

Foggetti, Nadina, "Cyber Terrorism and the reconstruction of customary rule about terrorism of the Special Tribunal for Lebanon in the recent case law", *IUS ET SCIENTIA*, 2015, Vol. 1, No. 1, pp. 54-78.

DOI: <http://dx.doi.org/10.12795/IETSCIENTIA.2015.i01.05>

Cyber Terrorism and the reconstruction of customary rule about terrorism of the Special Tribunal for Lebanon in the recent case law.

Ciber terrorismo y reconstrucción del Derecho Internacional Consuetudinario a partir de la jurisprudencia del Tribunal Especial para el Líbano

Dr. Nadina Foggetti. Ass. Professor of Public International Law. Università degli Studi di Bari Aldo Moro. nadinafoggetti@gmail.com

Abstract. In this article we focus attention on the remaining problem of defining Terrorism and Cyberterrorism. Throughout relevant decisions of the Tribunal of Lebanon as a case of study, recognizing international consuetudinary law on terrorism, we analyse critically the EU Antiterrorism measure and the right to privacy in the EU and ECHR prospective to conclude in the need for strengthening the protection of individuals against acts affecting the right to privacy.

Resumen. En este estudio centramos la atención en el persistente problema de encontrar una definición para el terrorismo y para el ciber terrorismo en particular. A través del análisis de pronunciamientos relevantes del Tribunal Especial para El Líbano -usado como un caso de estudio- en los que se identifican normas de derecho internacional consuetudinario sobre terrorismo, analizamos críticamente las medidas antiterroristas adoptadas en el seno de la UE en contraste con el derecho a la privacidad protegido por el Derecho de la Unión y por el Convenio Europeo de Derechos Humanos y sostenemos la necesidad de reforzar la protección de los individuos frente a actos que afecten al ejercicio de este derecho a la privacidad.

Key words. Cyber terrorism - Internationalized Tribunals and consuetudinary law - right to privacy

Palabras clave. Ciber terrorismo - Tribunales Internacionalizados y Derecho consuetudinario - Derecho a la privacidad.

1. Introduction

Cyber terrorism includes serious conducts such as targeted attacks, politically motivated, conducted with the help of computer technology and/or within the information technology, such as cloud computing, with significant consequences at economic, political and social level. In front of the proliferation of acts adopted in this sector, a specific legal instrument in the fight against cyber terrorism and a definition of cyber terrorism are lacking.

The first aim of the paper concerns the definition of cyber terrorism in the light of International Law and the case law of international tribunals and courts. In particular, the Appeals Chamber of the Special Tribunal for Lebanon recently has declared in Case No.

Foggetti, Nadina, "Cyber Terrorism and the reconstruction of customary rule about terrorism of the Special Tribunal for Lebanon in the recent case law", *IUS ET SCIENTIA*, 2015, Vol. 1, No. 1, pp. 54-78.

DOI: <http://dx.doi.org/10.12795/IETSCIENTIA.2015.i01.05>

STL-11-01/I (Feb. 16, 2011) that there is a customary international law definition of terrorism. We will analyze if it is possible to apply this definition to cyber terrorism. As regards the definition of terrorism, the decision of the STL will be analyzed in light of relevant practice in order to clarify whether it could include cyber terrorism. An answers is needed in order to define the localization of jurisdiction, including the possibility to affirm the competence of existing International criminal courts and the idea to establish an International Criminal Tribunal for Cyberspace. Defining the cyber terrorism is crucial in order to identify the difference among this typology of crime and cyber war, the sector of international law that we can apply, the acknowledgment of the crime and the related state/individual responsibility. In the public international law this is crucial in order to identify the applicability of international law of armed conflict or international law regarding the international criminal law¹.

¹ Cfr. Hosein, *Threatening the Open Society: Comparing Anti-terror Policies and Strategies in U.S. and Europe*, 2005, available at <http://www.statewatch.org/news/2005/dec/gus-hosein-terror-reportdec2005.pdf>; United Nation Office on Drugs and Crime (UNODC), *The Use of the Internet for Terrorist Purposes*, New York, 2012, available at

The second aim of the paper regards the surveillance powers related to cyber terrorism, taking into account the international acts introduced after attacks of 2001. Among these, the UN Security Council Resolutions for the creation of black lists of suspected terrorists and people and companies suspected to finance terroristic activities. In particular these Resolutions required to States and the UE to enact patrimonial and personal restrictive measures against them. States and the EU have increased surveillance and investigation powers implementing the named Resolutions. The increase of those powers results also from acts establishing forms of international cooperation among States, such as the 2005 Prüm Convention, promoted by EU Members to fight against crime. It is arguable the progressive formation of a normative corpus inspired to emergency criteria which allows, through the use of new ICT, the interception and collection of both neutral and sensitive personal data, also in the use of the smart grid services. If, on one hand, it is a tool used in the war on terrorism, on the other hand it implies the collection, treatment and recording of personal data that exceeds the need of security and could violate human rights. The administrative emergency, ultimately, must ensure the protection of human rights. The real problem is the disappearance of the temporary nature of the emergency requirement.

2. The Problem of defining Terrorism and Cyber terrorism.

The use of the Internet for terrorist purposes is a rapidly growing phenomenon, requiring a proactive and coordinated response from Member States. In particular, in 2011, the General Assembly, in its resolution 66/178, reaffirmed the mandate of UNODC to continue to develop specialized legal knowledge in the area of counter-terrorism and

http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

CTITF Working Group Compendium, *Countering the Use of the Internet for Terrorist Purposes. Legal and Technical Aspects*, New York, 2011, available

at http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf; UN Resolution A/res/60/288, adopted by the

General Assembly on 8 September 2006, available at [http://daccess-dds-](http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement)

[ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement](http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement); G. CARELLA, *Nominalismo e lotta al terrorismo internazionale: il caso delle extraordinary renditions*, in G. VENTURINI, S. BARIATTI (adited by), *Liber Fausto Pocar. Diritti individuali e giustizia internazionale*, vol. I, Milano, 2009, p. 111 ss. cfr. FOGGETTI, *Cyber-Terrorism and the Right to Privacy in The Third Pillar Perspective*, in *Masaryk University Journal of Law and Technology*, 2009, pp. 265-376.

pertinent thematic areas, including the use of the Internet for terrorist purposes². At this point it is necessary to examine whether at international level we can identify the notions of cyber terrorism and whether they have common traits. In a second step we must verify, if the definition of "customary" international terrorism it is applicable also to cyber terrorism. The literature has dealt with the issue, in the absence of a generally accepted definition of the phenomenon, often considered cyber terrorism "ordinary computer crimes but with the added intention to instill fear among a target audience"³. The most significant practices examined identifies two different definitions of cyber terrorism: one elaborate and implemented by the FBI and an other by NATO.

For the FBI cyber terrorism is a "*premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.*"⁴ According to this definition in order to qualify an attack as cyber terrorism it is necessary that it is politically motivated and puts in place by sub-national groups or clandestine agents and takes place against informatics systems, computer programs and data, and produces damages against not military objectives. For NATO, cyber terrorism is a "*cyber attack using or exploiting computer or communication networks sufficient to cause destruction or disruption to generate fear or to intimidate a society into an ideological goals.*"⁵ According to this definition, cyber attacks with an ideological aim that using or exploiting computer networks or communications, in order to cause the destruction or disruption capable of generating fear or intimidate society may fall into the category of cyber terrorism⁶.

² Cfr. Resolution No. 66/178 adopted by the General Assembly, in 89th Plenary meeting, concerning Technical assistance for implementing the international conventions and protocols related to counter-terrorism, of 19 December 2011, available at this URL: http://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2011/General_Assembly/Resolution_66-178.pdf

³ GARRETT-CLARKE, *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism*, (edited by) BIANCHI, Oxford- Portland, 2004, pp. 465 ss; DRAETTA, *The Internet and Terrorist Activities*, in Bianchi (edited by), *Ibidem*, in particular p. 453; RUOTOLO, *Internet (Diritto internazionale)*, in *Enciclopedia del diritto, Annali VII*, Milano, pp. 545-567; I D, *Internet-ional Law, Profili di diritto internazionale pubblico della rete*, Bari, 2012.

⁴ POLLIT, *Cyber-terrorism Fact or Fancy?*, *Proceedings of the 20th National Information Security Conference*, in (edited by) POLLIT, *Cyber terrorism: Fact or Fancy*, *Computer Fraud and Security*, 1998.

⁵ Everard, *Nato and Cyber terrorism*, in *Responses to cyber terrorism*, (edited by), Centre of Excellence Defence Against Terrorism of NATO, Ankara, 20

The two definitions have the same psychological element: the political and ideological aim, but they are different regarding the objective element. For the FBI definition Computer Systems is the target of the attack that becomes cyber attack in presence of this element. On the base of the second definition, the Computer system is the means through the cyber terrorist attack is realized.

The FBI definition includes only the attack carry out by individual or groups of persons independent, or "sponsored" by a State, but it not includes the State's Terrorism. The Nato definition's is more inclusive.

For the doctrine and case law, in the absence of a significant practice in relation to the definition of cyber terrorism can groped to frame the concept of cyber terrorism in light of general international law. In this context, particularly in the practice of the last ten years there have been major developments on the definition of terrorism⁷.

It is necessary to outline that in a significant number of case law, the Italian Court of Cassation and more Court of Appeal⁸, (Sent. 17-01-2007 Court of Cassation; Sent. 15-02-2006 case Baouyahia et al. Court of Appeal of Milan) stated that there is a need to interpret the national law regarding terrorism in light of International law, on the base of a common customary rule that defines terrorism in time of peace. In this case-law, the Supreme court has stated that, according to the doctrine, there are two possible definition of terrorism in Italian criminal law: one for time of peace and another in the context of *ius in bello*.

⁶ BRUNST, *Use of Internet by Terrorists - A Threat Analysis*, in *NATO Science for Peace and Security Series - E: Human and Societal Dynamics*, 2008, Ankara.

⁷ BETTONI, *Terrorismo e Internet: alcune considerazioni giuridiche, politiche e tecnologiche*, in *Cyberspazio e Diritto*, 2010 fasc. 1, pp. 231 - 249; Denning, *Cyberterrorism Testimony before Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, Available online at: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> ; CONWAY, *What is Cyberterrorism?*, Available in the NATO library at: CURRENT_HISTORY, vol. 101, no. 659, December 2002, pp. 436-442; NETANYAHOU, *Combattere le terrorisme international*, 2002, Paris; Noto, *Il terrorismo internazionale e le sanzioni del Consiglio di Sicurezza nella giurisprudenza italiana: il caso Daki*, in *Rivista di diritto internazionale private e processuale*, 2008, pp. 731-740.

⁸ Sent. 17-01-2007 Italian Court of Cassation n. 1072, Concorso di persone nel reato, associazione con finalità di terrorismo, available at <http://www.altalex.com/index.php?idnot=36174> ; Sent. 22/10/2008, Italian Court of Cassation n. 39545, available at <http://www.altalex.com/index.php?idnot=43932> ; Sent. 15-02-2006 case Baouyahia et al. Court of Appeal of Milan.

It is possible to define the terrorism in time of peace, identifying, according with doctrines, as the conduct that includes three constitutive elements: the transnational nature of the terrorist act; the intent of the perpetrator to cause a state of terror in the general public or population, or to coerce a State or an international organization to commit or to omit a certain conduct and a political/ideological/religious aim⁹.

In light of this issue it is possible to track the existence of an essential core for the creation of a customary rule about terrorism that includes just mentioned elements¹⁰.

In relation to the first element, that defines the *actus reus* of the crime, it is necessary that the conduct will transcend the boundary of the State. Cyber terrorism complies in this definition because it is transnational in nature. This definition and the core elements not are apply in the case in which " the offence is committed within a single State, the alleged offender is a national of that State and is present in the territory of that State and no other State has a basis ... to exercise jurisdiction"¹¹.

Concerning the second element, the subjective element (*mens rea*), it is composed by two main element: the first is the *dolus generalis*, relating to specific crime; the secondly regards the *dolus specialis*, and it consists in the intention to bring a State to do or not do

⁹ Cfr G. DELLA MORTE, *Sulla giurisprudenza italiana in tema di terrorismo internazionale*, in *Rivista di diritto internazionale*, 2009, pp. 443-475; A. CASSESE, *The multilateral criminal notion of Terrorism in International Law*, in *Journal of Int. Criminal Justice*, 2006, pp. 933-943; A. CASSESE, *Lineamenti di diritto internazionale penale - I. Diritto sostanziale*, Bologna, 2005; A. CASSESE, *Terrorism as an International Crime*, in *Enforcing International Law Norms Against Terrorism*, (edited by) A. BIANCHI, Oregon, 2004; VALSECCHI, *Sulla definizione di terrorismo "in tempo di guerra"*, in *Diritto penale contemporaneo*, available at <http://www.penalecontemporaneo.it/upload/Nota%20Valsecchi%20Tigri%20Tamil.pdf>; VALSECCHI, *Il problema della definizione di terrorismo*, in *Rivista italiana diritto e procedura penale*, 2004, p. 1127 ss. In particular the thesis of prof. Cassese is based on the international practice "Lies in, or results from, the converging adoption of national law, the handing down of judgement by national courts, the passing od UN General Assembly resolutions, as well as the ratification of international convention by great number of states".

¹⁰ Cfr. CASSESE, *Lineamenti di diritto internazionale penale*, Bologna, il Mulino, 2005, pp. 162-75, in particular p. 167; A. CASSESE, *Il sogno dei diritti umani*, Milano, Feltrinelli, 2008, pp. 177-84, in particular p. 179.

¹¹ Cfr. Article 3 of the Convention for the suppression of crime of financing terrorism, New York, 1999. See also G. DELLA MORTE, *Sulla giurisprudenza italiana in tema di terrorismo internazionale*, in *Rivista di diritto internazionale*, 2009, pp. 443-475; . G. CARELLA, *Lotta al terrorismo e protezione dei rifugiati*, in U. Lenza, (edited by) *Le migrazioni. Una sfida per il diritto internazionale, comunitario e interno*, Atti del IX Convegno SIDI svoltosi a Roma il 17 e 18 giugno 2004, Napoli, 2005, p. 177 ss.

something. In the light of the just mentioned doctrine and practice, the state of terror produced in the population is finalized at this result¹².

Concerning the third element, it excludes from its sphere of application, the private conducts, finalized at personal scope, i.e. private revenge or pursuing private economic goals.

In conclusion terrorism in time of peace, may be qualified in the context of the "crime against humanity"¹³. In this case the *actus reus* will be included in a series of actions of conducts qualified as "crime against humanity" in international customary rules and treaties. Moreover these conducts will be ascribable in the context of a systematic and wide attack against civilians and with the awareness of such an attack.

Moreover, the Special Tribunal for former Yugoslavia, states, concerning the crime of terrorism in time of peace, that "Customary law imposed individual liability for violation of the prohibition of terror against the civilian population as enshrined in Article 51 (2) of Additional protocol I and Article 13 (2) of Additional Protocol II"¹⁴

Recently the Special Tribunal for Lebanon stated about the existence of customary rule in this matter. At this point we may analyze this definition, the issues related, the possibility to apply this definition to cyber terrorism conducts and if there are the requirements to apply this definition¹⁵. The Special Tribunal for Lebanon was established by the Security Council, acting under Chapter VII of the UN Charter, after the Lebanese Parliament had failed to formally ratify an agreement between the UN and the Lebanese

¹² Cfr. G. CARELLA, *Terrorismo di Stati e terrorismo di individui: il caso Lockerbie*, in *Studi in ricordo di A. F. Panzera*, I, Bari, 1995, p. 201.

¹³ In the light of Statute of International Criminal Court the conduct that fill in the crime against humanity are homicide, torture, rape, persecution, or "other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health". On the bases of article 7 of the same Statute, par. 2, lett. A) "attack directed against any civilian population means a course of conduct involving the multiple commission of acts referred to in paragraph 1 against any civilian population, pursuant to or in furtherance of a State or organizational policy to commit such attack". In doctrine on this point see A. Arnold, *The ICC as a New Instrument for Repressing Terrorism*, New York, 2004,

¹⁴ Cfr. Sentence of Tribunal for former Yugoslavia, of 5 December 2005, *The Prosecutor v. Galic, Case T-98-29-T*, and of 30 November 2006, *The Prosecutor v. Galic, Case IT-98-29-A*, available at this URL: <http://www.icty.org/>

¹⁵ Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging (Appeals Chamber) STL-11-01/I 16 February 2011 at [1] ("Interlocutory Decision"). In doctrine cfr. SHARF, *Special Tribunal for Lebanon Issues Landmark Ruling on Definition of Terrorism and Modes of Participation*, ASIL Insights <<http://www.asil.org/insights110304.cfm>>. The author wrote that "the landmark decision will give a momentous effect on the decades-long effort of the international community to develop a broadly acceptable definition of terrorism."

Government setting up an international tribunal to try all those allegedly responsible for the attack, and related killings, on the former Lebanese Prime Minister Rafiq Hariri in February 2005¹⁶.

In Resolution 1757 (2007) the Security Council decided that the provisions of the agreement on the establishment of a Special Tribunal that was annexed to the resolution and the Tribunal's Statute attached to the agreement would enter into force on 10 June 2007, unless the Government of Lebanon notified the UN that the legal requirements for entry into force had been complied with before that date¹⁷.

The jurisdiction of the Special Tribunal covers the prosecution of persons responsible for the attack of 14 February 2005 resulting in the death of former Lebanese Prime Minister Hariri and in the death or injury of other persons, but could be extended if the Tribunal finds that certain other attacks that occurred in Lebanon between 1 October 2004 and 12 December 2005 are connected, in accordance with the principles of criminal justice, and are of a nature and gravity similar to the attack of 14 February 2005. Crimes that occurred after 12 December 2005 may also be included in the Tribunal's jurisdiction under the same conditions if it is so decided jointly by the Government of the Lebanese Republic and the UN and with the consent of the Security Council (Art. 1 STL-Statute)¹⁸. The Statute further establishes that the Tribunal shall apply the "provisions of the Lebanese Criminal Code relating to the prosecution and punishment of acts of terrorism, crimes and offences against life and personal integrity, illicit associations and failure to report crimes and offences, including the rules regarding the material elements of a crime, criminal participation and conspiracy as well as Articles 6 and 7 of the Lebanese law of 11 January 1958 on Increasing the penalties for sedition, civil war and interfaith

¹⁶ Report of the Secretary-General on the Establishment of a Special Tribunal for Lebanon 15 November 2006 (S/2006/893), unlike the Extraordinary Chambers in the Courts of Cambodia and the Special Court for Sierra Leone that also have limited jurisdiction over domestic crimes, the Special Tribunal for Lebanon's *ratione materiae* jurisdiction is limited solely to crimes under the Lebanese Criminal Code and does not extend to crimes under international law. Cfr. Clere, *An Examination of the Special Tribunal for Lebanon's Explosive Declaration of "Terrorism" at Customary International Law*, Otago, 2012, available at <http://www.otago.ac.nz/law/research/journals/otago043934.pdf>

¹⁷ Security Council Resolution 1757 (2007) Adopted by the Security Council at its 5685th meeting, on 30 May 2007, S/res/1757 (2007), available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N07/363/57/PDF/N0736357.pdf?OpenElement>

¹⁸ BUFALINI, Il tribunale speciale per i libano si pronuncia sul crimine di terrorismo nell'ambito di una singolare procedura, *Nota a Tribunale per il Libano, Camera d'Appello, Caso No. STL-11-01/I*, 16 febbraio 2011, Libano, in *Diritti umani e diritto internazionale*, 2011, fasc. 2 pp. 414 - 418.

struggle” (Art. 2 STL- Statute). Consequently, the STL is the first international criminal Court which will try persons who are accused solely of violating domestic, not international, criminal law.

2.1. The decision of the Tribunal of Lebanon concerning terrorism definition’s.

After having received an indictment filed by the Tribunal’s Prosecutor on 17 January 2011, the Pre-Trial Judge submitted fifteen questions of law to the Appeals Chamber¹⁹. With regard to the notion of terrorist acts, the Pre-Trial Judge requested a decision on the following issues: i) Taking into account the fact that Article 2 of the Statute refers exclusively to the relevant provisions of the Lebanese Criminal Code in order to define the notion of terrorist acts, should the Tribunal also take into account the relevant applicable international law? ii) Should the question raised in paragraph i) receive a positive response, how, and according to which principles, may the definition of the notion of terrorist acts set out in Article 2 of the Statute be reconciled with international law? In this case, what are the constituent elements, intentional and material, of this offence?

On 16 February 2011 the Appeals Chamber, having heard the Prosecutor, the Head of the Defense Office and *amici curiae* via an expedited filing schedule, issued its 153 page decision.

The Tribunal shall apply the Lebanese domestic crime of terrorism, interpreted in consonance with international conventional and customary law that is binding on Lebanon²⁰. Under Lebanese law the objective elements of terrorism are as follows: an act whether constituting an offence under other provisions of the Criminal Code or not; and the use of a means "liable to create a public danger". These means are indicated in an illustrative enumeration: explosive devices, inflammable materials, poisonous or incendiary products, or infectious or microbial agents. According to Lebanese case law, these means do not include such non-enumerated implements as a gun, a machine-gun, a

¹⁹ KIRSCH-OEHMICHEN, *Judges gone astray: The fabrication of terrorism as international crime by the Special Tribunal for Lebanon*, in *Durham Law Review online*, available at <http://www.hammpartner.de/data/veroeffentlichungen/online-fassung-text.pdf>

²⁰ Alvarez-Juménez, *Methods for the identification of customary international law in the international Court of Justice’s Jurisprudence, 2000-2009*, in *International and Comparative Law Quarterly*, 2011, pp. 681-712.

revolver, a letter bomb or a knife. The subjective element of terrorism is the special intent to cause a state of terror. Although Article 2 of the Statute enjoins the Tribunal to apply Lebanese law, the Tribunal may nevertheless take into account international law for the purpose of interpreting Lebanese law.

In this respect, two sets of rules may be taken into account: the Arab Convention against Terrorism²¹, which has been ratified by Lebanon, and customary International law on terrorism in time of peace. A comparison between Lebanese law and the Convention shows that the two notions of terrorism have in common two elements: they both embrace acts; and they require the intent of spreading terror or fear. However, the Convention's definition is broader than that of Lebanese law in that it does not require the underlying act to be carried out by specific means, instrumentalities or devices. In other respects the Arab Convention's notion of terrorism is narrower: it requires the underlying act to be violent, and it excludes acts performed in the course of a war of national liberation (as long as such war is not conducted against an Arab country). On the basis of treaties, UN resolutions and the legislative and judicial practice of States, there is convincing evidence that a customary rule of international law has evolved on terrorism in time of peace, requiring the following elements:

- (i) the intent (*dolus*) of the underlying crime and
- (ii) the special intent (*dolus specialis*) to spread fear or coerce authority;
- (iii) the commission of a criminal act, and
- (iv) that the terrorist act be transnational.

The very few States that still insist on an exception, for the Special Tribunal to the definition of terrorism can, at most, be considered persistent objectors. A comparison between the crime of terrorism as defined under the Lebanese Criminal Code and that envisaged in customary international law shows that the notion in the customary rule is broader with regard to the means of carrying out the terrorist act, which are not limited under international law, and narrower in that it only deals with terrorist acts in time of peace, it requires both an underlying criminal act and an intent to commit that act and it involves a transnational element.

²¹ The Arab Convention on the Suppression of Terrorism Signed at Cairo on 22 April 1998, entry into force in accordance with Article 40, available at this URL: https://www.unodc.org/tldb/pdf/conv_arab_terrorism.en.pdf

As a result, for the purpose of adjudicating these facts, the Tribunal is justified in applying, at least in one respect, a construction of the Lebanese Criminal Code's definition of terrorism more extensive than suggested by Lebanese case law. While Lebanese courts have held that a terrorist attack must be carried out through one of the means enumerated in the Criminal Code, the Code itself suggests that its list of implements is illustrative, not exhaustive, and might therefore include also such implements as hand guns, machine-guns and so on, depending on the circumstances of each case. This interpretation of Lebanese law better addresses contemporary forms of terrorism, such as cyber terrorism and also aligns Lebanese law more closely with the relevant international law that is binding on Lebanon.

A central issue concerns the compatibility of this interpretation with the principle of legality²². For Special Tribunal this interpretation does not run counter to the principle of legality (*nullum crimen sine lege*) because this interpretation is consistent with the offence as explicitly defined under Lebanese law. On the basis of the sentence of the Tribunal, moreover, it was accessible to the accused, especially given the publication of the Arab Convention and other international treaties ratified by Lebanon in the Official Gazette (none of which limits the means or implements by which terrorist acts may be performed), hence, it was reasonably foreseeable by the accused.

In sum, and in light of the principles enunciated above, the notion of terrorism to be applied by the Tribunal consists of the following elements:

- (i) the volitional commission of an act;
- (ii) through means that are liable to create a public danger; and
- (iii) the intent of the perpetrator to cause a state of terror.

²² Cfr. G. WERLW, F. JESSBERGER, *Principles of Intentional Criminal law*, Third Ed., Oxford, 2014; M. C. BASSIOUNI, *International Criminal Law*, Third ed., Vol. II, *Multilateral and Bilateral Enforcement Mechanisms*, 2008, Leiden; H. H. JESCHECK, *The General Principles of International Criminal Law set-out in Nuremberg, as Mirrored in the ICC Statute*, in *Journal of International Criminal Justice*, 2004, pp. 38-55; M. CAIANIELLO, E. FRONZA, *Il Principio di legalità nello Statuto della Corte Penale Internazionale*, in Aa. Vv., *La Corte Penale Internazionale per l'ex Jugoslavia*, (edited by) G. CARLIZZI, G. DELLA MORTE, A. MARCHESI, Napoli, 2003; M.C. BASSIOUNI, *International Crimes: "Jus Cogens" and "Obligation Erga omnes"*, in *Law and Contemporary Problems*, 1996, pp. 63-74; G. CARELLA, *Il Tribunale penale internazionale per l'ex Jugoslavia*, in P. PICONE, (edited by), *Interventi delle Nazioni Unite e diritto internazionale*, Padova, 1995, pp. 478 ss.

Considering that the elements of the notion of terrorism do not require an underlying crime, the perpetrator of an act of terrorism that results in deaths would be liable for terrorism, with the deaths being an aggravating circumstance; additionally, the perpetrator may also, and independently, be liable for the underlying crime if he had the requisite criminal intent for that crime.

This definition may be applied also for the cyber terrorism.

This definition also allows us to identify the differences between cyber terrorism and cyber war: the objective element is the same, but the actor is different, because the cyber war should be realized by a State. The fundamental difference is the nature of the aggressor. If this is the conclusion of the Special Tribunal for Lebanon, it is necessary to analyze two core issues related to it. The first is related to the definition of cyber terrorism and in particular to the possibility that the cyber terrorism is able to generate a public danger, considered the means used and the second is a legal technical issue concerning the conditions for the formation of a customary rule.

Concerning the first issue, the UNDOC (United Nations office on Drugs and Crime) in the official document "The Use of the Internet for Terrorist purposes, edited by UN in N.Y, established that " The use of the Internet to further terrorist purposes disregards national borders, amplifying the potential impact on victims". The existence of the possibility to cause "public danger" requirement will be analyzed on a case by case²³.

Massive and coordinated cyber attacks were in May 2007 launched against websites of the government, banks, telecommunications companies, Internet service providers and news organizations in Estonia²⁴. The attacks have been described as targeted and well organized from outside Estonia, and were attacks on the public and private critical information infrastructure of a State. It was estimated that 1 million computers around the

²³ United Nation Office on Drugs and Crime (UNODC), *The Use of the Internet for Terrorist Purposes*, New York, 2012, available at http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

²⁴ HERZOG, *Revisiting the Estonian cyber Attacks: Digital Threats and Multinational Responses*, in *Journal of Strategic Security*, 2011, available at <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss>; CZOSSECK, OTTIS, TALIHÄRM, *Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organization Changes in Cyber security*, in WARREN (edited by), *Case Studies in Information Warfare and Security*, 2013, London, pp.72-91; ALENIUS, *An Exceptional war that Ended in Victory for Estonia or an Ordinary e-disturbance? Estonian Narratives of the Cyber-Attacks, in 2007*, *ibidem*, pp. 55-71.

world were involved through the use of botnets. Some described it as "the Big Bang" as 4 million packets of data per second, every second for 24 hours, bombarded a host of targets that day. The attacks forced banks to shut down online services for all customers for an hour and a half, and disrupted government communications.

In the 2012, a new malware has affected the network authorize to the Informatics system control of the Iranian Center for Nuclear Energy: the computer of the Iranian Organization, at the moment of the collapse have reproduce the song "Thunderstruck" of the Australian hard-rock band AC/DC. The same song that in the Panama invasion of 1989, used by U.S. Army in order to force the General Noriega to leave the reinforced residence²⁵.

Cyber attack are used, generally, to disable or manipulate physical or critical infrastructure, for example the provision of electrical networks, railroads, or water supplies could be infiltrated to have wide negative impacts on particular geographical areas. Moreover cyber terrorism attacks are used against a cloud computing server in which are stored sensitive data, health data or security data²⁶.

NATO defines critical infrastructure or (CI) as those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functions of a government. CI can also include a dizzying array of physical assets, functions, information, people, and systems or what we now call nation's critical infrastructures. To protect CI, government and industry must collectively identify priorities, articulate clear goals, mitigate risk, measure progress and adapt based on feedback and the changing environment²⁷.

²⁵ SANGER, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, in *New York Times*, June, 1, 2012. Ruotolo, *Internet-ional Law, Profili di diritto internazionale pubblico della rete, op.cit.*, in particular p. 98 ss; BUYLER, *When Cyberweapons End up on Private Networks: Third Amendment Implication for Cybersecurity Policy*, in *American University law Review*, 2013, pp. 1204-1238; DENNING, *Stuxnet: What has Changed?*, in *Future Internet*, 2012, pp. 672-687.

²⁶ MURAT DOGRUL , ADIL ASLAN , EYYUP CELIK, *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, in *2011 3rd International Conference on Cyber Conflict*, C. CZOSSECK, E. TYUGU, T. WINGFIELD (Eds.) Tallinn, Estonia, 2011.

²⁷ In the past decade, NATO has made considerable progress in areas of importance to the Alliance such as operations, enhanced intelligence exchange and the development of technology solutions through the Defence against Terrorism Program of Work and the Science for Peace and Security Program. With respect to issues and concerns, security planners are confronted with panoply of possible future scenarios coming from sources ranging from the terrorists themselves—from either their public statements or intelligence

Concerning the second issue, the doctrine show that The Appeals Chamber's reasoning with regard to the notion of terrorism contains two major flaws:

0 it will be demonstrated that for tasks at hand it was unnecessary for the Appeal Chamber to establish whether terrorism was a criminal offence under international customary law or not.

1 The finding that a customary rule of international law regarding the international crime of terrorism, at last in time of peace, have evolved is based on insufficient and therefore cannot be upheld.

It is possible manage the first question, but it is necessary to look at the second aspect, that of the reconstruction of about the existence of a rule of customary law to define international terrorism.

Doctrine defines the reconstruction of the Appeal's Chamber as "revolutionary" and "highly inventive" for serious reason. Firstly, many scholars and other legal experts have already stated, currently no universal definition of terrorism exist. This agreement not only applies to international treaty law, but also to customary international law. For the doctrine the conditions for a rule establishing a definition of terrorism under customary criminal international law have not been met in the case of terrorism. The essence of custom, according to article 38 of the Statute of the International Court of Justice, is that it should present "evidence of a general practice accepted as law".²⁸ In order for a rule of customary international law to exist, tow requirements need to e fulfilled: the material

collected on their deliberations—to red-team brainstorming efforts to explore ways adversaries might attack in the future. NATO has prepared a 'Strategic Concept' in 2010, and revised it in 2011, to further develop its ability to prevent, detect, defend against and recover from cyber-attacks by expanding its capacity in cyber-security. NATO Member States reinforced the importance of international cooperation in the Chicago Summit Declaration of May 2012. Cooperation between member states is important for organizing, creating and enforcing a security standard about those national cyber-systems, which are vital for the effective functioning of the whole alliance. This includes collaboration on a number of fronts including optimized information sharing, situational awareness, and secure interoperability based on agreed sets of common standards. Countering terrorism and the protection of CI requires partnerships. Achieving NATO counter-terrorism goals requires an integrated, collaborative approach by government, the private sector, citizens, and other international partners. It will never be possible to stop all terrorist attacks. Cfr. *Critical Infrastructure Protection against Terrorist Attacks, Course Report*, Nato Coe Dat, Ankara, Turkey, 3-7, November 2014, available at this url: http://www.coedat.nato.int/publication/course_reports/12-CIP.pdf

²⁸

Article 38(1) of the Statute of the International Court of Justice is widely recognized as the most authoritative statement as to the sources of international law. It provides as follows: "the Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: (a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting parties; (b) international custom, as evidence of a general practice accepted as law; (c) the general principles of law recognized by civilized nations; (d) subject to the provision of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary

Foggetti, Nadina, "Cyber Terrorism and the reconstruction of customary rule about terrorism of the Special Tribunal for Lebanon in the recent case law", *IUS ET SCIENTIA*, 2015, Vol. 1, No. 1, pp. 54-78.
DOI: <http://dx.doi.org/10.12795/IETSCIENTIA.2015.i01.05>

means for the determination of rules of law.”

element, i.e. there must be a widespread repetition by States of similar international acts over time (State practice), and the psychological or subjective element, i.e. the belief that such behaviors is "law", i.e. legally binding (the formation of an *opinio iuris sive necessitatis* in international community), as opposed to a mere moral or social obligation or usage²⁹. A core issue concerns the *Opinio juris sive necessitates*, as a constitutive element of a customary rule in international law.³⁰ Doctrine states that the Appeal Chamber starts in a rather unconventional fashion, namely by citing a few - to be exact: five - selected decision of different national courts which are found to have acknowledged the existence of a common definition of terrorism under customary international law. Judicial decisions act as a subsidiary means for determining international legal rules on the bases of art. 38 (1) (d) of the ICJ Statute. For this reason, they may constitute persuasive evidence of a customary rule³¹. A limited number of isolated decisions suggest the emergence of a definition of "terrorism" under international law, they all offer different definitions of what it entails. Concerning the definition of terrorism, doctrine notes that the STL cites nine judicial decisions as evidence of explicit recognition of a crime of terrorism under customary international and that the Appeals Chamber does not discuss. Doctrine notes that it ignores, either by omission or relegation to a single footnote, a number of identifiable authoritative domestic precedents that directly contradict this conclusion.

²⁹ TEUBNER, *International Customary Law and Codification*, Leiden, 1972; TUNKIN, *Remarks on the Judicial Nature of Customary Norms of International Law*, in *California Law Review*, pp. 419-435; SEGURA SERRANO, *Internet Regulation and the Role of International Law*, in; *Max Planck Yearbook of United Nations Law*, 2006, p. 377 ss.; POLANSKI, *Customary Law in the Internet: in the Search for a Supranational Cyberspace Law*, Berlin, 2007; CHIK, *Customary internet-ional law: Creating a body of customary law for cyberspace*, in *Computer & Security Review*, 2010, pp. 3-28; DUMBERRY, *Incoherent and Ineffective: the concept of Persistent Objector Revisited*, in *International and Comparative Law Quarterly*, 2010, pp.778-802; ALVAREZ-JIMÉNEZ, *Methods for the Identification of Customary International Law in the International Court of Justice's Jurisprudence: 2000-2009*, in *International and Comparative Law Quarterly*, 2001, pp. 681-712; CONFORTI, *Diritto internazionale*, Napoli, 2014.

³⁰ CONFORTI, *Diritto internazionale*, Napoli, 2014; B.D. LEPARD, *The necessity of Opinio Juris in the formation of Customary international Law*, Discussion Paper for Panel on "Does Customary International Law Need *Opinio Juris*?", available at this URL: https://law.duke.edu/cicl/pdf/opiniojuris/panel_2-lepard-the_necessity_of_opinio_juris_in_the_formation_of_customary_international_law.pdf; J. KAMMERHOFER, *Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems*, in *European Journal of International Law*, 2004, pp. 523-534; M. MENDELSON, *The Subjective Element in Customary International Law*, in *British Yearbook of International Law*, 66, 1995, pp. 206-207. BIN CHENG, *United Nations Resolutions on Outer Space: 'Instant' International Customary Law?*, in *International Law: Teaching and Practice*, (edited by) BIN CHENG, London, 1982, pp. 251 in particular affirming that "international customary law has in reality only one constitutive element, the *opinio juris*".

Foggetti, Nadina, "Cyber Terrorism and the reconstruction of customary rule about terrorism of the Special Tribunal for Lebanon in the recent case law", *IUS ET SCIENTIA*, 2015, Vol. 1, No. 1, pp. 54-78.
DOI: <http://dx.doi.org/10.12795/IETSCIENTIA.2015.i01.05>

³¹ Cfr. A. D'AMATO, *The Concept of Custom in International Law*, New York, 1971.

In particular, there were no reference to the only known international precedent according to which "terrorism has never been singly defined under international law". Nonetheless, the Appeals Chamber presents the cited cases as reflective of the collective jurisprudence of the international community. Doctrine outlines that a closer scrutiny of the cases suggests that the Appeals Chamber appears to have "misread, exaggerated or misinterpreted every one of those decisions"³². Some national judicial decisions have recognized that specific offences of terrorism, such as hijacking and hostage taking, may have acquired customary status. Between these, only one decision explicitly states that terrorism has crystallized into a customary crime and provides a definition³³. Yet in that decision by the Italian Supreme Court of Cassation, the definition formulated departed from that proffered by Appeals Chamber. The Italian Court required an additional indispensable element in order for conduct to amount to terrorism. By disregarding a mandatory element of the Italian Court's definition, the Appeals Chamber's reliance is both selective than objectionable. Thus the key judgment on which the Appeals Chamber relies is fundamentally incompatible with its own conclusion. None of the decisions analyzed, individually or collectively, supports the Appeals Chamber's formulation of a customary crime of terrorism³⁴. For the doctrine these cases are not sufficient.

In the field of these objections it is possible to note that the Appeals Chamber is not blinded to the fact that these decisions are not, as such, sufficient to establish a rule under customary law.

³² *Prosecutor v Stanilav Galic (Trial Judgement and Opinion)* Appeals Chamber IT-98-29-T 5 December 2003.

³³ A. CLERE, *An Examination of the Special Tribunal for Lebanon's Explosive Declaration of "Terrorism" at Customary International Law*, Otago, 2012, available at this url: <http://www.otago.ac.nz/law/research/journals/otago043934.pdf> The case law cfr. *Bouyahia Maher Ben Abdelaziz et al*, Judgement of 11 October 2006 Corte di Cassazione.

³⁴ At [2.1] The Italian Court of Cassation required that the act in question must contain a "political, religious or ideological motivation in accordance with generally accepted international standards". The Court stated that without this purposive element, the concerned act cannot be constituted as terrorism as it lacks the additional characteristic that transforms other crimes into the special crime of terrorism. The Appeals Chamber (Interlocutory Decision, above n 23, at 106) observed that discrepancies in state practice concerning the inclusion of an element of ideological, political, religious or racial motive "has not yet been so broadly and consistently spelled out and accepted as to rise to the level of customary law....[I]t remains to be seen whether one day it will emerge as an additional element of the international crime of terrorism", and so omits the requirement from the definition formulated.

It states that: "*However significant these judicial pronouncements may be an expression of the legal view of the courts of different States, to establish beyond any shadow of doubt whether a customary rule of international law has crystallized on must also delve into other elements*".

It is possible, in this context to note that United Nation General Assembly has insisted since 1994 that "*criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons for political purposes are in any circumstance unjustifiable*"³⁵.

The UN has established the Ad Hoc Committee tasked to draft a Comprehensive Convention on Terrorism. The committee has not achieved to come up with such a comprehensive convention, because there are pending issues of constant disagreements that include:

- a) whether the Draft Convention should adopt an armed conflict or law enforcement approach to counter-terrorism;
- b) whether a definition of terrorism should include or exclude "state terrorism";
- c) whether armed resistance to an occupying regime or to colonial alien domination should be included or excluded.

For these elements it is possible to states that there are not an *opinion iuris* or an agreement, but it is possible that this agreement may concerns the substantial elements.

Moreover, the UN convention for the Suppression of the Financing of Terrorism provides the UN's clearest definition of terrorism, which includes the elements of (i) a criminal act (ii) intended to intimidate a population or compel an authority, and is limited to those crimes containing (iii) a transnational aspect³⁶.

The interpretation of Lebanon or Italian Criminal law concerning terrorism in light of international law, may be considered such as an "evolutionary adaptation" to the to the changing conditions of international community social norms.

³⁵ Cfr. Resolution 51/210, concerning Measures to eliminate international terrorism, adopted by the General Assembly in 88th Plenary meeting, A/RES/51/210, of 17 December 1996, available at this URL: <http://www.un.org/documents/ga/res/51/a51r210.htm>

³⁶ International Convention for the Suppression of the Financing of Terroris, Adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999, available at this URL: <http://www.un.org/law/cod/finterr.htm>

In this field it is possible to comply the three strictly requirement established by European Court of Human Rights in order to derogate the principle of legality: the adherence of the new *figura criminis* to the essential core of crime; the conformity with fundamental criminal international principles; its reasonable foreseeability for of the recipients.³⁷

The nature and the purpose of the institution of STL are not an obstacle to this interpretation. The persons accused in the future will be guaranteed by the need for International Tribunal to prove more adjective condition for prosecute the action.

Moreover, if the STL or other international o special Tribunal established on the Base of the VII Chapter of the UN Treaty, not apply a definition international oriented of crimes such as Terrorism, their function may be nullified. Their institution, in fact is justified on the inadequacy of national courts to prosecute the core crime, or the crime that transcend national bounders, that are transnational in nature.

The STL is a small but important step in the international community towards the preparation of breath supranational institutions capable of guaranteeing the human right of "last generation" already stated, albeit with a completely different semantic value, in

³⁷ F. COSTAMAGNA, *Derogating from ECHR Obligations to Fight International Terrorism: Analysis of Some Controversial Issues*, in *La Comunità Internazionale*, 2007, pp. 111-150; S. GREER, *The Margin of appreciation: interpretation and discretion under the European Convention on Human Rights*, Council of Europe, 2002, available at this URL: [http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17\(2000\).pdf](http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf);

H.C. YOUROW, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence*, The Hague/Boston/London, 1996; P. MAHONEY, *The Doctrine of the Margin of Appreciation under the European Convention on Human Rights: Its Legitimacy in Theory and Application in Practice*, 1998, in 19 *Human Rights Law Journal*, pp. 1-36; N.LAVENDER, *The Problem of the Margin of Appreciation*, 1997, in *European Human Rights Law Review*, pp. 380-390; E. BREMS, *The Margin of Appreciation Doctrine in the Case-Law of the European Court of Human Rights*, 1996, in *Zeitschrift für Ausländisches Öffentliches Recht und Völkerrecht*, pp. 240-341; T.H. JONES, *The Devaluation of Human Rights Under the European Convention*, in *Public Law*, 1995, pp. 430-449; R.ST.J. MACDONALD, *The Margin of Appreciation*, in R.ST.J. MACDONALD, F. MATSCHER AND H. PETZOLD (edidit by), *The European System for the Protection of Human Rights*, Dordrecht/Boston/London, 1993, pp. 83-124; A. CLAPHAM AND F. EMMERT (edited by), *Collected Courses of the Academy of European Law: Vol. 2, Book 2 - The Protection of Human Rights in Europe*, Dordrecht/Boston/London, 1990, pp. 99-161; *The Margin of Appreciation in the Jurisprudence of the European Court of Human Rights* in *Le droit international à l'heure de sa codification, Études en l'honneur de Roberto Ago*, Milan, 1987, pp. 187-208; H.C. YOUROW, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence*, in *Connecticut Journal of International Law*, 1987, pp. 111-159; T.A. O'DONNELL, *The Margin of Appreciation Doctrine: Standards in the Jurisprudence of the European Court of Human Rights*, in *Human Rights Quarterly*, 1982, pp. 474-496; C.S. FEINGOLD, *The Doctrine of Margin of Appreciation and the European Convention on Human Rights*, in *Notre Dame Lawyer*, 1977-78, pp. 90-107; C.C. MORRISSON, *Margin of Appreciation in European Human Rights Law*, In *Revue des Droits de l'Homme*, 1973, pp. 263-286.

the preamble of the Declaration Universal Declaration of Human Rights of 1948: freedom from fear ("freedom from fear"), or rather by terror.

3. The EU Antiterrorism measure and the right to privacy in the EU and ECHR prospective.

A moreover issue that we must examine is whether the acts in question meet the fundamental principles of European law and European Convention on Human Rights. The protection of privacy under the law remains anchored however to the First pillar, while the fight against terrorism and crime takes place in the Second and Third pillar. For this reason it is difficult to balance the protection of privacy with the fight against international terrorism and to assess the impact of measures taken by institutions in order to reach this specific purpose.

In the just mentioned case law, the European Court of the Court held that the powers of the Community should be exercised in accordance with international law. This provision applies even in the maintenance of international peace and security in the implementation of resolutions adopted by the CdS under Chapter VII of the Charter³⁸. The EU Court states that the Regulation is an EU act and then the Court is asked to assess their compatibility with fundamental rights.

In this contest, the EU Court of Justice in a Case of September 3, 2008, annuls the Council Regulation on May 27, 2002, n. 881, which imposes restrictive measures directed against certain persons and entities associated with Osama bin Laden, the Al-Qaeda and the Taliban, and repealing Regulation (EC) No 467/2001³⁹.

But it orders that effects of Regulation No 881/2002 to be maintained, so far as they concern Mr Kadi and the Al Barakaat International Foundation, for a period that may not exceed three months running from the date of delivery of this judgment⁴⁰.

However, the reasoning of the Court of Justice clearly shows the prevalence of the need to respond to the terrorist threat.

The Court, therefore, claims that the fight against terrorism prevails on fundamental

³⁸ Judgment of the Court of 20 May 2008, C-91/05, *Commission v Council*, in: www.europa.eu

³⁹ Judgment of the Court of 3 September 2008, C-402/05 P e C-415/05, *Yassin Abdullah Kadi c. Council*, in www.europa.eu.

⁴⁰ Council Regulation of 27 May 2002, Official Journal of EU, L 139, 2002.

rights.

In the second instance we must analyze if the PNR Agreement impair the European Convention on data retention and European Convention on Human rights.

To analyze the admissibility of the transfer of personal data in the light of the European Convention for the protection of data, we must consider the letter sent in July 2007 by DHS particularly the statement which outlined the terms and conditions for the data transfer .

The letter states that the data transferred to US authorities will be used solely for the prevention and suppression of international terrorism and related crimes and the prosecution of other serious crimes, including transnational organized crime⁴¹.

Personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes. The purpose of the fight against terrorism is determined. On the contrary, we cannot say that the aim is determined or determinable in relation with the crimes. The letter does not reveal, in fact, what are the serious crimes listed in the letter, which will be the criteria to be taken into consideration in order to identify these types of crimes.

We can therefore conclude that the agreement signed bring the Convention signed by EU Member States in relation to the obligation to ensure the definition and certainty of the purpose for which this is done.

The agreement also contrasts with Article 6 of the Convention concerning personal data. For this particular category of personal data, the Convention provides that they may not be processed automatically if national laws do not establish appropriate safeguards.

The same agreement also does not allow an adequate protection of the right to correct personal data subject to treatment and thus it is contrary to Article 8 of the European Convention for the protection of personal data.

⁴¹ N. FOGGETTI, *Cyber-Terrorism and the Right to Privacy in the Third Pillar Perspective*, in *Masaryk University journal of Law and Technology*, 2009, pp. 365-376.

The PNR agreement and the letter DHS, in fact, guarantee only the application of the law in force in the U.S. on the matter, such as the Patriot Act. But it is applicable only to U.S. citizens.

Neither is true that the mere reference made by the DHS letter of this legislation, ensure the extension of its scope to individuals holding the data processed regardless of the nationality of the same.

The agreement is contrary to Article 8 of the European Convention on Human Rights as interpreted by the Strasbourg court.

In particular, analyzing the prevailing case law of the European Court, it can be concluded that the collection and transmission of personal information by public authorities brings the article 8. On the basis of criteria identified by the Court in its jurisprudence, a treatment must pursue a legitimate aim of public interest, and it must be proportionate⁴².

4. The protection of individuals against acts affecting the right to privacy.

At EU level, citizens can appeal to the Court of First Instance and then to the Court of Justice of the European Union, but we have seen that recent case law is not in favor of the protection of fundamental rights when dealing with the fight against terrorism. We must then determine whether the conclusion of the PNR is attributable to the states. In order to solve this problem we must refer to the legal basis on which the agreement was concluded.

The legal basis is Articles 24 and 38 EU Treaty. An analysis of these provisions easily shows the crucial role played by Member States in concluding such agreements.

Article 24 states that the Council may decide by a qualified majority whether the agreement is expected to implement a common position or a joint action. It should be noted that these acts must be approved unanimously. Article 24 refers to Article 23, par. 2 which state that "If a member of the Council declares that, for important reasons of national policy, intends to oppose the adoption of a decision taken by qualified majority, a vote. The Council, acting by a qualified majority, requests that the matter be referred to the European Council for decision by unanimity.

The role of States is essential in this case. Data processing must respect the principle of proportionality.

In this particular context, the Court has noted, on several occasions, that in order to assess the proportionality of the same treatment, states must guarantee the right of access to data. The agreement provides only for transferring data from European airlines to US authorities. The agreement conflicts with the European Convention on Human rights.

The states are liable for the breach of the European Convention on Human Rights In the fight against terrorism.

5. Concluding remarks

Many countries introduced extraordinary laws and policies and emergency legislation. We see the introduction of new surveillance power of the State in answers to terrorism. Privacy was also affected by the use of very technologically advanced instruments of control⁴³.

The administration of emergency has ultimately become "*condicio sine qua non*" for the maintenance of international security.

In the USA and UK many of these laws have come to be questioned in parliaments,

⁴³ TERRASI, L.M., *Trasmissione dei dati personali e tutela della riservatezza: l'accordo tra Unione europea e Stati uniti del 2007*, *Rivista di diritto internazionale*, 2007, pp. 375-389.

through the media, the courts, and in the public sphere. Some have been seriously amended or found unconstitutional while others have been enhanced.

the program for intercepting telephone calls and e-mail authorized by Bush 2001 and renewed in subsequent years, was ultimately blocked for violation of the First and the Fourth Amendment. In particular, the Court of Detroit noted that "It is not possible to pursue the goal of security by depriving citizens of constitutionally guaranteed rights".

The administrative emergency, ultimately, must ensure the protection of human rights. The real problem is the disappearance of the temporary nature of the emergency requirement.

What is more significant in view of the measures taken to combat international terrorism, will be the loss of the temporary nature of the emergency requirement.

In short, the emergency and the rules designed to adjust from temporary became permanent.

The Court maintained that the proportionality test has to be applied by taking into consideration a number of factors, such as the nature of the rights affected and the duration of the measures.

The Court made clear that the States are bound to the continuous reassessment of the effectiveness of the measures adopted and to repeal if they are found inadequate to meet the danger.

A further element that plays an increasingly important role in assessing the measures proportionality is the existence of safeguards against the abuse of emergency powers. When the Executive interferes on fundamental values, such as personal freedom or privacy, the derogating measures are proportionate only when it provides a meaningful degree of judicial or independent control.

However, we doubt that the EU law, today, ensured an effective remedy for those affected and, hence, that the measures do not meet the proportionality requirement.

⁴⁶ Cfr. DE LEONARDIS, R.I. 2005, *Il principio di precauzione nell'amministrazione del rischio*, cit.