Themis competition 2015 edition

Semi-Final A – International Cooperation in Criminal Matters

International cooperation in the face of cyber-terrorism : current responses and future issues.

French team

Sylvia BODIN, Marc ECHILLEY and Odile QUINARD-THIBAULT

As the Internet has developed, become more accessible and taken on greater importance in our societies, terrorists have logically followed the trend and increasingly used it. But the combination of this new medium and the growing threat of global terrorism calls traditional legal responses into question and shakes them to the core.

States face three major difficulties in effectively responding to cyber-terrorism. The need to **identify** both criminals and territorial competence is greatly challenged by the loose and transnational structure of cyber-terrorist groups. The anonymity offered by the Internet shakes up both police investigations and the judicial principle of the individual nature of penalties. Similarly, the importance of **understanding** the methods and risks a criminal activity triggers is largely complicated by the highly technical nature of the devices and networks used, requiring specially trained experts in the fight against cyber-terrorism. The necessity of adequately **responding** to the terrorist cyber-threat is also defied by the rapidity of communications and the virtual nature of the information exchanged by terrorists over the Internet.

Furthermore, terrorism goes hand in hand with political demands or goals. Because liberal democracy is based on the allowance of free debate of political views, prosecutions based on the diffusion of terrorist messages or content on the Internet question the very core of our fundamental principles. The appropriate balance between civil liberties and the fight against assailants of our societies is hard to reach and always unstable. The first difficulty comes from the States' incapacity to reach an agreement on a universal definition of terrorism, although a European definition has been adopted. Logically, "cyber-terrorism" as a concept is greatly discussed. Some scholars argue that it should be limited to cyber-attacks carried out by terrorists whereas others contend that it should encompass all uses of the Internet for terrorist purposes. We will not address this semantic question: the fact that we have decided to use "cyber-terrorism" in its broad sense of use of the Internet for terrorist purposes is mostly for convenience.

This paper will focus on the responses that have been and should be made in reaction to the new challenges facing law enforcement in the light of cyber-terrorism. In addressing this issue, international cooperation has been and will be fundamental. It is obviously essential because the transnational nature of cyber-terrorism requires international investigations, but also, and above all, because the analysis, strategies and practices regarding this threat need to be set on common ground.

Regarding the numerous ways terrorists use the Internet, there has been an undisputable need to address these different types of behaviour collectively. By harmonising the incrimination of terrorism and cyber-crime and by collectively outlining new offences adapted to cyber-terrorism, international cooperation has brought about the coherence needed for responding to this issue (Section 1). On the basis of this agreement on the definition and incrimination of the phenomenon, European States have furthered international cooperation to respond to the cyber-terrorist threat via common strategies and tools (Section 2).

Thanks to this common understanding of cyber-terrorism and the common response, States may be able to fight cyber-terrorism effectively, while still respecting human rights.

I – IDENTIFYING TERRORIST BEHAVIOUR ON THE INTERNET

The Internet has multiplied terrorist capabilities, using it for the purposes of communication, propaganda, research, planning, publicity, fundraising and so on. It generally offers three kinds of benefits to terrorists: abundance of information, cheapness of communication and anonymity. However, violent organisations usually separate their operational wing, which requires anonymity, from their propaganda one that needs to be identified in order to reach a broad audience (Benson, 2014: 298). This report draws on this distinction.

A. Uses of the Internet for terrorist attack operational purposes: planning and fundraising

The most prevalent terrorist use of the Internet is probably communication. Cheapness of communication has enabled terrorists to exchange information more easily and to access valuable technical information such as anti-terrorist programmes, militant texts, maps, user manuals to build explosive devices, for instance, and even reports – freely available or hacked – from governmental institutions or companies detailing security weaknesses of key infrastructures (Brown and Korff, 2009: 121). In addition, the Internet might be a way to divert attention from real attack scenarios in order to mislead law enforcement (Thomas, 2003: 112-113).

The Internet has also eased terrorist financing – in cash, but also through non-traditional means such as electronic currencies (eg. Bitcoin, Peercoin, Dodgecoin) (Brantly, 2014). Fundraising is undertaken via three different means: direct solicitation, exploitation of charities and e-commerce, and online crimes. Already in 2002, for instance, Yahoo took fifty-five Jihad-related sites out of the Jihad Web Ring that promoted and organised donations for its cause (Conway, 2002). Furthermore, websites invite supporters to donate to supposedly humanitarian foundations, like The Benevolence International Foundation, which raised millions of dollars during the 1990's, and even benefited from tax-exemptions, while financing the 1993 World Trade Center bombing (Hinnen, 2004: 17). Similarly, some organisations rely on e-commerce, selling books, flags, DVDs or CDs (CoE, 2007: 38). Lastly, terrorists use the Internet to raise funds by stealing or using fake identities, and accessing bank and credit card accounts. In addition, terrorists can organise fund transfers thanks to convenient, fast and fluid online banking services – some of which do not require as much information as traditional banking systems, thus enabling laundering (Hinnen, 2004:38).

Insofar as the Internet offers new possibilities to violent organisations and multiplies terrorists' capabilities, it is often considered as a threat increase factor. Some authors, on the contrary, stress that state security actually gains at least as much capability from the Internet as violent groups do (Benson, 2014: 293): the Internet is a way to enhance counterterrorism through surveillance. Just as the terrorists henceforth publish and share more information than they used to, authorities access and exploit this new data. As a matter of fact, the Internet is not as anonymous as one might think: remaining anonymous in the long-term is proving difficult since most actions are likely to leave footprints.

However, the fight against terrorists on the Internet is dependent on the criminalisation of their activities. Incrimination must be specifically designed to encompass behaviour on the Internet and effective investigations and prosecutions, often based on international cooperation, require harmonisation of national legislations. In this context, two approaches have been adopted: one of cybercrime, the other of counter-terrorism. Concerning cyber-crime, 45 countries – including the United States – have signed the Council of Europe's Convention on Cybercrime (CoE, CETS No.: 185, 2001). It is the first international treaty which incriminates specifically computer-related crimes (see. *Infra, section 1, C*) (Archick, 2002: 3). Nevertheless, many of its legal provisions are not limited to cyber-crimes but extended to any offence which has to be proved with "electronic form" evidence (see *infra, section 2, B*). The counter-terrorism approach, on a global scale, has been impeded because of the failure of States to agree on a common definition of terrorism. Thirteen UN Conventions adopted in the 60s incriminate only several specific terrorist forms of behaviour (Saulnier-

Cassia, 2014). On a European Union scale, cooperation has been more fruitful, even though law-making harmonisation seems difficult to foster, as it encounters national prerogatives. The Framework Decision of 13 June 2002 (2002/475/JHA, 2002) has enabled Member States to harmonise the definition of terrorism and to align their legislation. In particular, it requires Member States to criminalise the direction of a terrorist group and the participation *"in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group"* (art. 2). This provision is perfectly applicable to the planning and financing of attacks via the Internet. Regarding the last issue, in addition to UN texts – The International Convention for the Suppression of the Financing of Terrorism adopted in 1999 and UN Security Resolution 1373 – the Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime includes provisions concerning the adoption of laundering offences (art 6), though excluding most terrorist financing as it does not cover financing with legally obtained funds. These instruments are found to be applicable to acts committed online.

Accordingly, international legal provisions do not incriminate cyber-terrorism precisely. But by combining incrimination of terrorist activities in general with the incrimination of specific cyber-crimes, European criminal law – and, to some extent, international criminal texts – manage to embrace operational activities of terrorists on the Internet. Moreover, counter-terrorism often leans on general law. Thus, international cooperation at European level has achieved the elaboration of a coherent and appropriate legal basis for combating terrorist operational activities on the Internet. A similar enterprise has been undertaken regarding propaganda and recruitment over the Internet, raising many issues over the potential danger for freedom of expression and information.

B. Uses of the Internet for terrorist strategic purposes: propaganda and recruitment

In addition to operational purposes, terrorists increasingly use the Internet to foster propaganda and recruitment: they can monitor their websites and therefore gather data that will enable them to target people likely to be future recruits. Moreover, multimedia is cheap, easy to use and appealing to the young and less educated, while it provides supporters with a sense of belonging. With the Internet, violent organisations have become more independent from traditional media, on which former terrorist groups – such as the IRA – relied.

Nowadays, not only do extremist groups bypass journalists by communicating directly with their targets and potential recruits, but journalists also spread terrorist content, and sometimes even appalling images (Brown and Korff, 2009: 121-122). In this context, control of online terrorist content has affected the ability of the media to gather and share information, pointing out the limits on freedom of speech and information. The tension between counter-terrorism and these liberties is highlighted by the debates surrounding the harmonisation and expansion of offences dealing with propaganda and recruitment.

Even before 2001, most legal systems had criminal law provisions punishing incitement to crime, some of which had already adopted legislation against incitement to terrorism. The Council Framework Decision of 2002 as well as the 2005 COE Convention on Prevention of Terrorism obligated Member States to criminalise it.

Acknowledging the delicate balance between criminalising provocation and incitement, on the one hand, and protecting freedom of expression on the other, the COE Convention includes safeguards: harmonisation has to be carried out "while respecting human rights obligations, in particular the right of freedom of expression, of association and of religion" (art. 12). Thus, Member State legislation must conform to ECHR case law requirements: incitement can be prohibited only in limited circumstances, within a strict context (method of communication, size of audience, position of the speaker and so on). Moreover, even though many of the laws prohibiting incitement to terrorism do not require a crime to have been committed or attempted, the ECHR expects "evidence of any concrete action" that reveals the "prima facie intention of the speaker" (ECHR, 4 June 2002, Yagmurdereli v. Turkey). The Court also looks carefully at limitations to political speech, in order to avoid interference with the freedom of speech of opponents to the government or its opposing parties. Accordingly, citizens are allowed to criticise the government's counterterrorism actions freely (ECHR, 18 July 2002, Sener v. Turkey). Moreover, the ECHR generally reminds Member States that journalists cannot be held responsible for reporting the words of others (ECHR, 23 September 2004, Jersild v. Denmark).

However, many have been concerned that these texts will be used expansively to justify significant restrictions on protected speech – especially by countries embedded in violent controversy over territorial issues. Since the Convention was open to non-Council of Europe ratification, these countries have not therefore been submitted to the ECHR (Banisar, 2009: 39). More generally, States have had a different approach to the extent of the protection of freedom of expression – broadly speaking, divided between a European approach admitting more restriction of free speech to protect others' rights or interests, and the American approach. As a result, many controversies have arisen.

Firstly, during the drafting of the Convention on Cybercrime, free speech considerations prevented States reaching an agreement on the inclusion of provisions relating to the criminalisation of racism and xenophobic speech. Therefore, an *optional* Protocol on Xenophobia and Racism to the Cybercrime Convention, introduced in 2002, had to be adopted (Sieber, 2006: 420). Because it prohibits online racist speech, it can serve as a basis for legislation prohibiting hate speech that is terrorism-related.

Secondly, a discussion has emerged regarding the extent of the acts prohibited under counter-terrorist legislation. Following the path established by the 2005 COE Convention on Prevention of Terrorism, the EU 2002 Framework Decision was amended in 2008 to criminalise not only incitement but also "public provocation to commit a terrorist offence", "recruitment" and "training", in order to fight against the dissemination of terrorist content on the Internet (2008/919/JAI). Despite this text, Member States have not complied entirely with the obligation to criminalise public provocation, at least not to the extent required in the decision. Even further is the prohibition of glorification and praise. It concerns those who, without inciting terrorist action, "praise, support or justify terrorism" (CODEXTER, 2004). Criminalising such acts would impose even stricter limitations on freedom of expression. This controversial question has called for varied answers from Member States. Since none of the texts mentioned above requires States to criminalise praise for terrorism, only a few countries have prohibited it, including Denmark, France, the UK and Spain. Russia criminalised it and used it to prohibit journalists discussing counterterrorism policies.

C. Use of the Internet for cyber attacks

A third (mis)use of the Internet by terrorists needs to be considered, that is cyber-terrorism in its most narrow perspective[1]. Put schematically, terrorist cyber-attacks could have two major targets: data (that can be stolen or corrupted) and control systems (linked to physical infrastructure such as electricity, networks, water supplies and so on), especially SCADA (Supervisory Control and Data Acquisition). Whereas numerous sophisticated and damaging

[1] Denning defines it as "*unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives*" (Denning: 2000); also see (POLLITT, 1998: 8-10).

cyber-attacks have been reported hitherto[2], none of them seems to have had a real terror goal. Moreover, none of them has aimed at a critical infrastructure, mainly using for now the Denial of Service (DOS) technique. Scholars disagree on the likelihood of terrorist groups soon being able to master such kinds of attacks, this argument being based usually on four factors - cost, complexity, low destruction and media impact (CONWAY, 2014: 107-122). One can wonder, though, if the unlikelihood is not underestimated these days.

- ***Incrimination***: Considering the growing number of cyber-attacks States are facing and the serious damage they could trigger, there is a need for a legal response. The first international answer was the Council of Europe's Cybercrime Convention of 23.11.2001 (CETS No.: 185), which covers most kinds of data and computer interference that are prerequisite for terrorist cyber-attacks. Thus, the Convention requires its signatories to establish as criminal offences, intrusion techniques of interception and hacking of computer data (articles 2 and 3), as well as data and system interference (articles 4 and 5). As for the EU Council Framework Decision on Attacks Against Information Systems (2005/222/JHA), largely inspired by the Cyber Crime Convention, Member States are required to deem similar actions as criminal offences, such as illegally accessing information systems (article 2) or illegally interfering with data (article 4).

Unlike these "cyber-specific" approaches of cyber-terrorism, the EU Council Framework Decision on Combating Terrorism (2002/475/JHA) follows a terrorist-specific vision, focusing on the political intent of the attack. It requires the criminalisation of "*extensive destruction to a Government or public facility [...], an infrastructure facility, including an information system*", when committed with specified terrorist aims.

One wonders if these legal responses, dating back ten years, still offer sufficient protection, especially considering the rapid technological advances in this domain. By means of broad criminalisation, these international instruments actually seem to cover all serious and imaginable cyber-attacks. In fact, the real difficulty in this matter is the lack of universal consensus on the definition of punishable actions, and especially the absence in the ratification process of countries that are havens for cybercriminals.

- ***Protection of critical infrastructure****:* Stakeholders at European level have been very active in recent years in institutionalising cyber-security, competing with a traditionally national area

[2] Reported under massive cyber-attacks, several can be cited: the 1998 DOS Cyber Attack in Sri Lanka that flooded the country's embassies with 800 emails a day; the 2007 Estonian botnet Cyber Attack that disrupted the websites of the country's main institutions (government, ministries, news organisations and banks); the stuxnet worm discovered in 2010.

of responsibility (Argomaniz, 2014:7). Within the framework of the EU Critical Infrastructure Protection (CIP) Policies and its "institution-building" Strategy, various Actions Plans[3] have been elaborated to increase readiness in the face of cyber-attacks. In this regard, the inter-institutional Computer Emergency Response Team (CERT-EU) and the European Network and Information Security Agency (ENISA) both provide advice on good practices, assistance and expertise in the analysis of existing risks to Member States and European Authorities. On top of this, Europol set up a cyber-crime centre (EC3) in 2013, which among other things focuses on fighting cyber-attacks affecting information systems and critical infrastructure (EUROPEAN COMMISSION, 2012: 4).

With a view to reducing the vulnerability of critical infrastructure across Europe, ENISA carried out a "Cyber Europe 2010" exercise in November 2010, the first pan-European cyber stress test, gathering 30 participating Member States. "*The exercise increased [...] the understanding of how cyber incidents are handled [...] and demonstrated the need for efficient communications*" based on trust; "*The exercise has shown that the procedures on how to handle cyber incidents do not yet exist on a pan-European level. Such procedures need to be identified and tested in future such exercises*" (ENISA, 2011: 8).

International level: Regarding the need for protection of national and international infrastructure notably by means of cyber deterrence, the military approach of international cooperation is frequently called upon (DOGRUL, ASLAN, CELIK, 2011: 39-40). With this in mind, NATO could play a key role in building a "cyber-attack defence shield" (NATO, 2010: 5), which it already does via several organisations[4]and projects, such as the Computer Incident Response Capability project (NCIRC).[5]

At this point, a coordinated answer to terrorist cyber-attacks needs to be addressed with the broader perspective of the possible tools and strategies to be implemented in order to deal with terrorist use of the Internet.

[3] Such as the Commission's 2013 Cyber-security Strategy and the Council's 2009 Action Plan on a collaborative European approach to Network and Information Security (NIS).

[4] Like the Cyber Defence Management Authority, or the Cooperative Cyber Defence Centre of Excellence.

[5] Launched in 2013, it is meant to offer better protection of the Alliance's information systems.

II – A COORDINATED ANSWER TO TERRORIST USE OF THE INTERNET: STRATEGY AND TOOLS

A. Monitoring and understanding terrorism in cyberspace

The starting point for efficient international cooperation lies within the States' faculty to understand cyber-terrorism, its causes, trends and methods. Such a process of analysis is hardly possible however without an effort to collectively monitor, observe and review terrorist activities in cyberspace, as well as share the information collected.

- ***Monitoring and collecting***: The first step should consist in monitoring and reviewing terrorist organisation websites, forums, blogs and more generally, all terrorist-linked activities on the web. The goal would not only be to collect this information for prosecution purposes but also for a better understanding of cyber-terrorism, especially when we know that approximately 80% of the information concerning radical Islamist terrorism is available "open source" (Knop, 2008: 8-23). In fact, "*many Internet pages in various languages have to be monitored and evaluated, which requires enormous technical and human resources*" and therefore should be done "*by sharing this task on a voluntary basis*" (CoEU, 2007: 3). In this respect, the "Check the Web" (CTW) initiative can be considered as one of the most interesting attempts to collect information concerning terrorist cyber-activities, within the framework of Europol's counter-terrorism Unit, in accordance with its "Strategy for combating radicalisation and recruitment". Consisting in a technical platform providing, among other things, a database of websites collected by police officials with expertise in examining these sites, language capabilities and technical expertise[6] (Argomaniz, 2014: 9), CTW is accessible for national experts and authorities as well as for Europol.

- ***Expert Analysis***: There is the undisputable need to analyse the data gathered to understand terrorist use of the Internet, in particular through international expert groups. Within the European framework, a significant number of these groups have been set up, such as the ENER (European Network of Experts on Radicalisation) or the CODEXTER (Committee of Experts on Terrorism). Such informal and academic aspects of international cooperation can serve as a provider of expertise to policy makers in the Member States and the EU by releasing policy papers and publications to disseminate information (CTC, 2011). One

[6] While at first most of the data was collected by the CTW team, now most of the information comes from Member States. Thanks to this, the library now contains several hundreds of websites, links to many extremist publications, and terrorist statements translated into English (Argomaniz, 2014: 9)

relevant example of international cooperation in expert gathering, the Europol TE-SAT report, enables policy makers to get a comprehensive perspective of European figures and trends concerning terrorist use of the Internet, thanks to information given by EU Member and partner States, partner organisations and open sources (EUROPOL, 2014).

- ***Information exchange for prosecution and expertise***: The institutionalisation of a European Counter-terrorism Coordinator falls within a desire to improve "the information flow across Member States and promote a more coherent set of counterterrorism policies" (Bossong, 2012: 528), thus guaranteeing a high level of communication and exchange. To this extent, the EU-US Terrorist Finance Tracking Programme (TFTP) Agreement is an interesting attempt to organise international data exchange concerning money flow linked to terrorism. Remaining "*an important instrument to provide [...] information about activities associated with suspected acts of terrorist planning and financing, [...the TFTP] helps to identify and track terrorists and their support networks worldwide*" (EC, 2014: 6). Under this Agreement, the US judicial authorities have the ability to file a request with the EU to obtain data concerning terrorism and its financing, with Europol then deciding on the transfer of the information requested. The possibility of a European version of this Programme has been identified by the European Commission and is still under debate.

Furthermore, the cooperation of Financial Information Units has been organised through the FIU.NET project (European Network of Financial Intelligence Units), launched in 2007. Focusing on the fight against money laundering and terrorist financing, this decentralised computer network enables the anonymous matching and exchanging of financial data stored on the premises of the participating countries.[7]

B. Tools and practices adapted for the specific nature of terrorist use of the Internet

States have developed specific tools and strategies to address both the transnational nature of Internet-based terrorist actions and the virtual nature of the evidence needed for prosecution[8].

[7] Anonymity is guaranteed by the use of the "Ma3tch" technology, standing for "Autonomous Anonymous Analysis". "To allow connected FIUs to match their data with other FIUs in an anonymous way, it converts FIU data into uniform anonymised filters without sensitive personal data. These filters can therefore safely be shared with and used by other FIUs": https://www.fiu.net/fiunet-unlimited/match/match3

[8] This part focuses on the most salient challenges to investigation and prosecution of terrorists' use of the Internet. For a detailed account of the various problems emerging from cyber-terrorism, see (Gercke, 2010).

- Multi-national investigations: While the use of the Internet allows for international action by terrorist groups (using computers, servers or websites hosted in different countries), sometimes from locations remote from effective prosecution, the response of law enforcement agencies is traditionally bound by territoriality or nationality[9]. Therefore, formal and informal international cooperation appears essential in the investigation and prosecution of terrorist behaviour on the Internet.

- *On a global scale:* Traditionally, international cooperation is implemented directly by States, as expressed for instance in the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and through mechanisms such as letters rogatory and extradition. In this regard, it is often essential that the crime prosecuted by the requesting State is also deemed unlawful in the executing State (principle of dual criminality). This condition is more easily met if offences have been harmonised by international conventions (see *supra*). International investigations are greatly facilitated by the cybercrime programme of INTERPOL, designed to assist countries in gathering and exchanging information (for example by a network of contact officers) and coordinate investigations, *inter alia*, in the fight against cyber-terrorism.

- *In Europe:* Cooperation has been more significant in the EU, relying on mutual recognition. The main tool is the European Arrest Warrant, introduced in 2002. It inspired the European Evidence Warrant established in 2008. These tools make cooperation easier between EU Member States by excluding dual criminality requirements for a list of offences, including terrorism[10], and reducing the motives for non-implementation. Furthermore, the procedure for their use is simple and undertaken directly by judicial authorities. However, the European Evidence Warrant has often been judged useless because it requires certainty about the presence of the evidence requested (Catelan, Cimamonti and Perrier (dir.), 2014). As a consequence, a new instrument, the European Investigation Order (directive 2014/41/EU), has been created which covers almost all investigative measures and does not have this requirement. These instruments are crucial in the fight against the use of the Internet for terrorist purposes because they allow fast international cooperation.

Besides these, agencies have been specially designed to facilitate this coordination. The fight against terrorism figures among the objectives of both the European Police Office, created by

[9] Consequently, jurisdiction is a very complex issue in prosecuting cyber-terrorism. While the legal rules are classical (for example, the Council of Europe cybercrime convention uses territoriality as the primary factor constituting jurisdiction: art. 22) their application to Internet-based crimes is very difficult and interpretation varies from one State to another (see Brenner and Koops, 2004 ; Cottim, 2010).

[10] Article 2 of the 2002 Framework decision on the European Arrest Warrant; article 14 of the 2008 Framework decision on the European Evidence Warrant.

a Convention signed on 26th July 1995, and the judicial cooperation agency, Eurojust, created by a Council decision in 2002.[11] Europol and Eurojust facilitate the collection and exchange of information and evidence between law enforcement agencies and judicial authorities. Europol has also developed a "First Responder Network", a network of experts providing support for investigation to a Member State just after a terrorist attack.[12] Moreover, cooperation in Europe against terrorist use of the Internet has been greatly improved by the establishment of joint investigation teams, a mechanism created by Council Framework Decision 2002/465/JHA.[13] Europol and Eurojust may participate together in the establishment of such teams at the request of a Member State.[14] Such teams may also be set up with Third States, on a judicial basis like the 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of the CoE or the 2009 Agreement on mutual legal assistance between the EU and the US (Catelan, Cimamonti and Perrier (dir.), 2014).

Finally, although such crimes would still be tried before national courts, the fight against cyber-terrorism would benefit greatly from coordination of prosecution under a European public prosecutor (Catelan, Cimamonti and Perrier (dir.), 2014). The Lisbon treaty allows for the extension of "*the powers of the European Public Prosecutor's Office to include serious crime having a cross-border dimension*".

Thus established, international cooperation for investigation and prosecution must rely on collectively drafted processes and strategies to address the specificity of evidence collected on computers and networks.

- Processes to collect evidence on computers and networks: Most of the evidence in relation to terrorist use of the Internet is data-based, thus requiring specific legal instruments to ensure the efficiency of collection and the preservation of procedural and substantial liberties.

- *Efficiency of procedures:* The Council of Europe Convention on Cybercrime is the key legal instrument in this domain. It requires States to establish different processes to collect data. The rules establishing a framework for computer-specific investigations must address several

[11] Lisbon Treaty, art 88 for Europol; concerning Eurojust, art. 85 only mentions "*serious crime affecting two or more Member States*" but the Eurojust council decision mentions terrorism on several occasions.

[12] First used for attack by Anders Breivik in Norway in 2011. (Catelan, Cimamonti and Perrier (dir.), 2014)

[13] In addition, the Council adopted a Recommendation in 2002 to set up multinational ad hoc teams for the gathering and exchanging of information on terrorism.

[14] Article 6 of the 2009 Agreement between Europol and Eurojust and art. 6 of the consolidated Eurojust Council Decision.

issues. Relevant data must be quickly identified and retrieved. Accordingly, the Council of Europe Convention on Cybercrime calls on signatories to create "quick freeze" procedures (Section 2, Title 2 – *Expedited preservation of stored computer data),* in order to guarantee the preservation of data by third parties (such as websites or Internet service providers) pending a judicial decision on the presentation of such evidence (UNODC, 2012: 62). Moreover, computer data is easily altered when retrieved and collected. Henceforth, appropriate processes must be implemented to ensure the integrity of evidence thus collected. In particular, forensic experts specialised in digital matters should be called upon in investigations of this nature and, more generally, States and institutions must provide research and training about the recovery of computer data.[15]

- *Preserving human rights and rule of law while collecting computer-based evidence:* In this regard, several questions have emerged. Firstly, concerning terrorist use of the Internet, intelligence agencies are greatly involved and their links with police investigations are tightening (Brown and Korff, 2009: 127). Therefore, questions arise about the protection of privacy but also fair trial and the use of secret evidence and evidence collected through secret means.

Secondly, one of the most sensitive issues regarding the fight against terrorism is data retention. On the one hand, the capacity to fight cyber-terrorism is dependent on the ability to monitor traffic data and to trace back communications or the identity of the users. On the other hand, the retention of traffic data directly infringes on the right to privacy and the right of protection of personal data. On that subject, the EU legislator adopted the 2006 Data retention directive (2006/24/EC), obligating Member States to enact legislation requiring Internet service providers to retain service data relating to electronic communications (such as location and subscriber data, but not content) for periods varying from 6 to 24 months. Nevertheless, in a landmark decision, the CJEU decided that the Directive violated the EU Charter of Rights: *"Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary".*

[15] The US Department of Homeland Security has developed a guide about "Best practices for seizing electronic evidence, a pocket guide for first responders"; see also ENISA, 2013 and Akhgar, Staniforth and Bosco, 2014.

Along with these investigations of terrorist offences, States must prevent the extension of radicalisation and recruitment via the Internet by controlling terrorist content on the Internet.

C. Coping with terrorist content

Concerning terrorist content on the Internet, governments must aim both at its removal and at promoting counter-narratives.

- Removing terrorist content: Even though terrorist websites can be infiltrated to gain intelligence on terrorist groups, governments must, in the end, remove terrorist content from the Internet in order to prevent radicalisation and recruitment. But governments have to deal with the expansion of video-hosting websites and user-generated content. Monitoring such content requires considerable resources and cannot be achieved without cooperation with private stakeholders, both formal and informal. A graduated response seems most appropriate.

- The first answer to terrorist content is *self-regulation*: "most Internet service providers, web hosting companies, file-sharing sites and social networking sites have terms-of-service agreements that prohibit certain content" (Mantel, 2010: 135). These agreements are usually enforced thanks to content-flagging mechanisms on offer to users[16].

- As a second answer, governments have intended to strengthen regulation via rather *informal public-private partnerships*. However, these enterprises are constrained by several imperatives. Experts and advocacy groups are particularly watchful of the preservation by law enforcement agencies of freedom of speech and information, the right to privacy and the protection of personal data, protected by the European Convention on Human Rights and the EU Charter of fundamental rights (see Brown and Korff, 2009; Banisar, 2009). Moreover, the implementation of public-private partnerships is dependent on the good will of private stakeholders. With regards these issues, public-private cooperation has not always been successful. In particular, the "Clean IT" initiative, a consultation of the private sector financed by EU funds, was vigorously criticised and finally abandoned (Argomaniz, 2014: 10), due to the very controversial nature of the proposals (compulsory reporting by Internet companies, surveillance of websites, user identity checks, etc.) and the uncertainty regarding its actual authority. This failure demonstrates that any ambiguity in the legal framework governing

[16] Public-private cooperation can support this self-regulation: Google Inc, Youtube's parent company introduced such a flagging mechanism following discussions with governments of the UK and the US (UNODC, 2012: 128)

Internet monitoring is highly prejudicial and that content-regulation seems barely reachable through very formal and stringent means.

Therefore, the best approach promoted today is based on simple and mildly formal procedures, such as “notice and takedown procedures”, as enacted in the EU Directive on electronic commerce. Host providers are notified of the presence of illegal contents on their servers and are then obligated to remove or block such content. Similar procedures could be implemented to obligate search engines to remove search results linked to terrorist websites. Furthermore, these initiatives are in accordance with the liability of Internet service providers and websites in Europe. The Directive (2000/31/EC) mostly exempts Internet providers from civil and criminal liability when they do not have actual knowledge of terrorist content they host or transmit. And article 15 of the Directive states:*“1. Member States shall not impose a general obligation on providers* […] *to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity”.* However, States must put rapid court action into place to control any restriction on freedom of expression and information. Thus, the articulation of self-regulation and procedures characterised by their rapidity, simplicity and mild formality – such as notice and takedown procedures – seems the best way to identify terrorist content on the Internet.

- *Third response: blocking content:* Due to its technical and legal difficulties and to its potential threat for human rights, the blocking or filtering of content appears to be a last resort that is best not used. In respect to freedom of expression, a Recommendation of the Council of Europe in 2008 (CM/Rec (2008) 6) aims at providing guidelines to accommodate this tool with article 10 of the ECHR. However, experts have already pointed out the misuse of filtering techniques by some governments, in particular in Turkey and Russia (Banisar, 2009: 56). As blocking is dependent on cooperation with Internet Service Providers, respective obligations of States and ISPs must be well defined and accompanied by strong guarantees and extensive judicial supervision. Another source of complexity lies in the fact that terrorist content is disseminated through various means. In response, filtering mechanisms often use black lists and key words, phrases and signatures to identify websites to block, thus raising very stringent questions about the criteria and accuracy of classification (for a detailed analysis of technical issues regarding content filtering, see Australian computer society, 2009)

- ***Producing counter narratives:*** The fight against terrorism also requires the provision of critical analysis and answers for an audience that may be fragile or young and therefore more receptive to terrorist propaganda. Relying on the EU Strategy for Combating Radicalisation and Recruitment adopted in 2005, and revised in 2008 and 2014, the European Commission developed the Radicalisation Awareness Network in 2011, connecting organisations and local actors involved in countering radicalisation. This network, *inter alia*, helps create exit strategies and projects. Regarding terrorist content on the Internet in particular, the Commission funds audio-visual production that provides counter narratives. These initiatives often associate victims of terrorist acts in order to provide less formalised and institutionalised messages.

To conclude this study, we would like to sum up several ideas that appear essential in furthering international cooperation in the fight against cyber-terrorism. First of all, prevention has to be greatly enhanced. This aim could be reached through strengthened public-private partnership and a flexible approach. Rather than compelling private partners such as ISPs or social networks, it would be more efficient to include them in preventive measures and actions. As a matter of fact, they appear to be well placed to take on this role: as such, private partners could actively help authorities with monitoring and moderating terrorism-related content. To this effect, it is conceivable for governments to subsidise self-regulation procedures. Moderators could be provided by private partners while being paid by the States, in accordance with an agreement on policies and rules that private and public partners would elaborate together. The response would therefore be even briefer and more accurate. Still, in order to foster prevention, authorities and private partners – and especially, to this extent, social networks – could also work together on elaborating and broadcasting targeted, preventive messages in order to raise awareness among the public and more precisely among people who are likely to be sensitive to terrorists or violent content. Since social networks are already able to target their audience for advertising or suggested content, one could easily imagine setting up the same process for preventing terrorism. Lastly, prevention could even involve stakeholders beyond the public-private partnership sphere and, for instance, include the whole Internet community. Indeed, citizens could take part in the moderating/monitoring processes, as some online newspapers already do. With the help of government subsidies, authorised moderators could highlight content that appeared inappropriate as far as website policies were concerned from their home or workplace.

Most of the debates regarding terrorist use of the Internet concern the removal of content and its conjunction with freedom of expression. Nowadays, a balance between these two imperatives is set in place by officials and, as a last resort, judges. Content is blocked according to key words and lists without effective reflection on what content is acceptable or not, thus allowing governments to deem legitimate content unlawful. Primarily, transparency regarding blocking or withdrawal mechanisms must be fostered: removal decisions must be motivated and contestable before the courts; key words should not be the sole basis for such decisions and, in general, criteria must be made public. More generally, these criteria should be drafted in common and refined. While criminal provisions are defined in broad terms and refer to the intent of the perpetrators, most decisions likely to infringe on freedom of expression focus on specific terms and do not require the intention of the diffuser. In order to prevent States from exploiting the vagueness of legal provisions, common standards and definitions must be established to ensure clarification of phrases such as *"conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed"* (art. 3 of the consolidated 2002 EU Framework decision, "provocation"); and that they are interpreted in a way that is acceptable to all European countries. Finally, guidelines must be drafted to help determine under which criteria content can be removed to address the massive diffusion of terrorist content, which renders case-by-case solutions difficult. These guidelines could be outlined through cooperation with public stakeholders such as media groups, ISPs or search engines. In the end, the solution does not appear to be the creation of new offences and content-removal mechanisms, but rather the clarification and specification of existing ones.

In the near future, the fight against cyber-terrorism should actively strive for strengthened increase in its efficacy. With this in mind, two obstacles to an efficient answer to terrorism must be overcome: territorial boundaries and technical complexity. The latter could be addressed by means of extensive training of the stakeholders involved in cyber-terrorism. This training programme for experts, policemen, prosecutors and judges should be international in order to provide for common strategies and practices. Moreover, day-to-day cooperation and dialogue between these players would be strengthened by the use of common tools and reflexes. Furthermore, this training should rely on the work of existing expert groups that could enlighten the theoretical and technical aspects of cyberspace and the terrorist phenomenon, giving those involved both a broader and more precise idea of their capabilities and competency**.** In this regard, ENER or ENISA could reinforce their ability to provide practical and usable expertise on a European scale, and communicate it to all those concerned.

With regards the territorial obstacle to an efficient fight against cyber-terrorism, two suggestions may be considered, though on different scales. Firstly, the institution of a

European Public Prosecutor would probably enable a common European criminal policy, but also allow for the overcoming of most of the complexity regarding territorial competency. However, the global nature of the terrorist threat leads one to believe that the European level may not be the most adequate. In fact, for as long as no further identification of the phenomenon is undertaken, the exclusion of criminal havens will always reduce the efficiency of the fight against cyber-terrorism. For this reason, the UN (or NATO) scope should be taken into consideration as the future leader against counter-terrorism, in both characterising criminal offences and organising the necessary legal response.

BIBLIOGRAPHY

SOURCES

- ***Legal and institutional sources***

Directive 2000/31/EC of the European Parliament and the Council of 8.6.2000 on certain legal aspects of information services, in particular electronic commerce, in the Internal Market

Council Framework Decision, 13 June 2002 on Combating Terrorism, 2002/475/JHA, 2002

Council of Europe, Convention on Cybercrime CETS No.: 185, 2001

Optional Protocol on Xenophobia and Racism to the Cybercrime Convention, 2002

Council of Europe, Convention on Prevention of Terrorism, CETS No.: 196, 26 May 2005

Directive 2006/24/EC of the European Parliament and of the Council of the European Union of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks

Décision cadre 2008/919/JAI modifiant la décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme.

Recommendation CM/Rec (2008) 6 of the Committee of Ministers of the Council of Europe on measures to promote the respect for freedom of expression and information with regard to Internet filters, 2008

Agreement between Europol and Eurojust, 2009

Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organisation, 2010.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

- ***Official reports***

ARCHICK Kristin, *Cybercrime: The Council of Europe Convention*, CRS Report for Congress, 2002.

AUSTRALIAN COMPUTER SOCIETY, *Technical observations on ISP based filtering of the Internet*, 2009.

CODEXTER, *"Apologie du Terrorisme" and "Incitement to Terrorism": Analytical Report*, 2004.

COUNCIL OF THE EUROPEAN UNION, *Council conclusions on cooperation to combat terrorist use of the Internet, "Check the Web"*, 2007.

DENNING Dorothy, "Cyber terrorism", Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 2000.

ENISA, *Cyber Europe 2010 - Evaluation Report*, 2011.

ENISA, *Digital forensics – Handbook, Document for teachers*, September 2013.

EU COUNTER TERRORISM COORDINATOR, *Note in preparation of the informal meeting of Justice and Home Affairs Ministers in RIGA*, January 2015.

EU COUNTER TERRORISM COORDINATOR, *Note: EU Action Plan on combating terrorism*, January 2011.

EUROPEAN COMMISSION, *Fighting Terrorism at EU level, an overview of Commission's actions, measures and initiative*, Brussels, 2015.

EUROPEAN COMMISSION, {COM(2014) 513 final} *Joint Review Report of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, 2014

EUROPOL, *Terrorism Situation and Trend Report*, 2014/2013/2012

SIEBER Ulrich and BRUNST Philipp W., *Cyberterrorism – the use of the Internet for terrorist purposes*, Council of Europe Publishing, 2007, 502 p.

UNITED NATIONS OFFICE ON DRUGS AND CRIME, *The use of the Internet for terrorist purposes,* NY, 2012.

SYMPOSIUM REPORTS

DOGRUL Murat, ASLAN Adil, CELIK Eyyup, *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism,* 3rd International Conference on Cyber Conflict, COE Publication, 2011, pp. 29-43.

VON KNOP K., "Institutionalization of a Web-Focused, Multinational, Counter-Terrorism Campaign*", NATO Science for peace and Security Series : Responses to Cyber Terrorism*, Vol. 44, Center of Excellence Defense Against Terrorism, Ankara, 2007, pp 8-23.

BOOKS

AKHGAR Babak, STANIFORTH Andrew and BOSCO Francesca (dir.), *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Syngress, 2014, 306 p.

CATELAN Nicolas, CIMAMONTI Sylvie, PERRIER Jean-Baptiste (dir.), *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne*, Presses Universitaires d'Aix-Marseille, 2014, 280 p.

CONWAY Maura, *Reality Check: Assessing the (Un)Likelihood of Cyber terrorism*, in CHEN, TOM and JARVIS, *Cyber Terrorism : Understanding, Assessment and Response*, New-York, Springer, 2014, pp. 103-122.

SAULNIER-CASSIA Emmanuelle (dir.), *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne*, L.G.D.J, 2014, 515 p.

SOTTIAUX Stefan, *Terrorism and the Limitation of Rights: The ECHR and the US Constitution, Bloomsbury*, Cornwall, 2008, 441 p.

PERIODICAL ARTICLES

ARGOMANIZ Javier, "European Union responses to terrorist use of the Internet", *Cooperation and Conflict*, September 1, 2014.

AVERSA Jeannine, "Cutting Terror Funds Said Effective", Associated Press, September 2002.

BANISAR David, "Speaking of Terror: a Survey of the Effects of Counter-Terrorism Legislation on Freedom of the Media in Europe", *International Journal of Civil Society Law*, Volume VII, Issue 3, 2009, pp. 33-64.

BENSON David, "Why the Internet is not increasing Terrorism", in *Security Studies*, 2014, pp. 293-328.

BOSSONG Raphael, "Peer reviews in the fight against terrorism: A hidden dimension of European security governance", in *Cooperation and Conflict*, Vol. 47/4, 2012, 19 p.

BRANTLY Aaron, "Financing terror bit by bit", *CTC Sentinel*, Vol 7/10, 2014, pp. 1-5.

BRENNER Susan and KOOPS Bert-Jaap, "Approaches to cybercrime jurisdiction", *Journal of High Technology Law*, Vol. 4, n°1, 2004, 46 p.

BROWN Ian and KORFF Douwe, "Terrorism and the proportionality of Internet surveillance", *European Journal of Criminology*, Vol. 6, 2009, pp. 119-134.

CONWAY Maura, "Reality Bites: Cyber terrorism and Terrorist Use of the Internet", *First Monday*, Vol. 7, n°11, 2002.

COTTIM Armando A.,"Cybercrime, cyber terrorism and jurisdiction: an analysis of article 22 of the COE convention on cybercrime", *European Journal of Legal Studies*, Vol 2, n°3, 2010.

GERCKE Marco, "Challenges in developing a legal response to terrorist use of the Internet" in *Defence Against Terrorism Review*, Vol. 3, n°2, Fall 2010.

HINNEN Todd, "The cyber-front in the war on terrorism: curbing terrorist use of the Internet", *The Columbia Science and Technology Law Review*, Volume V, 2004.

MANTEL Barbara, "Terrorism and the Internet: should web sites that promote terrorism be shut down?", in *Issues in Terrorism and Homeland Security: Selections From CQ Researcher,* SAGE Publications, Inc, 2010, pp. 129-153.

THOMAS Timothy, "Al Qaeda and the Internet: the danger of cyber-planning", *Parameters*, Spring 2003.

SIEBER Ulrich, "International Cooperation against terrorist use of the Internet", *Revue internationale de droit pénal*, Vol. 77, 2006/3, pp., 395-449.

WEBSITES

http://www.consilium.europa.eu/fr/policies/fight-against-terrorism/counter-terrorism-coordinator/

http://www.interpol.int/en/Internet/Crime-areas/Cybercrime/Cybercrime

https://www.fiu.net/fiunet-unlimited/match/match3