of classical jurisdictional principles to the issue of cyberterrorism that it is extremely likely that jurisdictional conflicts might rise, due to the claiming of jurisdiction by several States[594]. Such a situation is plausible due to the fact that cyberattacks in general and cyberterrorist attacks, can be launched from more places just like they can be perceives in more States. If such a situation was to concretise, High Contracting Parties would be required to confront each other and choose the most appropriate venue for the prosecution of the crime at stake[595]. The obligation under this paragraph does not guarantee a resolution of jurisdictional conflicts, due to the fact that High Contracting Parties might find no agreement on how to proceed with the prosecution of the offence; but at least a basis for the finding of a solution is established and, most important, providing for such a possibility reduces the instances in which the dispute is submitted to the arbitration of an international Court, allowing to avoid poisoning the relations among countries. In addition to that, the Budapest Convention provides for a framework of harmonization of both substantive and procedural law and international cooperation[596], allowing to reduce the possibilities of disputes among countries.

3.5 The jurisdictional basis proposed by the Stanford Draft

In the second chapter we took into account the academic proposal for an international convention specifically addressing cyberterrorism, we will now proceed to consider hoe the Stanford Draft proposes to assess jurisdiction over matters of cyberterrorism.

First of all, the jurisdictional issue is governed by article 5 of the Stanford Draft. The first paragraph of the article reads as follows:

---

[593] Ibid.
[594] Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268.
[595] Cottim, A. A. (2013) *Cybercrime, Cyberterrorism and Jurisdiction : An Analysis of Article 22 of the COE Convention on Cybercrime*, European Journal of Legal Studies, Vol. 2, No. 3, 2013, pp. 55-79.
[596] Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425, available at https://btlj.org/?s=The+Council+of+Europe%27s+Convention+on+Cybercrime&submit=Search.

> "1. Each State Party to this Convention shall take such measures as may be necessary to establish its jurisdiction over the offenses set forth in Articles 3 and 4 in the following cases: (a) when the offense is committed in the territory of that State or on board a ship, aircraft or satellite registered in that State or in any other place under its jurisdiction as recognized by international law; (b) when the alleged offender is a national of that State; (c) when the alleged offender is a stateless person whose primary residence is in its territory; (d) when the alleged offender is present in its territory and it does not extradite such person pursuant to this Convention[597]".

As we explained in the second chapter, the Stanford Draft builds upon the CoE Convention on Cybercrime and this paragraph clearly mirrors the Budapest Convention, by respecting the prominence of the territoriality principle in the jurisdictional framework and setting it forth as the main jurisdictional basis.

Paragraph 2, contrary to the previous one, adds something that is clearly not included in the Budapest Convention, as it makes reference to the *mens rea* underlying the acts that are criminalised by the Draft.

> "2. Each State Party to this Convention may take such measures as may be necessary to establish its jurisdiction over the offenses set forth in Articles 3 and 4 in the following cases: (a) when the offense is committed with intent or purpose to harm that State or its nationals or to compel that State to do or abstain from doing any act; or (b) when the offense has substantial effects in that State[598]".

In this paragraph the drafters recall the terrorist intent that needs to be present in order to be dealing with a cyberterrorist act and not just a generic cyberattack. Despite the fact that the Stanford Draft sets forth the nationality principle as main jurisdictional basis, this paragraph seems to be more suitable for the assessment of jurisdiction under the protective principle. As a matter of fact, the application of the latter is not excluded by the Draft. Paragraph 3 of article 5, just like paragraph 4 of article 22 of the Budapest Convention, allows for the application of other jurisdictional principles different from the territoriality one; provided that they are "exercised in accordance with domestic law" or "established pursuant to any other bilateral or multilateral treaty[599]".

---

[597] Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, art. 5, 29-30, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf.
[598] Ibid.
[599] Ibid.

The last paragraph recalls once again the principles that States should make reference to, in order to assess jurisdiction; however, the principles are listed in a hierarchical order, therefore conferring different relevance to different principles. The most basic interpretation of the nationality principle is put in the first places, by stating that "the State Party in which the alleged offender was physically present when the alleged offense was committed[600]" has jurisdiction over the offence at stake. The variation of the territoriality principle that focuses on the effects caused by the offence is set in the second place of the hierarchical scale. As a matter of fact, it is established that "the State Party in which substantial harm was suffered as a result of the alleged offense[601]". In those cases in which these two interpretation of the territoriality principle cannot be applied, a State Party shall rely on the nationality principle, according to the statement that "the State Party of the alleged offender's dominant nationality[602]" has the jurisdictional right on the matter. The fourth ground establishes that "any State Party where the alleged offender may be found" has jurisdictional power over the matters at stake. Considering the fact that, as previously explained, one of the only two conditions that need to be fulfilled in order to apply the universality principle is to have the suspect in custody; this statement seems to be a reference to the universality principle. Finally, it is reiterated that States are not forbidden to apply other jurisdictional grounds, provided that they consist on "reasonable basis for jurisdiction[603]".

Contrary to the Budapest Convention, the Stanford Draft does not propose a forum to be used in order to settle jurisdictional disputes among Member States and this is doubtlessly a black mark of this academic proposal, considering the likelihood of jurisdictional conflicts in the cyberspace.

Conclusions

Depicting the actual complexity of the jurisdictional matter inside one chapter of this dissertation is clearly impossible. However, this analysis provides an overview on one if the most problematic aspects of international law. As a matter of fact jurisdiction is linked to the core principle of sovereignty, which needs to be respected, but at the same time cannot be unlimited. The jurisdictional principles we took into analysis seek both to guarantee States' sovereignty and to avoid the application of this principle without

[600] Ibid.
[601] Ibid.
[602] Ibid.
[603] Ibid.

right. However, if this is no easy task in the physical world, it is even more complicated in the cyberspace, which disregards geopolitical divisions and extends all over the globe.

As far as the jurisdictional matter at the CoE level is concerned, we saw how the tendency to confer a prominent role to the most classical jurisdictional principle, that is territoriality, is respected despite the complications that are caused by the peculiarities of the cyberspace. Still, the nationality principle is explicitly referred to and accepted as jurisdictional basis. In addition to that, the Budapest Convention does not exclude the application of other principles of jurisdiction, allowing for the potential application of all of the five principles we took into analysis.

A similar framework is proposed by the Stanford Draft, which however provides Member States with a hierarchy of the jurisdictional principles; yet allowing for the application of all of them, just like the Budapest Convention.

In the light of our analysis, it could be claimed that the choice to respect the prominence of territoriality, first, and nationality, in the second place, despite the difficulties that arise in their application to the cyberspace; might be caused by the fact that other jurisdictional principles, such as the protective and universality one, are actually more easily applicable to the cyberspace, but at the same time they are still animatedly debated.

Conclusions

This research was driven by two main questions: what is cyberterrorism? Is this threat covered by the Council of Europe existing international legal instruments? The investigation started with an overview of the most plausible manifestations of cyberterrorism, based on two factors. First and most important, in order to identify something as possible target of cyberterrorism, the cyber component needs to play a relevant role and not just a marginal one. Otherwise, if the cyber aspect did not play such a pivotal role for the proper functioning of the target it would not even make sense to ponder the deployment of a cyberattack with a terrorist *mens rea*. Second, the means and knowledge to exploit such cyber element need to be realistically available and not impossible to achieve for any kind of actor.

After having ascertained that several and differentiated scenarios meet these two criteria and are therefore deemed to be a concrete threat to civil society we moved on to the theoretical aspect regarding cyberterrorism, by focusing on the definitional matter. Despite of the fact that the previous statement is agreed on by international organisations as well as by experts of the field and that cyberterrorism is recognised, more or less openly, as a concern for the peace and security of the international community; no broad consensus on the matter has been reached yet. As a matter of fact, the academic field is still divided between two contrasting approaches: on the one hand it is claimed that cyberterrorism should be defined in a restrictive way, in order to avoid the overlapping of this new concept with other ones; while, on the other hand it is claimed that a broader categorisation of cyberterrorism would allow to tackle this issue in a more efficient way. Despite the lack of consensus, the most relevant definitions advanced by scholars have been analysed and evaluated.

The lack of a definition of cyberterrorism characterises international law as well and not just the academic debate. As a matter of fact, no definition of the issue at stake has been provided and a broad consensus on the matter seems to be still far to reach. The difficulties in reaching an international consensus on the definition of cyberterrorism are rooted in the pre-existing difficulties in defining the two constituent elements of cyberterrorism: cyberspace and terrorism. As far as the former is concerned, no universally agreed definition has been established yet and most of the international legal instruments addressing criminality in the cyberspace tend to define the illicit conducts perpetrated on the cyberspace that need to be criminalised, and skip the matter of

defining what is meant by cyberspace. If we move on to the second constitutive element, the situation does not change, or at least it does not change for the better. Indeed, no consensus definition of terrorism has been established either. The international community has made a long-lasting effort in order to try and solve this deadlock, also by trying to outline, at the United Nations level, a treaty criminalising terrorism per se[604], instead of criminalising it by targeting the manifestations that international community has experienced so far. However the *impasse* still remains and the UN sectoral framework on terrorism is still the one that is referred to by other international organisations, when addressing the terrorist threat. However, if some argue that the difficulties that arise in the process of defining terrorism are still too complicated to solve, other argue that the latest events in the field of terrorism, such as the attacks perpetrated by the Islamic State, pushed the international community towards a higher degree of consensus that might facilitate the task of finding a broadly accepted definition for terrorism[605]. Such a development might play a pivotal role in the field cyberterrorism, because the establishment of a consensus definition of terrorism would solve one of the main problems that are currently hindering the outlining of the definition of the object of our analysis.

Nonetheless, there is no guarantee that this deadlock will be solved any time soon; whereas it is widely agreed that cyberterrorism consists of an imminent threat to the international community. For this precise reason, we took into analysis two Council of Europe Conventions and one Additional Protocol that are linked to the issue of cyberterrorism. On the basis of our analysis of the CoE Convention on Cybercrime and its Additional Protocol on Xenophobia and Racism, it can be claimed that these two international legal instruments criminalise the offences that are necessary in order to perpetrate a terrorist cyberattack. As a matter of fact, the offences established by the convention are considered to be the basic steps of any kind of cyberattack and, in the light of that, it can be inferred that the early stages of a cyberterrorist attack are covered by the Budapest Convention. As far as its additional protocol is regarded, we concluded that it is suitable to cover some of those activities that are referred to as *cyberterrorist support*, such as propaganda and the spreading of threats and insults. A remarkable

[604] UN General Assembly (2000= *Draft comprehensive convention on international terrorism*, fifty-fifth session, agenda item 166, p.3, available at https://digitallibrary.un.org/record/422477#record-files-collapse-header.
[605] De Vido, S. (2017) *The future of the draft UN Convention on international terrorism*, Journal of Criminological Research Policy and Practice, Vol. 3, Issue 3, pp. 233-247.

aspect of this international legal instrument is doubtlessly the framework for international cooperation that it establishes among High Contracting Parties. As a matter of fact, since cyberterrorism is a transnational threat that is perpetrated by means of or against the cyberspace, which disregards territorial borders, international cooperation might actually be the key for the tackling of cyberterrorism. This acknowledgement was driven by the fact that no single State can effectively address a threat that is so transnational in nature and that evolves at the pace of technology.

However, it is obvious that an international legal instrument that was not conceived for terrorist offences might be completely suitable in order to address the gravity of the matter. As a matter of fact, despite the lack of a consensus definition for terrorism, the relevance of the underlying *mens rea* seems to be consolidated[606] and this aspect is obviously not included in the Budapest Convention. That is why we took into analysis the CoE Convention on the Prevention of Terrorism. As it emerged for the analysis of the most relevant provision of the Treaty, the wording of the articles would allow their application to terrorist instances perpetrated by means of cyberspace. However, due to the fact that the Convention is not aimed at tackling the issue of cyberterrorism, the application of its articles to the issue at stakes results to be a matter of interpretation; leading to a case-by-case approach decided at sentencing level[607].

After assessing whether the application of the two aforementioned CoE international legal instruments to instances of cyberterrorism is possible, we moved on to the matter of cyberjurisdiction. If the assessment of jurisdiction under international law is a delicate task, the situation gets even more controversial when this concept is extended to the cyberspace. As a matter of fact, despite of the relevant changes that took place in the international community, the current jurisdictional framework is still based on the principles that were established in the Harvard Draft of 1935. Needles to say that back then the use of the cyberspace for the perpetration of a terrorist attack could only be conceive ad science fiction. For this precise reason the application of the existing jurisdictional framework presents a series of difficulties. The latter were taken into analysis after providing an overview of the five jurisdictional principles and its evolutions. It emerged that, despite the peculiarities of the cyberspace and its unique

[606] De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova: Cedam, vol. 7, pp. 2-10.
[607] Draetta, U. (2005) *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism*, edited by A. Bianchi, Studies in International Law, pp. 453-464.

nature, a tendency consolidated in States' praxis. As a matter of fact, States as well as international organisations tend to respect the prominence that is conferred to the territoriality principle, immediately followed by the nationality principle. As it emerged from our analysis, the jurisdictional basis that is established by the Council of Europe indeed sets forth the territoriality principle as main reference and the nationality principle as alternative. Such prominence might seem controversial, due to the fact that the territorial localisation and nationality of the user can be easily hidden when operating in the cyberspace. Notwithstanding the possibility circumvent these two principles, they still prevail on the protective and universality principles. However, the application of the latter is not excluded by the CoE international legal instruments as they allow High Contracting Parties to apply other jurisdictional basis, provided that they are included in their national legislations. The application of other principles of jurisdiction, such as the protective and universality one, would actually be more practical. Nonetheless, such a choice would imply a series of other difficulties, such as the overlapping of different jurisdictional claims leading to conflicts of jurisdiction. The fact that such conflicts are likely to poison international relations is probably on the reasons that allowed the territoriality and nationality principles to keep prevailing on the other principles, despite the changes and developments in international community.

On the basis of our analysis, it results to be clear that the existing CoE legal framework grants only partial coverage to the issue of cyberterrorism. Still, it needs to be recognised that this is a good starting point, considering the fact that we are dealing with international legal instruments that were not purposefully designed for the matter of cyberterrorism. In addition to that, the Budapest Convention is internationally recognised as the most prominent treaty dealing with criminality in the cyberspace and it enjoys a relatively high level of ratification; considering the fact that the Council of Europe is a regional institution. As a matter of fact, the Convention on Cybercrime can be ratified also by non-Member States allowing, at least potentially, for its ratification extend far beyond Europe.

In the light of these acknowledgments, we claim that a good way to try and fill the legislative gap that characterises the issue of cyberterrorism could be to add a further additional protocol to the CoE Convention on Cybercrime. Such a solution would have more than one positive implication and would be feasible in a considerably shorter time span, that the one that would be needed in order to outline a brand new treaty and its

entry into force. Considering the incredibly high speed at which technology evolves and, as a consequence, the possibility of exploitation of the cyberspace multiply, the relatively less time that would be required plays a crucial role in the fight against cyberterrorism. On top of that, the Council of Europe is currently undertaking an effort to reform the Budapest Convention to broaden its scope and the inclusion of the criminalisation of cyberterrorism would doubtlessly meet this aim.

The choice of an additional protocol as means to tackle the threat of cyberterrorism would avoid the risk of overlapping with pre-existing provisions, such as those ones included in the Budapest Convention that are enough to tackle the basic steps of a cyberterrorist attack. Furthermore, the outlining of an additional protocol would not bind High Contracting Parties that already ratified the Convention on Cybercrime, due to the fact that ratification is required for additional protocols just like it is required for treaties. As a matter of fact, in the second chapter we highlighted the fact that the matter of xenophobia and racism in the cyberspace was dealt with by means of an additional protocol precisely due to the fact that there was no consensus opinion on the matter and including this topic in the Convention would have hindered a wide ratification. The same reasoning could be worth for the matter of cyberterrorism. Amending the Convention in order to add the criminalisation of cyberterrorism could indeed be a hazardous move, leading many States to withdraw from the treaty. On the contrary, addressing the matter in an additional protocol would not damage the ratification rate of the Budapest Convention, in such a way that at least the partial coverage of the matter that is granted by the Convention remains in place even though a State chooses not to ratify the additional protocol.

A part from criminalising the threat of cyberterrorism in a direct way, an additional protocol to the Convention on Cybercrime would also be useful in order to better regulate the matter of cyberjurisdiction. As a matter of fact, some scholars claim that the protective and universality principles are the most suitable ones in order to face the threat of cyberterrorism, but, as stated above, these approaches often imply multijurisdictional claims. Article 22 of the Budapest Convention sets forth that States claiming jurisdiction over the same matter are required to confront among each other in order to assess the best way to proceed; an additional protocol could use this article as a good starting point to go more into depth in this aspect and try and find a more efficient

solution to conflicts of jurisdiction that does not poison international relations, such as the submitting of the dispute to an international court.

Last but not least, recalling the possible scenarios we outlined in the first chapter, the damages caused by a cyberterrorist attack could be devastating, leading to the loss of human lives and the destruction of the core infrastructures of contemporary society. For this precise reason, taking a preventive approach to the matter, by outlining an international legal instrument in order to address the threat before it concretises could be worth the effort. As a matter of fact, as we have seen in the second chapter, the existing sectoral framework on terrorism established at the UN level was established mainly on a responsive basis. Considering the highly detrimental damage that a cyberterrorist attack would cause to society as a whole, taking a preventive approach and tackling the issue in advance would have positive implications for the international community, among which the possibility that such an additional protocol exerts the role of a deterrent. Such a preventive approach, has already been adopted by the CoE in the Case of the Convention on the Prevention of Terrorism, which, as we have seen in chapter two can apply to those activities that are considered to be support activities to cyberterrorism. Therefore, the fact that it already belongs to the praxis of the Council of Europe could allow to conceive its use also in the case of an Additional Protocol to the Convention on Cybercrime on the fight against cyberterrorism.

Bibliography

Akhagar, B., & Brewster, B. (2016) *Combatting Cybercrime and Cyberterrorism: Challenges, Trend and Priorities*, Advanced Science Technology for Security Applications, Springer.

Akhgar, B., Bosco, F., & Staniforth, A. (2014) *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Syngress.

Amnesty International (2001) *Universal Jurisdiction: The duty of states to enact and enforce legislation*, available at https://www.amnesty.org/download/Documents/128000/ior530032001en.pdf.

Armstrong, D. (2011) *Routledge Handbook of International Law*, Routledge International Handbooks.

August, R. (2002) *International Cyber-Jurisdiction: A Comparative Analysis*, American Business Law Journal, vol. 39, pp. 531-573, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-1714.2002.tb00305.x.

Aust, A. (2005) *Handbook of International Law*, Cambridge.

Austin, G., & Gady, F. S. (2010) *Russia, the United States and Cyber Diplomacy: Opening the Doors*, East West Institute, available at https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

Balough, C. D., &. Balough, R. C (2013) *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, Business Law Today, Business Law Section, available at https://www.balough.com/wp-content/uploads/2013/12/Cyberterrorism-on-Wheels_-Are-Today%e2%80%99s-Cars-Vulnerable-to-Attack_-_-Business-Law-Section.pdf.

Bansted, G. (2012) *Hi terrorist financing and the Internet: dot com danger*, Information & Communications Technology Law, Vol. 21, Issue 3, pp. 237-256.

Barlow, J. P. (1996) *A declaration of the Independence of Cyberspace*, available at https://scholarship.law.duke.edu/dltr/vol18/iss1/2/.

Bianchi, A. (2004) *Enforcing International La Normas Against Terrorism*, Hart Publishing, First Ed.

Bogdanoski, M., & Petreski, D. (2013) *CYBER TERRORISM– GLOBAL SECURITY THREAT*, International Scientific Defence, Security and Peace Journal, Vol. 13, Issue 24, pp. 59-73.

Brenner, S. W. (2007) *"AT LIGHT SPEED": ATTRIBUTION AND RESPONSE TO CYBERCRIME/TERRORISM/WARFARE*, Journal of Criminal Law & Criminology 379, Northwestern University, School of Law.

Breuer, M., & Schmal, S. (2016) *The Council of Europe: Its Law and Policies*, Oxford.

Brickey, J. (August 2012) *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, CTC Sentinel, Vol. 5, Issue 8, pp. 5-6, available at https://www.researchgate.net/publication/235782714_Defining_Cyberterrorism_Capturing_a_Broad_Range_of_Activities_in_Cyberspace.

Bruce, S. L., Flynn, S. M., & McConnell, C. R. (2010) *Essenziale di economia*, Milan: McGraw-Hill, second edition.

Brunst, P. W., & Sieber, U. (2007) *Cyberterrorism- the use of internet for terrorist purposes*, Strasbourg: Council of Europe Publishing.

Casale, D. (2008) *EU Institutional and Legal Counter-Terrorism framework*, Defence against Terrorism Review, Vol. 1, No. 1, pp. 49-77, available at https://www.tmmm.tsk.tr/publication/datr/volume1/04-EU_Institutional_and_Legal_Counter-terrorism_Framework.pdf.

Cassese, A. (2013) *Diritto internazionale*, Bologna: Il Mulino.

Chen, T., Jarvis, L., & McDonald, S. (2014) *Cyberterrorism- Understanding, Assessment and Response*, New York: Springer.

Clough, J. (2014) *A world of difference: the Budapest Convention on cybercrime and the challenges of harmonisation*, Monash University Law Review, Vol. 40, No. 3, available at https://www.researchgate.net/publication/277892666_A_World_of_Difference_The_Budapest_Convention_On_Cybercrime_And_The_Challenges_Of_Harmonisation.

Cohen, A. (2010) *Cyberterrorism: Are We Legally Ready?*, Journal of International Business and Law, Vol. 9, No. 1, pp. 1-40.

Collin, B. (1997) *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, Crime and Justice International, Vol.13, Issue 2, available at http://www.crime-research.org/library/Cyberter.htm.

Combs, C. C. (2018) *Terrorism in the Twenty-first Century*, Routledge, eighth edition.

Conway, M. (2004) *Cyberterrorism: Academic Perspectives*, 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK.

Conway, M. (2002) *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet*, Trinity College Dublin, Ireland, First Monday, Vol. 7, No. 11, available at http://doras.dcu.ie/498/1/first_mon_7_11_2002.pdf.

Conway, M. (2007) *Cyberterrorism: Hype and Reality*, in Armistead, Leigh, (ed.) Information warfare: separating hype from reality. Potomac Books, Inc., pp. 73-93.

Conway, M. (2018) *Is cyberterrorism a real threat? Yes: why we should start from this assumption*. In: Jackson, Richard and Pisoiu, Daniela, (eds.) Contemporary Debates on Terrorism (2nd edition). Routledge (Taylor & Francis), Abingdon and New York, pp. 102-108, available at http://doras.dcu.ie/22241/.

Cottim, A. A. (2013) *Cybercrime, Cyberterrorism and Jurisdiction : An Analysis of Article 22 of the COE Convention on Cybercrime*, European Journal of Legal Studies, Vol. 2, No. 3, 2013, pp. 55-79.

Cybercrime Convention Committee (2020) *The Budapest Convention on Cybercrime: benefits and impact in practice*, Strasbourg, available at https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

De Vido, S. (2012) *Il contrasto del finanziamento al terrorismo internazionale. Profili di diritto internazionale e dell'Unione europea*, Padova: Cedam, vol. 7.

De Vido, S. (2017) *The future of the draft UN Convention on international terrorism*, Journal of Criminological Research Policy and Practice, Vol. 3, Issue 3, pp. 233-247, available at https://doi.org/10.1108/JCRPP-09-2016-0020.

De Vido, S. (2019) *All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive*, in DPCE Online, vol. 38, pp. 59-76.

Denning, D. E. (2001) *Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, in J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defence Research Institute RAND, pp. 289-288, available at https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.

Dickinson, D. E. (1935) *Draft Convention on Jurisdiction with Respect to Crime*, American Journal of International Law, Vol. 29, art. 3, p. 480, available at https://www.jstor.org/stable/i312472#:~:text=Description%3A,journal%2C%20published%20quarterly%20since%201907.&text=The%20Journal%20also%20contains%20analyses,U.S.%20practice%20in%20international%20law.

Douglas, C. A., Griffith, C.,. Murray, G. R, Heslen, J. J., Davies, K. L., Hunter, Y., Jilani-Hyler, N., & Ratan, S. (2019) *Towards Creating a New Research Tool: Operationally Defining Cybeterrorism*, Augusta University.

Elngar, A. (2018) *IT-based Efficient Tamper Detection Mechanism for Healthcare Application*, International Journal of Network Security, Vol.20, No.3, pp. 489-495, available at https://www.researchgate.net/publication/323935849_IoTbased_Efficient_Tamper_Detection_Mechanism_for_Healthcare_Application.

Fenz, S. (2005) *Cyberspace Security: a Definition and a Description of Remaining Problems*, University Vienna - Institute of Government & European Studies.
Ford, R., & Gordon, S. (November 2002) *Cyberterrorism?*, in Computers & Security, Vol. 21, No. 7, pp. 636-647, available at https://www.researchgate.net/publication/222546033_Cyberterrorism.

Financial Action Task Force (2014) *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, available at https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Gable, K. E. (2010) *Cyber Apocalypse-Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, Vanderbilt Journal of Transnational Law, Vol. 43, no. 10, pp. 57-118.
Giacomello, G. (2004) *Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism*, Studies in Conflict & Terrorism, Vol. 27, pp. 387-408.

Giantas, D., & Stergiou, D. (2018) *From Terrorism to Cyber-terrorism: The Case of ISIS*, Hellenic Institute of Strategic Studies, pp. 1-32, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927.

Goldman, M. G., & Stockton, P. N. (2014) *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, Stanford Law & Policy Review, Vol. 25, pp. 211-268, available at https://law.stanford.edu/wp-content/uploads/2018/03/stocktongoldman.pdf.

Helmbrecht, U. (2017) *ENISA overview of cybersecurity and related terminology*, version 1, European Union Agency for Network and Information Security, available at https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

Hirsh-Hoefler, S., Pedahzur, A., & Weinberg, L (2004) *The Challenges of Conceptualizing Terrorism*, in Terrorism and Political Violence, Vol. 16, No. 4, pp. 777-794.

Hiryaev, Y. S. (2012) *Cyberterrorism in the Context of Contemporary International Law*, San Diego International Law Journal, Vol.14, no. 1, p. 141.

Hmoud, M. (2006) *Negotiating the Draft Comprehensive Convention on International Terrorism: Major Bones of Contention*, Journal of International Criminal Justice, Vol. 4, Issue 5, pp. 1031–1043, available at https://doi.org/10.1093/jicj/mql081.

Hoffman, B., & Riley, K. J. (1995) *Domestic Terrorism: A National Assessment of State and Local Preparedness*, supported by the National Institute of Justice, US Department of Justice, RAND, available at https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR505.pdf.

Hopkins, S. L. (2003) *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, Journal of High Technology Law, Vol. 2, No. 1, pp. 101-122.
Hunt, A. (2006) *The Council of Europe Convention on the Prevention of Terrorism*, European Public Law 603, Vol. 12, No. 4, available at https://www.researchgate.net/publication/228209564_The_Council_of_Europe_Convention_on_the_Prevention_of_Terrorism.

Hunt, J. (2011) *The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them*, Information & Communications Technology Law, Vol. 20, No. 2, pp. 133-152.

Iqbal, M. (2004) *Defining Cyberterrorism*, in The John Marshall Journal of Information Technology & Jerome, O. U. (2012) *Russia and the Council of Europe Convention on Cybercrime*, Computer and Telecommunication Law Review, pp. 16-17, available at

https://www.researchgate.net/publication/322083052_Russia_and_the_Council_of_Europe_Convention_on_Cybercrime.

Jongman, A., Schmid, A. *et al.* (1988) *Political Terrorism: A New Guide To Actors, Authors, Concepts, Data Bases, Theories, And Literature*, Transactions Publishers.
Kaspersen, H. W. (2009) *Cybercrime and Internet jurisdiction*, Discussion paper (draft) of the Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, available at https://rm.coe.int/16803042b7.

Kavanagh, C. (2017) *The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century*, UNIDIR Resources, available at https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

Kenney, M. (2015) *Cyber-Terrorism in a Post-Stuxnet World*, Orbis, Vol. 59, Issue 1, pp. 111-128, available at https://www.sciencedirect.com/science/article/pii/S0030438714000787.

Kerttunen, M., & Tikk, E. (2020) *Rutledge Handbook of International Cybersecurity*, Routledge International Handbooks.

Kramer, F. D. (2009) *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in Franklin D. Kramer, S. Starr and L. K. Wentz, eds., *Cyberpower and National Security*, Washington DC: National Defence University.

Kyriakopoulos, G. D. (2017) *Cyber-attack, Cyber-warfare: arranging definitions*, in J.-P. Jacqué, F. Benoît-Rohmer, P. Grigoriou & M.-D. Marouda (Eds.), Liber Amicorum Stelios Perrakis, I. Sideris, Athens, pp. 497-511.

Leach, P. (2017) *Taking a Case to the European Court of Human Rights*, Oxford, fourth edition, student version.

Lewis J. (2004) *Cultural Studies - The basics*, SAGE Publications.

Lorents, P., & Ottis, R. (2011) *Cyberspace :Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, available at https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf.

Manap, N. A., & Tehrani, P. M. (2013) *A rational jurisdiction for cyber terrorism*, Computer Law & Security Review, Vol. 29, pp. 689-701, available at https://www.sciencedirect.com/science/article/abs/pii/S0267364913001362.

Manap, N. A., Taji, H., & Tehrani, P. M. (2013) *Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime*, Computer Law & Security Review, Vol. 29(3), pp. 207-215.

Martin, C., & Schell, B. (2006) *Websters' New World Hackers Dictionary*, Wiley Publishing Inc.

Mayer, M., Martino, L., Mazurier, P., & Tzvetkova, G. (2014) *How would you define Cyberspace?*, Pisa, available at https://www.academia.edu/7097256/How_would_you_define_Cyberspace.
Menthe, D. C. (1998) *Jurisdiction in Cyberspace: A Theory of International Spaces*, Michigan Telecommunications and Technology Law Review, Vol. 4, Issue 1, 1998, pp. 69-103.

Nelson B. *et al*, (1999) *Cyberterror: Prospects and Implications*, Centre for the Study of Terrorism and Irregular Warfare, Monterey, CA, available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a393147.pdf.

Pollitt, M. M. (February 1998). *Cyberterrorism- Fact or Fancy?* Computer Fraud & Security, Vol. 8, issue 2, pp. 8-10.

Rahman, M. O. (2008) *Towards Understanding Personal Jurisdiction in Cyberspace*, International Journal of Law and Management, pp. 105-120, available at https://www.emerald.com/insight/content/doi/10.1108/17542430810877445/full/pdf?casa_token=99nCe0YmCPMAAAAA:lSNO0yjT9Y4zU6t-JEX3Rw5JGj4E7U69pvdF0-7swnrFmzbR1cdmG1jD2lg4KKqk13bMhKw9kpd8aeDiUTWwuDQCnkxZJmiI8IvvKzexIaJPHwd39Mo.

Rapoport, D. C. (2008) *The four waves of modern terrorism*, In *Terrorism Studies: A Reader*, eds. John Horgan and Kurt Braddock, pp. 46-73, available at https://www.international.ucla.edu/media/files/Rapoport-Four-Waves-of-Modern-Terrorism.pdf.

Ryngaert, C. (2015) *Jurisdiction in International Law*, Oxford, Second Ed.

Saul, B. (2015) *Defining Terrorism: a Conceptual Minefield*, Sydney Law School, Legal Studies Research Paper, No. 15/84.

Seger, A. (2012) *The Budapest Convention 10 years on: lessons learnt*, in Cybercriminality: finding a balance between freedom and security, ISPAC International Scientific and Professional, Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme, edited by S. Manacorda.

Sofaer, D. A., & Goodman, S. E (2000) *A Proposal for an International Convention on Cyber Crime and Terrorism*, Stanford, pp. 25-45, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf.

START (2019) *Global Terrorism Database. Codebook: inclusion criteria and variables*, available at https://www.start.umd.edu/gtd/downloads/Codebook.pdf.

Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*, Oxford.

Vassilys, F. (2004) *What is 'Cyberspace'?*, available at https://www.researchgate.net/publication/328928631_What_is_'cyberspace'#:~:text=is%20'cyberspace'%3F-,Vassilys%20Fourkas,use%20in%20Gibson's%20novel%20Neuromancer.

Vatis, M. A. (2010) *The Council of Europe Convention on Cybercrime*, available at http://www.nap.edu/catalog/12997.html.
Vellinga, N. E. (2017) *From the testing to the deployment of self-driving cars: Legal challenges to policymakers on the road ahead*, Computer Law & Security Review 33, pp. 847-863.

Weber, A. M. (2003) *The Council of Europe's Convention on Cybercrime*, in Berkley Technology Law Journal, Vol. 18:425, available at https://btlj.org/?s=The+Council+of+Europe%27s+Convention+on+Cybercrime&submit=Search.

Weimann, G. *www.terror.net* - *How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report, available at https://www.usip.org/sites/default/files/sr116.pdf.

Wilson, C. (2008) *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service.

Zappa, F. (2014) *Cybercrime: risks for the economy and the enterprises at the EU and Italian level*, United Nations Interregional Crime and Justice Institute, available at http://www.unicri.it/in_focus/files/Cybercrime_and_the_Risks_for_the_Economy_Flavia_Zappa_2015_06_11.pdf.

Conferences

Rossi, S. (25 March 2019) *Moneta e banche: le origini strutturali della crisi*, Conference held at Ca' Foscari University of Venice, stable URL https://www.unive.it/data/16437/1/26936.

Conway, M. (28-29 June 2004) *Cyberterrorism: Academic Perspectives*, 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, pp. 41-50.

International legal instruments

Council of Europe (1949) *Statute of the Council of Europe*, London, available at https://rm.coe.int/1680306052.

Council of Europe (1950) *Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.

Council of Europe (1978) *European Convention of the Suppression of Terrorism*, ETS No. 90, Strasbourg, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800771b2.

Council of Europe (2004), *Explanatory Report to the Convention on Cybercrime – CETS No. 185*, Budapest, available at https://rm.coe.int/16800cce5b.

Council of Europe (2006) *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems – CETS No. 189*, Strasbourg, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

Council of Europe (2006) *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, Strasbourg, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680989b1c.

Council of Europe (2007) *Convention on the Prevention of Terrorism CETS No. 196*, Warsaw, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.

Council of Europe (2007) *Explanatory Report to the Convention on the Prevention of Terrorism – CETS No. 196*, Warsaw, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3811.

Council of Europe Committee of Ministers (1989) *Recommendation No. R. (89) 9 on Computer-related Crime*, available at https://dig.watch/instruments/recommendation-no-r-89-9-committee-ministers-member-states-computer-related-crimes.

Council of Europe, (2004) *Convention on Cybercrime ETS No. 185*, Budapest, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Council of Europe, (2007) *Appendix – Council of Europe Convention on the Prevention of Terrorism*, Warsaw, available at https://rm.coe.int/168008371b.

Council of the European Union (1999), *Common Position 1999/364/JHA*, Official Journal of the European Communities, available at https://op.europa.eu/en/publication-detail/-/publication/42be716f-31a9-444f-afe0-56c6929f78b3.

Council of the European Union (2001) *Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism*, Official Journal of the European Communities, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0093:0096:EN:PDF.

Council of the European Union (2002) *Council Framework Decision 2002/475/JHA on combating terrorism, Official Journal of the European Union*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN.

European Parliament (2015) *Understanding definitions of terrorism*, Briefing European Parliamentary Research Service, available at https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS_ATA(2015)571320_EN.pdf.

European Union (2001) *Proposal for a Council framework Decision on combating terrorism*, Official Journal 332 E, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52001PC0521:EN:HTML.

International Law Commission (1996) *Draft Code of Crimes against the Peace and Security of Mankind*, available at https://legal.un.org/ilc/texts/instruments/english/draft_articles/7_4_1996.pdf.

Office of the United Nations High Commissioner for Human Rights, (2008) *Human Rights, Terrorism and Counter-terrorism*, Geneva, pp. 3-7, available at https://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf.

UN General Assembly (1995) *A/RES/49/60 Measures to Eliminate International Terrorism*, forty-ninth session, agenda item 142, p. 4, available at https://undocs.org/en/A/RES/49/60.

UN General Assembly (1970) *Declaration of principles of International law friendly relations and co-operation among States in accordance with the Charter of the United Nations*, available at https://www.un.org/ruleoflaw/files/3dda1f104.pdf.

UN General Assembly (1997) *Measures to eliminate international terrorism: resolution / adopted by the General Assembly A/RES/51/210*, 51st Session, available at https://www.refworld.org/docid/49997ae127.html.

UN General Assembly (2000) *Draft comprehensive convention on international terrorism*, fifty-fifth session, agenda item 166, available at https://digitallibrary.un.org/record/422477#record-files-collapse-header.

UN General Assembly (December 1999) *International Convention for the Suppression of the Financing of Terrorism*, in resolution 54/109, art. 2.1(b), available at https://www.un.org/law/cod/finterr.htm.

UN Genral Assembly (1996) *International Covenant on Civil and Political Rights*, available at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

UN Security Council (2001) *Resolution 1373*, available at https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf.

UN Security Council (2004) *Resolution S/RES/1566*, available at https://www.un.org/ruleoflaw/files/n0454282.pdf.

UN Security Council (2014) *Resolution 2178*, available at https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2178.pdf.

United Nations (1970) *Convention for the Suppression of Unlawful Seizure of Aircraft*, The Hague, available at https://treaties.un.org/doc/db/Terrorism/Conv2-english.pdf.

United Nations (1971) *Convention for the suppression of unlawful acts against the safety of civil aviation*, Montreal, available at https://treaties.un.org/doc/Publication/UNTS/Volume%20974/volume-974-I-14118-English.pdf.

United Nations (1973) *Convention on the Prevention and Punishment of Crimes Against Internationally protected Persons*, *including Diplomatic Agents*, available at https://legal.un.org/ilc/texts/instruments/english/conventions/9_4_1973.pdf.

United Nations (1979) *International Convention Against the Taking of Hostages*, available at https://treaties.un.org/doc/db/terrorism/english-18-5.pdf.

United Nations (1982) *Convention on the Physical Protection of Nuclear Material*, Vienna available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub615web.pdf.

United Nations (1982) *Convention on the Physical Protection of Nuclear Material*, Vienna available at https://www-pub.iaea.org/MTCD/Publications/PDF/Pub615web.pdf.

United Nations (1988) *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, Rome, available at https://treaties.un.org/doc/db/Terrorism/Conv8-english.pdf.

United Nations (1988) *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*, Montreal, available at https://treaties.un.org/doc/db/Terrorism/Conv7-english.pdf.

United Nations (1999) *Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf*, New York, available at https://treaties.un.org/doc/Publication/UNTS/Volume%201678/v1678.pdf.

United Nations (2013) *Report of the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996*, available at https://undocs.org/A/68/37.

United Nations, (October 2009) *Tackling the Financing of Terrorism*, CTITF Working group report, CTITF publication series, available at https://www.un.org/counterterrorism/ctitf/sites/www.un.org.counterterrorism.ctitf/files/ctitf_financing_eng_final.pdf.

Web references

Cambridge dictionary, *Cyberspace*, stable URL: https://dictionary.cambridge.org/it/dizionario/inglese/cyberspace, last accessed 26 February 2020.

Christensson, P. (2006) *Cyberspace Definition*, stable URL https://techterms.com, last accessed 4 March 2020.

Council of Europe, *Budapest Convention and related standards*, stable URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention, last accessed 26 July 2020.

Council of Europe, *Chart of signatures and ratifications of Treaty 185*, stable URL https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=f1bIKBSP, last accessed 29 July 2020.

Council of Europe, *Chart of signatures and ratifications of Treaty 189*, stable URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=Q8wGkgaa, last accessed 10 August 2020.
Council of Europe, *Chart of signatures and ratifications of Treaty 196*, stable URL https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196/signatures?p_auth=AbrF0dEE, last accessed 22 August 2020.

Council of Europe, *Council of Europe action against Cybercrime*, stable URL https://www.coe.int/en/web/portal/coe-action-against-cybercrime, last accessed 24 January 2020.

Council of Europe, Council of Europe Committee on Counter-Terrorism, stable URL https://www.coe.int/en/web/counter-terrorism/cdct, last accessed 10 April 2020.

Council of Europe, *Details of Treaty No. 185 – Convention on Cybercrime*, stable URL https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, last accessed 15 April 2020.

Council of Europe, *European Committee on Crime Problems*, stable URL: https://www.coe.int/en/web/cdpc/home, last accessed 10 July 2020.

Kauffman, J. (2019) *What Is Censorship Resistance, And Why Does It Matter?*, stable URL https://lbry.com/news/what-is-censorship-resistance-and-why-does-it-matter, last accessed 27 March 2020.

Legal Information Institute, *14th Amendment*, stable URL https://www.law.cornell.edu/constitution/amendmentxiv, last accessed 15 September 2020.

Merriam-Webster, *Legal Definition of Procedural Law*, stable URL: https://www.merriam-webster.com/legal/procedural%20law, last accessed 11 August 2020.

New America, *Appendix: the SDGs and Cybersecurity*, Securing Digital Dividends, stable URL https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/appendix-the-sdgs-and-cybersecurity/ , last accessed 21st March 2020.

Oxford Reference, stable URL https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095728554, last accessed 10 September 2020.

Purdy, E. R. (2019) Cyberterrorism, Salem Press Encyclopedia.

Security Council – Counter Terrorism Committee, *International legal* instrumemts, available at https://www.un.org/sc/ctc/resources/international-legal-instruments/ Last accessed 9 March 2020.

UN Office on Drugs and Crimes (2019) Hacktivism, stable URL: https://www.unodc.org/dohadeclaration/index.html, last accessed 20 July 2020.

United Nations Treaty Collection, *Glossary*, stable URL https://treaties.un.org/Pages/Overview.aspx?path=overview/glossary/page1_en.xml#:~:text=of%20Treaties%201969%5D-,Accession,treaty%20has%20entered%20into%20force, last accessed 18 July 2020.

Case Law

English Court of Appeal (2000) *R v Waddon*, available at https://www.lccsa.org.uk/r-v-graham-lester-ian-waddon-2000/.

European Court of Justice, (2010) *Joined Cases C-585/08 and C-144/09*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CA0585.

International Criminal Court (1970) Case Concerning *the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain),* available at https://www.icj-cij.org/files/case-related/50/050-19700205-JUD-01-00-EN.pdf.

Permanent Court for International Justice (1927) *The case of the s.s. "Lotus"*, Series A-No. 1, available at https://documents.law.yale.edu/sites/default/files/ss_lotus_-_pcij_-_1927.pdf.

United States Court of Appeal (2004) *Yahoo! INC V. La Ligue Contre le Racisme et L'Antisémitisme*, No. 01-17424, available at https://caselaw.findlaw.com/us-9th-circuit/1308396.html.

US District Court for the Western District of Pennsylvania (1997) *Zippo Manufacturing Company V. Zippo Dot Com, Inc*, 952 F. Supp. 1119, available at https://law.justia.com/cases/federal/district-courts/FSupp/952/1119/1432344/.