

**Regulating Illegal Material on the Internet:
The European Legislative Landscape**

Request for Comment

IIEA NLM RFC 1

Oisin Suttle

**Institute of International and European Affairs
www.iiea.com**

Introduction to the RFC Document Series	4
IIEA study of non-legislative measures to prevent the distribution of violent radical content on the Internet.....	6
PROJECT INTRODUCTION.....	7
OBJECTIVE OF THIS PAPER	8
SCOPE	10
GENERAL PROVISIONS AFFECTING ISP LIABILITY IN EUROPE	11
Relevant Provisions	11
Implications	12
ISP LIABILITY AND COPYRIGHT MATERIAL	13
Relevant Provisions	13
Relevance to IIEA Study of Non-Legislative Measures	16
HATE SPEECH.....	18
Council of Europe Measures	18
The Additional Protocol to the Cybercrime Convention 2003	18
Background and Analysis.....	19
Relevance to IIEA Study of Non-legislative Measures.....	19
Other Relevant Measures.....	20
CHILD PORNOGRAPHIC CONTENT.....	22
European Union Measures	22
Framework Decision 2004/68/JHA.....	22
Background and Analysis.....	22
2009 Proposed Framework Decision amending Framework Decision 2004/68/JHA	24
Other Relevant Provisions.....	25
Alternative Approaches – US Model	25
General Observations	26
European Union Measures – Framework Decision 2002/475/JHA and Framework Decision 2008/919/JHA.....	27
Background and Analysis.....	28
HUMAN RIGHTS ANALYSIS	31

Relevant Provisions	31
Background and Analysis.....	31
CONCLUSION AND REQUEST FOR COMMENTS.....	34
ANNEX 1 – E-COMMERCE DIRECTIVE	36
ANNEX 2 – COPYRIGHT DIRECTIVE.....	39
ANNEX 3 – CYBERCRIME CONVENTION – ADDITIONAL PROTOCOL ..	41
ANNEX 4 – CONVENTION ON THE ELIMINATION OF RACIAL DISCRIMINATION.....	44
ANNEX 5 – FRAMEWORK DECISION 2004/68/JHA	45
ANNEX 5 – PROPOSED FRAMEWORK DECISION COM(2009)135 FINAL .	48
ANNEX 6 – FRAMEWORK DECISION 2002/475/JHA	50
ANNEX 7 – FRAMEWORK DECISION 2008/919/JHA	52
ANNEX 7 – EUROPEAN CONVENTION ON HUMAN RIGHTS	54

Introduction to the RFC Document Series

In the early days of computer networking, as a company called BBN started building the IMPs (Interface Message Processor computers) for the ARPANET (the forerunner to the Internet), an important piece of the network was missing: the software that would govern how computers would communicate with each other. Graduate students at various facilities funded by the US Department of Defense Advance Research Projects Agency (ARPA) had been given the task in 1969 of developing the missing communication protocols. They formed an informal “network working group”. Finding themselves working in a vacuum, they began developing not only these technical protocols, but also the informal protocols that would influence interpersonal communications on the Internet in general.

Uncertain of their positions within the hierarchy of the ARPANET project, the students issued notes on their protocols under the title of “Request for Comments” (RFC). Steve Crocker, a graduate student who had received his bachelors degree at UCLA only a year before, used the title Request for Comments to make the invitation to participate as open as possible, and minimise any claim to authority that working on so crucial an aspect of the network as its protocols might imply. The first RFC document, which set the tone for the next half century of Internet culture and initiated the process of defining the protocols that now govern virtually all data exchange on the planet, was composed in humble circumstances. Its author recalls: “I had to work in a bathroom so as not to disturb the friends I was staying with, who were all asleep”.¹

Crocker was writing a document that outlined some broad ideas on how the students would pass around ideas through “temporary, informal memos”.² Even as he drafted the prospect of disapproval from far above in the academic hierarchy weighed heavily upon him: ‘In my mind, I was inciting the wrath of some prestigious professor at some phantom East Coast establishment. I was actually losing sleep over the whole thing’³.

Crocker was eager to open up the process to as many of his peers as possible: ‘Closely related to keeping the technical design open was keeping the social process around the design open as well. Anyone was welcome to join the party’⁴. Vint Cerf, an early participant in the informal networking group, and now Vice President of Google, sums up the approach and context:

Keep in mind that the original developers of the host level protocols were mostly graduate students. We adopted a humble and inclusive posture

¹ Steve Crocker, “How the Internet got its rules”, *New York Times*, 6 April 2009; Steve Crocker, Request for Comments, 7 April 1963 (URL: www.ietf.org/rfc/rfc0001.txt, last accessed 2 December 2009).

² *ibid.*

³ *ibid.*

⁴ Steve Crocker to Johnny Ryan, E-mail, 19 April 2009.

and a mantra that Dave Clark ultimately coined as "rough consensus and running code" - that means we don't really vote exactly, we just try to assess rough consensus among the group trying to agree on proposed standards.⁵

Through this open and collaborative process the group first developed the Network Control Protocols (NCP) and then proceeded to work on a more advanced protocol that could allow different networks to communicate with each other. Much as the packet-switched network concept is an essential characteristic of the internet that informs the communications and culture on it, so the network protocols and the manner in which they were developed were an important development toward less hierarchical and formal norms.

RFC 3, released in April 1969, elaborated on the character and objectives of the RFCs. (Note that the word "Host" here refers to a connected computer.)

These standards (or lack of them) are stated explicitly for two reasons. First, there is a tendency to view a written statement as ipso facto authoritative, and we hope to promote the exchange and discussion of considerably less than authoritative ideas. Second, there is a natural hesitancy to publish something unpolished, and we hope to ease this inhibition.⁶

RFC 3 continues in the counter-hierarchical vein, establishing the principle that no text should be considered authoritative, that there is no final edit. Authority was to be derived from merit rather than fixed hierarchy.

Crocker's RFC, though penned in a humble circumstances, set the open, inviting tone of the next half century of Internet culture. Almost 6,000 RFCs have since been published, maintaining an open, collaborative approach in Internet engineering circles.

The IIEA (Institute of International & European Affairs) has adopted the RFC to disseminate materials that are not yet in final release form, and which could usefully benefit from the input of a wider group of contributors and commentary. These RFCs reflect work in progress. Our hope is that, having read this paper, you will have comments on it, whether in terms of approach, methodology, content or presentation. Please do not hesitate to send your comments to the project coordinator, Caitriona Heidl, at caitriona.heidl@iiea.com.

Johnny Ryan
Principal Investigator

⁵ Vint Cerf to Johnny Ryan, E-mail, April 2009.

⁶ Steve Crocker, RFC 3, April 1969 (URL: www.faqs.org/rfcs/rfc3.html, last accessed 2 December 2009).

IIEA study of non-legislative measures to prevent the distribution of violent radical content on the Internet

Please note that, as work in progress, these reports should not be treated as complete or authoritative, and should not be relied on in any way. In particular, they do not constitute and should not be regarded as legal or other advice. Any person seeking guidance on legal or other aspects of Internet regulation should seek the advice of a solicitor or other appropriate professional. Neither the Institute of International and European Affairs nor any researcher or other person involved in the preparation of this paper accepts any liability in respect of its contents.

Project Introduction

The Institute of International and European Affairs (the “IIEA”) has been commissioned by the European Commission to prepare a study of non-legislative measures to prevent the distribution of violent radical content on the Internet.

More detail on this research project can be found at <http://www.iiea.com/staff?workingGroupUrlKey=violent-radicalisation> and in the project’s Terms of Reference⁷.

This study is part of a wider set of legislative and non-legislative measures proposed by the European Commission as part of its response to the threat of international terrorism. This has included the adoption of Council Framework Decision 2008/919/JHA on combating terrorism, mandating the creation of a number of new offences including recruitment for terrorism, training for terrorism, and public provocation to commit a terrorist offence. A stated goal of the European Commission in proposing these new offences was to provide a sound legal basis for action against terrorist propaganda on the Internet.

⁷ http://ec.europa.eu/justice_home/funding/tenders/2009_S041_058796/annex_1_en.pdf

Objective of this Paper

This Request For Comments is intended to provide an overview of formal legal measures at the European and international level which are specifically adapted to combat illegal content on the Internet, or which are potentially relevant to that task.

The approach adopted in this RFC, and in the IIEA study on countering violent radical content more generally, involves seeing the problem of violent radical content in the context of Internet regulation and content control more generally.

While many of the challenges posed by violent radical content are unique to this area, there are also significant parallels with other classes of illegal material that may be distributed through the Internet. Various initiatives already exist to tackle other types of illegal or harmful material on the internet; in particular, the challenges of child pornography and hate speech have been recognised since relatively early in the development of the internet, and measures have been taken at national, European and international levels to counter these threats. Controlling the dissemination of copyright infringing material on the Internet has also been the focus of significant activity, primarily by private actors, through both formal and informal measures.

The IIEA study will examine non-legislative measures (“NLMs”) taken to combat these various classes of material, assessing their effectiveness and considering their potential applicability at a European level to the problem of violent radical content on the Internet.

However, in order to assess the effectiveness and appropriateness of NLMs, it is also necessary to consider the legal context in which they operate. In their operation, NLMs are complementary to legislative measures in respect of particular classes of illegal material; while, to a limited extent, they may be able to function purely on the basis of voluntary codes of conduct and terms of service accepted by ISPs and content hosts, in general they will interact with the criminal and civil legal framework relating to the relevant class of material⁸. The content of those criminal and civil legal provisions will be an important factor in determining whether, and if so how well, particular NLMs achieve their objectives, and the costs associated with such measures. Differences in the legal context between different classes of content, or across different jurisdictions, may impact on the effectiveness of particular NLMs in a particular field. Further, the relevant legal context is not limited to provisions specifically addressing online content; in many cases, online speech or dissemination of material is simply a specific case of speech and dissemination generally, and laws designed to

⁸ SEC(2009) 356 ‘*Commission Staff Working Paper: Accompanying document to the Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA Summary of Impact Assessment*’

regulate speech and dissemination in general will also be applicable to internet content.

The present review aims to support the ongoing analysis of non-legislative measures in respect of illegal material by providing this necessary legal context. To that end, it outlines the relevant provisions across a number of areas, as well as considering more general provisions on internet liability and human rights which may impact on the operation and effectiveness of non-legislative measures.

Scope

This paper considers relevant legal provisions across the following areas:

- i) general provisions affecting the liability of internet service providers (ISPs);
- ii) specific provisions relating to ISPs and copyright;
- iii) provisions addressing child pornographic content (“CPC”);
- iv) provisions addressing hate speech and racist content (“HS”);
- v) provisions addressing violent radical content (“VRC”); and
- vi) human rights provisions relevant to Internet content control and access.

This paper is limited to considering legal issues as they arise at the international and / or European level. It does not consider issues at the national level, although in places it refers to the experience at the national level, and to material that may address this level.

Review has been limited to the European level in order to limit the scope of this exercise. As noted above, the specific legal context in particular jurisdictions may also be relevant to considering the value of particular measures. However, the practicalities of undertaking a comprehensive legal review in respect of 27 EU member states (and potentially also some non-European jurisdictions) place it outside the scope of this study.

In addition, review has been limited to legal issues. Additional questions of consumer internet use patterns, incentives to report material, and indeed questions around the political and economic will to enforce particular measures will also be relevant in considering whether NLMs from one subject space will be functional in another space. While these issues are touched upon at various points, they are not the focus of this paper and are not analysed in a comprehensive manner. These issues may become the subject of a future RFC and Working Paper.

At this stage of the project, this review is of necessity quite general in tone; it has focussed on two issues that are particularly likely to affect non-legislative responses to illegal material, namely clarity and international harmonisation. However, as the wider project continues and recommendations begin to be formulated it may become necessary to return to and review some or all of the analysis in this paper.

General Provisions affecting ISP Liability in Europe

'Notice and Takedown' procedures, whereby internet service providers, whether hosting services or access providers, may be required to remove material from their services, or to block particular websites, once they have been made aware of them and of their illegal content, constitute a common response to illegal material on the internet. They have the benefit of not requiring that ISPs engage in active monitoring of content, instead transferring the surveillance function to members of the public, law enforcement, interested parties etc. The role of the ISP is rather to act on reports that are brought to its attention.

In addition to subject-specific provisions mandating such procedures (such as that proposed in respect of child pornography, discussed below), the liability provisions of the e-Commerce directive effectively mandate a general notice-and-takedown system for ISPs in respect of illegal material hosted on their services.

Relevant Provisions

The liability regime for ISPs is set out in Articles 12 – 15 of Directive 2000/13/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (the "**e-Commerce Directive**")⁹.

The legal obligations applicable to an ISP depend on the specific services being provided; in particular, different rules apply in respect of the provision of internet access, caching of material for the purpose of transmitting data, and hosting services.

Articles 12 and 13 provide that ISPs have no liability in respect of transmitting material as a 'mere conduit', or caching material for technical reasons, subject to certain conditions which an ISP, acting in the ordinary course of business, will usually meet.

Article 14, in respect of hosting, provides that an ISP providing a service consisting of the storage of information (i.e. hosting) should not be liable for information stored at the request of service recipients, on condition that "(a) the [ISP] does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; and (b) the [ISP], upon obtaining such knowledge or awareness acts expeditiously to remove or to disable access to the information" (Art 14(1)).

⁹ See Annex 1

Article 15 establishes the principle that there is no general obligation on ISPs to monitor the information they transmit or store, nor any general obligation actively to seek facts or circumstances indicating illegal activity.

Implications

This system of liability effectively forces ISPs providing hosting services to operate a notice and take-down procedure in respect of material that they host on behalf of clients.

Whereas the combined effect of Articles 14 and 15 is to ensure that ISPs have no incentive to monitor content they host on their own initiative (as they have no obligation to do so, and no liability in respect of content unless they have actual knowledge of its illegal nature), the proviso to Article 14 means that, once ISPs become (or more likely are made) aware of illegal content hosted on their servers, they must remove it or risk incurring liability in respect of it. This liability regime, together with the lack of clarity around a number of the content-specific provisions discussed below may encourage ISPs to err on the side of caution in removing material where its legality is unclear, relying on their own terms of service to justify such action.

The position in respect of ISPs providing Internet access services is less clear-cut. The 'mere conduit' and caching defences in Articles 12 and 13 apply regardless of whether an ISP is aware that illegal content is being accessed, provided they do not 'select or modify the information' being downloaded, or modify material being cached¹⁰. Again, this creates a strong incentive for ISPs to resist monitoring users, or preventing their accessing material unless required to do so by a court or administrative authority (Art 12(3) and 13(2)).

The e-Commerce Directive therefore establishes a set of incentives (a) for hosting services to operate a notice and take-down procedure; and (b) for ISPs providing internet access to avoid monitoring or interfering with users' internet use, even where they know or suspect that they are accessing illegal material. This framework needs to be borne in mind when considering how far NLMs can operate as a basis for blocking or notice-and-takedown systems.

¹⁰ However, see below in respect of the provisions of the Copyright Directive which arguably challenge this principle.

ISP Liability and Copyright Material

The analogy between violent radical content (“VRC”), child pornographic content (“CPC”) and hate speech and racist content (“HS”) is clear; each represents a class of material whose distribution is commonly prohibited by the criminal law. However, in recent years debates on the scope of permissible internet use, and on strategies to restrict illicit use, have focussed heavily on another class of material, namely illegally distributed copyright material, including in particular copyright music and films.

The issues raised by copyright infringement through the internet are somewhat different to those posed by HS, CPC and VRC. In particular, the distribution of copyright material is commonly addressed through civil rather than criminal law remedies (although criminal provisions may also be relevant); and the fight against copyright infringing material has been led by the private sector, and in particular the music industry, with a very secondary role for law enforcement authorities.

Relevant Provisions

At the European level, the relevant provisions are set out in Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (the “Copyright Directive”)¹¹. As regards preventing the online distribution of copyright material, the policy underlying the directive is set out in recital 59, which notes that that: *“[i]n the digital environment ... the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore ... rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject-matter in a network”*.

This policy is implemented through Article 8. While Article 5(a) establishes a general exemption from liability for network intermediaries, Article 8 qualifies that exemption, providing that: *“Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right”*.

This provision may appear to contradict the provisions of the e-Commerce directive. Certainly, it challenges the general principle in Article 12 of that directive that ISPs should have no liability in respect of content which users access. However, it is mirrored in the proviso to Article 12, which provides that *“[t]his provision shall not affect the possibility for a court or administrative authority, in*

¹¹ See Annex 2

accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement" (Art 12(3)).

Article 8 must also be read in light of Article 15 of the e-Commerce Directive, which provides that *"Member states shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity"*. Thus, it presumably would not be appropriate to grant an injunction, on the basis of Article 8, that would require monitoring of users' Internet activity in order to comply with that injunction. The better interpretation may be that an injunction might be granted, in accordance with Article 8 and Article 12(3), provided it referred to specific material which could feasibly be blocked or filtered without requiring ongoing monitoring, whether because it was hosted in a particular location, or because it relied on a particular technology or protocol.

A number of attempts have been made in recent years, by both Member State governments and courts, to reconcile these provisions in a manner which places responsibility on ISPs to take action against copyright infringement by users.

In France, this has taken the form of legislation requiring ISPs, where a user has persisted in using the internet to infringe copyright following two warnings to the contrary, to disconnect that user's internet connection, and further providing for the blacklisting of that user, preventing them obtaining ISP services from third parties during a period of prohibition, of between two months and one year¹². This legislation in its original form was found unconstitutional by the French Conseil Constitutionnel; however, an amended version of the legislation has since been adopted¹³. This provides for similar sanctions, but requires the intervention of a judge before sanctions can be imposed¹⁴.

Similar provisions have been proposed in both the United Kingdom and Spain, while the Belgian courts have gone some way towards mandating a filtering system on the basis of Article 8¹⁵.

In Ireland, a similar result appears to have been reached by non-legislative means. Under the terms of a settlement agreed between eircom, the country's largest broadband ISP, and a consortium of record companies, eircom has agreed to implement a three-strikes policy vis-à-vis its users. Where record companies notify eircom that one of its users is infringing copyright, eircom will first inform the user that they have been detected infringing copyright. If infringing use continues, they will next inform the user that if such use persists their internet connection will be disconnected. In the event of further infringing use, the

¹² <http://www.guardian.co.uk/technology/blog/2009/may/13/france-three-strikes>

¹³ <http://www.eff.org/deeplinks/2009/06/three-strikes-dead-in-france>

¹⁴ <http://www.ip-watch.org/weblog/2009/10/23/french-hadopi-law-now-complete-can-brandish-its-weapons/>

¹⁵ <http://www.eff.org/deeplinks/2009/10/uk-and-three-strikes-what-not-do-election-year>
<http://euobserver.com/9/29041/?rk=1>

connection will be terminated. Record companies have agreed to seek similar agreements with other ISPs¹⁶.

The European Commission and European Parliament have sought to oppose laws which would restrict internet access without a judicial decision. This opposition has recently been reflected in the European Telecommunications Reform package¹⁷. The relevant text as agreed between the Parliament and Council provides as follows:

Measures taken by Member States regarding end-users' access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law.

Any of these measures regarding end-users' access to or use of services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of presumption of innocence and the right to privacy. A prior fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to an effective and timely judicial review shall be guaranteed.

(Art 1(3)a of the new Framework Directive)

Once enacted, this provision will limit the extent to which Member States can rely on three strikes laws. In particular, it will require that such laws be “appropriate, proportionate and necessary in a democratic society”, and that they provide for a fair and impartial tribunal, including a right of judicial review. It is, however, unclear how this provision will affect non-legislative three strike schemes, such as that adopted in the eircom settlement. Such measures are not necessarily “measures taken by Member States”; however, by confirming that the termination of internet access is to be considered in human rights terms, this measure makes such agreements less defensible. Further, it raises the possibility

¹⁶ <http://www.out-law.com/page-9761>

¹⁷ MEMO/09/491 EUROPA – Pres Release ‘Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens’ Brussels 5 November 2009
<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491&format=PDF&aged=0&language=EN&guiLanguage=en>

that where such agreements are implemented, the relevant Member States may be challenged for failing to adequately protect the rights of internet users, even where they are not directly involved in the violation of those rights. Certainly, the legal effectiveness of such agreements cannot be assumed pending further action by the Commission, and potentially by Member State and European courts.

Relevance to IIEA Study of Non-Legislative Measures

A number of points should be considered in assessing the relevance of these measures to the VRC space:

1. As noted above, the primary enforcers of copyright restrictions on the Internet have been copyright owners, in particular music and film companies. As large commercial entities with significant financial interests in the enforcement of copyrights, these have been prepared to commit significant resources to monitoring infringements and pursuing infringers through the courts. They have thus constituted a compliance constituency with the necessary incentive, and prepared to adopt the necessary usage patterns, to monitor illegal use more effectively than has been possible in other areas. Even bearing this in mind, very little progress has been made in limiting the availability of copyright material online.
2. The response of the ISP industry to copyright material has been very different to that in respect of CPC in particular. While ISP lobbies have generally been supportive of attempts to combat CPC (while seeking to limit the costs they are required to incur for this purpose), the debate around copyright material has been characterised by opposition between ISPs and rights holders. This debate has focussed in particular on the extent of ISPs' responsibilities to monitor internet users, block access to particular material, or disconnect users who infringe copyright¹⁸.
3. Public perceptions of online copyright infringement are very different to those in respect of CPC, HS and VRC. There is a widespread toleration amongst members of the public of online copyright infringement. Whereas internet users may report CPC which they encounter, they are far less likely to report copyright material which is illegally shared online. Anecdotal reports suggest that users and administrators of internet fora specifically intended to facilitate the sharing of copyright material have been prepared to self-enforce prohibitions on CPC, and even to report such material to law enforcement authorities where it is posted in such fora.

¹⁸ See e.g. EuroISPA Press Release 'EuroISPA calls for sustainable, effective and proportionate response to online piracy', Brussels, 1 April 2008, http://www.euroispa.org/files/content_online_press_release.pdf

4. Copyright material raises legal concerns in respect of both publishers and recipients. Whereas the legal interest in respect of VRC and HS is primarily (though not exclusively) to tackle the publishers of such material, legal concerns exist in respect of both publishers / uploaders and recipients / downloaders of CPC and copyright material. This may be relevant in considering the most appropriate measures to respond to such material.

Hate Speech

Council of Europe Measures

The Additional Protocol to the Cybercrime Convention 2003

The principal international provision in respect of hate speech is the Council of Europe Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems 2003 (the “**Additional Protocol**”)¹⁹.

The Additional Protocol concerns “*racist and xenophobic material*” which is defined as “*any written material, and image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors*”. (Article 2).

The Additional Protocol requires states party to criminalise “*the distribution or otherwise making available*” of racist and xenophobic material through a computer system, provided that this is done “*intentionally and without right*” (Art 2(1)).

There is an explicit carve-out for states that cannot effectively criminalise such conduct due to established principles in their national legal system concerning freedom of expression (Art 2(3)).

Additional provisions address racist and xenophobic threats (Art 4) and insults (Art 5), and denial or approval of genocide and crimes against humanity (Art 6).

States are further required to criminalise acts of aiding and abetting the foregoing offences (Art 7).

Of 27 EU Member States, only 8 have ratified the Additional Protocol, while a further 12 have signed but not ratified, and as such are not yet bound by its terms. Seven EU states (Bulgaria, the Czech Republic, Ireland, Italy, Slovakia, Spain and the United Kingdom) have not signed the protocol²⁰. This compares with the Cybercrime Convention itself, which has been signed by all EU member states, and ratified by 19²¹.

¹⁹ See Annex 3

²⁰ The following states have ratified the Additional Protocol: Albania, Andorra, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Romania, Serbia, Turkey, Ukraine.

The following have signed but not ratified: Austria, Belgium, Estonia, Finland, Germany, Greece, Iceland, Liechtenstein, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Poland, Portugal, Sweden, Switzerland, Canada, South Africa.

²¹ The following states have ratified the Cybercrime Convention: Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine, United States.

Background and Analysis

The Explanatory Memorandum to the Additional Protocol (the “**Explanatory Memorandum**”) notes that the provisions on HS were not included in the Cybercrime Convention itself because, while it was considered when the convention was being negotiated, it was impossible to achieve consensus on the criminalisation of such material. In particular, some delegations opposed such a provision on freedom of expression grounds (Para. 4).

It is clear from the explanatory memorandum that there is little consensus on the criminalisation of material set out in the Additional Protocol, and that human rights considerations have motivated the adoption of a relatively narrow definition of racist and xenophobic material which “*advocates, promotes or incites hatred, discrimination or violence*” (Para. 10 – 18). This will exclude much material that might in ordinary speech be viewed as racist or xenophobic.

The Explanatory Memorandum also highlights the importance of objectionable conduct being carried out “*without right*” (Para. 24). It is clear that this goes beyond the application of common criminal defences to consider whether a person has a justification for making the speech act complained of; it falls to states party to consider the scope of this provision.

Relevance to IIEA Study of Non-legislative Measures

Two essential points arise from this consideration:

- i. The limited ratifications of the Additional Protocol, together with the discussion in the Explanatory Memorandum, make clear that there is limited consensus at national levels over the definition and scope of criminalisation of HS. This suggests that difficulties are likely to arise in facilitating cross-border action against HS, as different local provisions are likely to exist in different jurisdictions, including different definitions of HS and different views on the appropriate response to it.
- ii. The definition of HS is detailed and nuanced, requiring a consideration of (a) the extent to which the material advocates, promotes or incites hatred, discrimination or violence’ (b) the intent behind the distribution of the relevant material; (c) whether there may be a claim of right in respect of that distribution. Further, because the question of a claim of right will be determined by national provisions, even in states that have ratified and implemented the convention, it is likely to vary between states. These factors make it particularly difficult to

The following have signed but not ratified: Austria, Azerbaijan, Belgium, Czech Republic, Georgia, Greece, Ireland, Liechtenstein, Luxembourg, Malta, Montenegro, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom, Canada, Japan, south Africa.

determine with certainty whether material which may constitute HS should be subject to action, whether legal or otherwise.

iii. As is clear from the Explanatory Memorandum, HS is a field that raises particularly challenging questions around human rights and freedom of expression. This point is discussed further below in the human rights analysis. However, it serves at this point to note that non-judicial organs may be particularly ill-suited to consider the balancing exercises that will inevitably arise in applying HS provisions.

iv. The key offence in the Additional Protocol, distribution or otherwise making available, is clear and broadly drawn; in so far as HS material can be identified, and subject to the comments above relating to intention and claim of right, it should not be difficult to determine whether this offence is being committed,

Other Relevant Measures

The United Nations International Convention on the Elimination of All Forms of Racial Discrimination (“**ICERD**”) contains provisions that may be relevant for our purposes²².

In particular, Article 4 (a) provides that states parties “*shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin*”.

This provision clearly addresses a substantially broader class of material than that covered by the Additional Protocol. However, rather than making it easier to identify objectionable material, this simply increases the complexity of the balancing exercise which will be required in any case where it is sought to apply this provision. Vastly divergent human rights traditions are likely to result in different outcomes to this balancing exercise in different jurisdictions.

While the ICERD has been ratified by all 27 member states, it is not clear how far its provisions have been reflected in national laws or, in so far as they have, how compatible the various national provisions are with one another. The Office of the High Commission for Human rights (which is responsible for overseeing the ICERD) does not produce statistical data on implementation. However, the Committee on the Elimination of Racial Discrimination’s annual reports on the convention are illustrative; in its most recent report, five EU member states are reviewed, of whom one has not fully implemented Art 4(1), one has a current constitutional challenge to its hate speech legislation, and three are criticised for failing to fully enforce the relevant rules²³. Further, given the frequency with

²² See Annex 4

²³ Report of the Committee on the Elimination of Racial Discrimination, Seventy-second session (18 February-7 March 2008), Seventy-third session (28 July-15 August 2008); General Assembly

which UN conventions are ratified but not implemented, it seems unlikely that the ICERD constitutes a strong basis for international cooperation in this area. Stakeholder consultations which will be carried out in the course of the wider IIEA research project may provide a clearer answer on this point.

Official Records, Sixty-third session, Supplement No. 18 (A/63/18). The relevant states are, respectively, Austria, Belgium, German, Italy and Sweden.

Child Pornographic Content

Child pornographic content (“CPC”) has generated most non-legislative initiatives and as such will be the most likely source of measures that may be applied by analogy to the VRC space. It is therefore particularly important to consider the legal regime currently and previously applied to this material.

European Union Measures

Framework Decision 2004/68/JHA

Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography (the “CP Decision”) sets out the current legal regime for CPC at the EU level²⁴.

The CP Decision defines “*child pornography*” as “*pornographic material that visually depicts or represents: (i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or (iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i)*” (Art. 1).

The key offence in the CP Decision is committed when any of the following is done without right: “(a) production of child pornography; (b) distribution, dissemination or transmission of child pornography; (c) supplying or making available child pornography; (d) acquisition or possession of child pornography” (Art 3(1)).

Additional offences of instigating, aiding, abetting and attempting the foregoing are also provided for (Art 4).

There is a specific provision in the CP Decision addressing the jurisdictional confusion which may arise where offences are committed via the Internet; Art. 8(5) provides that “Each Member State shall ensure that its jurisdiction includes situations where an offence under Article 3 and, insofar as it is relevant, under Article 4, is committed by means of a computer system accessed from its territory, whether or not the computer system is on its territory”.

Background and Analysis

A number of points merit mention:

²⁴ See Annex 5

i. The definition of child pornography is both clear and expansive. In particular, by including both images of children and images of real persons appearing to be children and realistic images of non-existent children, it greatly eases the burden of identifying whether material is or is not child pornography. Questions will still arise at the margin, but it is difficult to imagine a clearer definition of an objectionable class of material. The clarity of this definition is likely to greatly facilitate both non-legislative action and cross-border cooperation, as there are less likely to be disagreements about the scope of the prohibition, or over whether particular material is captured by it. In this respect, CPC stands in clear contrast to HS, discussed above, and VRC, discussed further below.

ii. The CPC regime, unlike either the HS or VRC regimes, prohibits the acquisition or possession of the prohibited material. In the case of HS and VRC, the person making or disseminating the objectionable communication is criminalised, while in the case of CPC both disseminator and recipient are criminalised. This is analogous to the liability regime in respect of copyright infringing material. This is likely to affect the attitude of both law enforcement officials (whose interest in removing material and/or prosecuting publishers is balanced by an interest in prosecuting the individual downloading the material); recipients of material (who are less likely to notify authorities as they are themselves committing an offence but who may also be subject to pressure from law enforcement for this reason); and members of the public (who are likely to perceive both the material and the individuals involved differently).

iii. The balancing exercise in respect of CPC is less complicated than that in respect of HS or VRC. As Akdeniz notes, there is no respectable liberal argument in support of CPC, in the way there is for HS and to a lesser extent VRC²⁵. CPC is generally viewed as intrinsically objectionable. This contrasts with HS and VRC, where communications are only criminalised where they relate to particular consequences that are viewed as undesirable. This consideration both makes it easier to evaluate this material in a non-judicial context, and less likely that political or legal authorities will object to this. In this latter respect, it is worth considering the following view expressed by a French government committee considering the operation of Internet hotlines: *"It is essential to know who is managing the [hot]lines and in accordance with what criteria. In this connection, although it is seemingly effective, the British arrangements for handling unlawful messages has provoked a lot of criticism on the grounds that it gives the hotline very wide prerogatives both with regard to classifying the content of the sites and the possibility of cutting access to them. Has an association of access providers this right? Is there not a risk of censorship or of substitution for the court?"*²⁶. The question of who is the appropriate decision-maker, and of the extent to which non-judicial and NGO procedures involve a relevant decision, are central to the evaluation of NLMs.

iv. The policy underlying the prohibition on CPC is, at least in part, quite different to that underlying HS/VRC. In the case of HS/VRC, the objection to the

²⁵ Akdeniz, Yaman (2008) Internet Child Pornography and the Law p. 4

²⁶ Conseil d'Etat 'Internet et les reseaus numeriques' 8 Septemeber 1998, cited in Akdeniz, Yaman (2008) Internet Child Pornography and the Law

relevant communication lies in the effects it is likely to have on those to whom it is addressed. In this case, successfully blocking receipt of the relevant communications will achieve the desired objective. In the case of CPC, the principal concern is the process whereby the CPC is produced, and the protection of children depicted (generally referred to as victims). In order to address this concern, it is necessary to act against the sites that produce and distribute such material. Blocking receipt may go some way towards this goal, in limiting the market for commercially produced CPC and so reducing production, and may also serve certain other goals connected with the effects viewing CPC is assumed to have. However, the problem structure remains fundamentally different.

2009 Proposed Framework Decision amending Framework Decision 2004/68/JHA

The Commission has proposed a revised Framework Decision (COM(2009)135 final) amending the CP Decision (the “**CP Proposal**”).

Relevant changes include a redefinition of child pornography to refer to “(i) any material that visually depicts a child, or any person appearing to be a child, or realistic images of a non-existent child, engaged in real or simulated sexually explicit conduct; or (ii) any depiction for primarily sexual purposes of the sexual organs of a child, or any person appearing to be a child, or of realistic images of a non-existence child”(Art. 1(b)).

This definition has been amended to approximate to the Council of Europe convention against child sexual exploitation and sexual abuse and the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (see below). It maintains the clarity and breadth of the current definition, the importance of which is discussed above.

The offences in respect of child pornography are also slightly extended, covering production, distribution, dissemination, transmission, offering, supply, making available, acquisition possession and knowingly obtaining access to CPC (Art. 4). Again, this maintains the principal features of the offences under the CP Decision discussed above.

One innovation in the CP Proposal is Art. 18, which provides that each Member States “*shall take the necessary measures to enable the competent judicial or police authorities to order or similarly obtain the blocking of access by internet users to internet pages containing or disseminating child pornography, subject to adequate safeguards, in particular to ensure that the blocking is limited to what is necessary, that users are informed of the reason for the blocking and that content providers are informed of the possibility of challenging it*”.

The possibility of blocking access to illegal sites is not new; as discussed above, the provisions of the e-commerce Directive already effectively create such a

regime where ISPs become aware of illegal content. However, it is significant for highlighting the elements that the Commission consider to be desirable in such a system, namely:

- a) the involvement of judicial or police authorities
- b) adequate safeguards
- c) blocking must be limited to what is necessary
- d) users must be informed of the reasons for the blocking
- e) content providers have the option to challenge the blocking, and are informed of that possibility

These points will need to be considered in assessing the appropriateness of self-regulatory approaches involving notice and takedown. Some of these points are considered further below in connection with the human rights analysis.

Other Relevant Provisions

The Council of Europe Convention on the Protection of Children against Sexual Exploitation includes (in Article 20) a definition and prohibition of child pornography in broadly similar terms (albeit slightly less detailed) as the CP Proposal. The Convention also includes quite general provisions (Art. 38) relating to international cooperation for the purpose of prevention, investigation and prosecution of offences and protection of victims.

The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography also includes a similar definition of CPC (Art. 2). The Optional Protocol requires states to criminalize, whether the offences are committed domestically or transnationally or on an individual or organized basis, “*producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography*” (Art 3(1)(c)). The reference to ‘the above purposes’ in this article is unclear as to its meaning. There are broad provisions in respect of international cooperation in the investigation or criminal or extradition proceedings in respect of the offences under the Optional Protocol (Art. 6).

Alternative Approaches – US Model

Specifically in the CPC space, the US provides an alternative approach to ISP obligations in respect of illegal material. ISPs are excluded from liability for such material, even where they have notice of it (Communications Decency Act 1996 s. 230(c)(1)) (Contrast the European e-Commerce Directive, discussed above). However, they have a specific obligation to report child pornography accessed by service subscribers. This is limited to cases where they obtain knowledge of the relevant facts, and is limited to specific named offences rather than covering the full gamut of illegal material (42 USC 13032). Further, there is no requirement for ISPs to actively monitor users or content.

A similar approach is proposed in Council Decision 2000/375/JHA to combat child pornography on the Internet, which requires Member States to “*take the necessary measures to encourage Internet users to inform law enforcement authorities, either directly or indirectly, on suspected distribution of child pornography material on the Internet, if they come across such material*” (Art 1). However, it is worth noting that this measure is limited to ‘encouraging’ Internet users to report illegal material, without imposing an obligation to do so²⁷.

General Observations

The number of relevant measures at the European, Council of Europe and UN level in respect of child pornography highlight the political importance attached to this issue. They also highlight the remarkable degree of at least rhetorical agreement on the definition of, and need to criminalise, the production, distribution and consumption of CPC. The inclusion in the international measures on CPC of provisions requiring international cooperation in prevention, investigation and prosecution are relevant in considering the potential barriers to extending non-legislative measures which exist in this space to other areas; the absence of international measures and in particular the lack of specific provisions relating to the relevant subject matter and providing for international cooperation may reduce the likelihood of successful cross-border cooperation.

²⁷ It is worth noting that Australia is in the process of implementing an alternative approach, legally mandated filtering of illegal content hosted outside the country to prevent it being viewed by users within Australia.

http://www.msnbc.msn.com/id/34429714/ns/technology_and_security/

Violent Radical Content

European Union Measures – Framework Decision 2002/475/JHA and Framework Decision 2008/919/JHA

Council Framework Decision 2002/475/JHA on combating terrorism (the “**First VRC Decision**”) does not specifically address the problem of VRC, either on the Internet or off-line. Rather, its goal is to approximate certain laws relating to terrorist offences more generally.

In so far as the distribution of VRC may have been criminalised under the first VRC decision, this is only be the case where it can be brought within the terms of one of the other offences provided for in that decision. The most relevant provisions are “*directing a terrorist group*” or “*participating 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 would contribute to the criminal activities of the terrorist group*” (Art 2(a) and (b)).

The First VRC Decision also includes provisions in respect of inciting, aiding or abetting any of the offences in the decision, which include a broad range of violent offences (killing, assault, hostage-taking, destruction of public property, weapons and explosives offences) where carried out with a view to intimidating a population, compelling a government or international organisation to act or abstain from some act, or seriously destabilising or destroying the fundamental political, economic or social structures of a country or an international organisation (Art 4 and Art 1(a)).

As will be clear from the foregoing, much VRC is likely to fall within the provisions of the First VRC Decision, including in particular the provisions relating to directing, participating and inciting. However, the complexity of these offences, and the indirect manner in which they cover VRC, mean that it is difficult to say with certainty whether particular material is or is not illegal. The Commission, in its analysis of deficiencies in the First VRC Decision, highlighted the lack of explicit provisions relating to terrorist propaganda, and the existing uncertainty over whether and to what extent such material was prohibited under the First VRC Decision²⁸.

The First VRC Decision explicitly does not alter “*the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union*” (Art 1(2)).

Council Framework Decision 2008/919/JHA amending Framework Decision 2002/475/JHA on combating terrorism (the “**Second VRC Decision**”) addresses

²⁸ Commission Staff Working Document – Accompanying document to the Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism – Impact Assessment (COM(2007) 650 final) (SEC(2007) 1425) Para. 2.1.2

this omission. It introduces three new concepts, “public provocation to commit a terrorist offence”, “recruitment for terrorism” and “training for terrorism”.

Public provocation to commit a terrorist offence means “the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in [Article 1 of the First VRC Decision], where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed”.

Recruitment to terrorism is defined as “soliciting another person to commit one of the offences listed in [Article 1 or 2(2) of the First VRC Decision]”.

Training for terrorism refers to “providing instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the offences listed in [Article 1 of the First VRC Decision], knowing that the skills provided are intended to be used for this purpose”.

Member states are required to criminalise each of these three acts (Art 1 amending Article 3(2) of the First VRC Decision).

The Second VRC Decision includes an explicit proviso for freedom of expression, emphasising the importance of human rights considerations in this area; “The Framework Decision shall not have the effect of requiring Member States to take measures in contradiction of fundamental principles relating to freedom of expression, in particular freedom of the press and the freedom of expression in other media as they result from constitutional traditions or rules governing the rights and responsibilities of, and the procedural guaranteed for, the press or other media where these rules relate to the determination or limitation of liability” (Art 2).

Background and Analysis

As will be evident from the foregoing, the legal situation at the European level in respect of VRC will be very different following the implementation of the Second VRC Decision. The deadline for implementation of the decision is 9 September 2010.

Under the First VRC Decision, it is relatively difficult to determine whether particular VRC is or is not illegal. As is clear from the Commission’s Working Document accompanying the proposal for the Second VRC Decision, whether particular material is prohibited under the First VRC Decision will depend *inter alia* on the particular rules applied in member state legal systems in respect of causation, liability of co-offenders, and liability for attempts²⁹. In the absence of specific provisions targeting VRC, a decision-maker is required to consider

²⁹ Commission Staff Working Document – Accompanying document to the Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism – Impact Assessment (COM(2007) 650 final) (SEC(2007) 1425)

whether and if so to what extent it may be captured by the various other offences provided under the First VRC Decision. This analysis will require both legal expertise and a comprehensive understanding of the particular material and of the surrounding facts. It is unlikely that a hotline agency would be in a position to make this assessment with any confidence, or indeed that it would be viewed as an appropriate agency for doing so. The uncertainties connected with these issues are also likely to inhibit international cooperation between law enforcement authorities, as they are likely to take different views on the permissibility of particular material.

The Second VRC Decision goes some way to address this issue. By creating a number of explicit offences relating to provocation, solicitation and training, it highlights the importance of focussing on communications connected with terrorism. The offences of public provocation to commit a terrorist offence and training for terrorism in particular are well adapted to allow a person viewing material to determine whether or not it constitutes prohibited VRC. The requirement in each offence that communication be with a particular intent does draw a decision-maker's attention to issues that may not be explicit from the material reviewed; however, it is likely that a decision maker (and in the final analysis a court) would be prepared to infer intent from the material itself. The proviso that public provocation to commit a terrorist offence does not require that material directly advocate the commission of an offence is instructive in this regard (e.g. a communication glorifying suicide bombing and condemning the targets of suicide bombers may be assumed to be intended to incite the commission of an offence, even if this is not explicit in this regard and it is impossible to identify or directly examine the intention of the author).

The broad scope and relatively self-contained nature of these offences can be assumed to be likely to facilitate their use for blocking illegal material.

However, difficulties remain in using these offences as a basis for implementing NLMs in respect of VRC. First, the saver for freedom of expression highlights the importance of balancing considerations relating to the fight against terrorism with fundamental human rights considerations. VRC, far more than CPC, and possibly even more than HS, raises questions about the limits of legitimate speech in a democratic society. VRC is, almost by definition, political in nature; and courts at both national and regional (ECtHR) levels, are particularly wary of restricting political speech. This is not to suggest that offences of the kind created by the Second VRC Decision are not compatible with human rights norms; however, where human rights are restricted in light of other considerations, a detailed balancing exercise is required (see more generally the discussion below). A legitimate question might be raised about the appropriateness of a non-judicial body making decisions in this respect. The concerns which have been raised at various stages about non-judicial processes to tackle CPC and intellectual property (most recently in debates around French 'three strikes' laws), seem to apply *a fortiori* to decision-making in respect of this most political of speech.

Second, the political nature of VRC may make it more difficult to effectively cooperate through non-legislative measures with states outside the European

Union, including in particular the United States. Analysis of the US First Amendment treatment of VRC is outside the scope of this report. However, it is understood that US courts have been more wary of restricting political speech, even political speech that advocates violent action, than of restricting other types of speech³⁰. Where third states have adopted a different balance between freedom of speech and other values, this is likely to inhibit cross-border cooperation.

Third, even notwithstanding the human rights considerations, the definition of prohibited material is less clear than that in respect of CPC. This uncertainty is an unavoidable function of the nature of the material under consideration, and of the different policy objectives motivating the targeting of this material; whereas there may be uncertainty of fact as to whether a person represented in a pornographic image is a child or not, or is being presented as a child, once this question is answered the question of legality requires no further analysis. A likely result of this uncertainty is to make it more difficult to implement non-legislative responses to VRC, and to implement smooth cross-border cooperation.

³⁰ In this respect, see the discussion in Davis, Benjamin R., 'Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance' 15 CommLaw Conspectus 119 (2006-2007)

Human Rights Analysis

At a number of points above this paper refers to the need for a human rights analysis of measures, whether legislative or non-legislative, which seek to tackle illegal material on the internet. This note does not set out a comprehensive analysis of this issue. Rather, it sets out the key provisions at the European level in this respect, highlights the manner in which these provisions are applied, and discusses their application to NLMs in particular.

Relevant Provisions

The key instrument in this regard is the European Convention on Human Rights 1950, as amended (the “**Convention**”). The most relevant provisions of the Convention are articles 8 (Privacy) and 10 (Freedom of Expression), but article 6 (Fair Trial) may also be relevant to this issue³¹.

The relevance of Articles 8 and 10 is obvious. The protection of privacy, including private life, home and correspondence, will prima facie cover communications through the Internet. This will not cover all VRC with which this study may be concerned; for example, it seems unlikely that content on a publicly accessible website would be captured by this. However, emails and possibly also posts on message boards where these are addressed to a relatively small group may fall within the definition of private life and correspondence.

The more obvious conflict is with the protection of the right of freedom of expression in article 10. The blocking, removal or criminalisation of material on the Internet is a direct restriction on the right ‘to hold opinions and to receive and impart information’, protected by article 10. This is the case regardless of the type of illegal material under consideration.

Article 6 does not directly address the question of the application of non-legislative measures to combat Internet content. However, its focus on judicial decision-making by an independent and impartial tribunal is echoed elsewhere, most visibly in the CP Proposal and the telecommunications reform program discussed above. Further, it will inform the interpretation of ‘*in accordance with law*’ and ‘*prescribed by law*’ in Articles 8(2) and 10(2); it is therefore worth bearing this provision in mind.

Background and Analysis

Both Articles 8 and 10 have a similar structure: in their first paragraph they set out in broad terms the right to be protected; while in their second paragraph they identify permissible restrictions on the relevant right. Neither right is absolute, and the question of the compatibility of measures with Convention will generally fall to be considered by reference to these permissible exceptions. This will

³¹ See Annex 7

involve considering whether they are proportionate to the legitimate aims pursued, are in accordance with law, and are necessary in democratic society.

This is obviously a somewhat imprecise test. The European Court of Human Rights, in reviewing domestic measures, whether legislative provisions or administrative decisions, applies a doctrine of 'margin of appreciation', deferring to national decision-makers in evaluating the necessity of provisions, and intervening only where they have exceeded this margin of appropriate discretion.

Non-legislative responses to illegal material on the internet raise particular questions about the appropriateness of having these evaluations made by private actors, whether NGOs or industry bodies, rather than by public authorities with a democratic mandate to make these judgements.

The operation of blocking systems without a clear legislative basis also raises questions around whether such systems are in accordance with / prescribed by law. This requirement goes beyond the question of whether a restriction is legally permitted to include the requirement that legal provisions impose a sufficient element of control on the relevant decision-maker so as to avoid arbitrary action; that persons affected by a rule should have access to it; and that laws restricting Convention freedoms should be sufficiently clear to allow citizens to regulate their conduct. In a case where a blocking system is operated not on the basis of legislative provisions but rather relying on broadly drafted provisions in an ISP's terms of service, and where public authorities, whether at a European or national level, are promoting such informal action rather than implementing legally grounded responses, a strong argument might be made that such restrictions are not in accordance with law.

It is unclear how far the fact that ISPs are generally private companies providing services under the terms of contracts obviates these concerns. The Council of Europe have published a set of Human rights guidelines for Internet Service Providers (2008), which consider the human rights aspects of Internet content control in detail³². These seem to suggest that Internet access may now be assumed so essential to communication in a modern democracy that it is appropriate to apply a human rights analysis to restraints on those services³³. These guidelines make clear that, in general, ISPs should only block or remove content after verifying its illegality³⁴. The possibility that Internet access might be viewed as an essential right is also borne out in the European Union telecommunications reform package, discussed above.

Subject to these comments, it should be noted that, in general, the prohibition of VRC is likely to be compatible with the Convention (see, in this respect, the analysis in the Commission Working Document accompanying the proposal for

³² Human rights guidelines for Internet service providers Developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA) (2008)

³³ Par. 1, 2

³⁴ Par. 21

the Second VRC Decision³⁵. The key issue will be considering how far human rights considerations raise additional difficulties for NLMs identified to support that prohibition.

A detailed analysis of the human rights implications of specific NLMs will be required at a later stage in the present study, once the most effective and appropriate NLMs have been preliminarily identified.

³⁵ Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism - Impact Assessment (COM(2007) 650 final) (SEC(2007) 1425) SEC/2007/1424 final; par. 5.1.4

Conclusion and Request for Comments

This paper has outlined the key legal provisions at a European and international level in respect of content regulation on the Internet. It has highlighted measures in four specific areas, namely copyright infringing content, hate speech and racist material, child pornographic content and violent radical content, as well as considering the implications of the general ISP liability regime, and of the European human rights regime.

The goal of this paper is to provide a background for analysis of non-legislative measures, rather than to draw independent conclusions. However, a number of points are worth drawing from the foregoing analysis;

- i) The legal regimes in respect of various classes of illegal and rights infringing content vary widely. As such, it will be necessary in analysing non-legislative measures to consider how differences in the legal context may impact on the effectiveness of those measures. To that end this paper, together with further legal studies of specific issues relating to content regulation, will provide a necessary context to our analysis.
- ii) The clarity with which objectionable material and conduct is defined will be an important factor in determining how effective non-legislative responses can be. In the absence of clear definitions, it may be difficult to act against objectionable material without judicial involvement. The degree of clarity in relevant definitions varies significantly between the classes of illegal content considered.
- iii) International harmonisation is important in facilitating cross-border cooperation in tackling illegal content. In this respect, the degree to which provisions are harmonised, and the level at which that harmonisation has been effected (European Union, Council of Europe, UN Convention etc) varies across the classes of material considered. While the criminalisation of VRC has been mandated at a European level, differences between European and non-European jurisdictions remain, and are likely to impact on the effectiveness of non-legislative responses to this material. The possibility of hosting material outside the European Union, including in the United States, limits the effectiveness of harmonised measures within the EU.
- iv) Human rights considerations must be a necessary part of the debate on content regulation. This is clear both from the human rights analysis above, and from the texts emerging from the European telecommunications reform process. Further, the balancing exercise implicit in any human rights analysis of restraints on freedom of expression will be quite different depending on the type of content

under consideration. This further implies that non-legislative measures that are appropriate in one area may be inappropriate in another.

As indicated at the outset, this paper is a work in progress, feeding into a larger project which will run until late 2010. Our goal in publishing this paper is to invite comments from interested stakeholders, both on this paper and on our project as a whole, and we will be very grateful for any feedback that we receive.

Please direct all comments to caitriona.heinl@iea.com.

Annex 1 – E-Commerce Directive

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Relevant Provisions

Article 12 – "Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13 – "Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 – Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 – No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Annex 2 – Copyright Directive

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

Relevant Provisions

Recitals

(33) The exclusive right of reproduction should be subject to an exception to allow certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made. The acts of reproduction concerned should have no separate economic value on their own. To the extent that they meet these conditions, this exception should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information. A use should be considered lawful where it is authorised by the rightholder or not restricted by law.

(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

Article 5 – Exceptions and limitations

1. Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:

(a) a transmission in a network between third parties by an intermediary,
or

(b) a lawful use

of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.

Article 8 – Sanctions and remedies

1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

Annex 3 – Cybercrime Convention – Additional Protocol

Council of Europe Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems - Strasbourg, 28.I.2003

Relevant Provisions

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as “the Convention”), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1. For the purposes of this Protocol:

"racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2. The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2. A Party may either:

(a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

(b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international

law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2. A Party may either

(a) require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

(b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Annex 4 – Convention on the Elimination of Racial Discrimination

International Convention on the Elimination of All Forms of Racial Discrimination adopted and opened for signature and ratification by General Assembly resolution 2106 (XX) of 21 December 1965

Relevant Provisions

Article 4

States Parties condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention, inter alia:

- (a) Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof;
- (b) Shall declare illegal and prohibit organizations, and also organized and all other propaganda activities, which promote and incite racial discrimination, and shall recognize participation in such organizations or activities as an offence punishable by law;
- (c) Shall not permit public authorities or public institutions, national or local, to promote or incite racial discrimination.

Annex 5 – Framework Decision 2004/68/JHA

Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography

Relevant Provisions

Article 1 – Definitions

For the purposes of this framework Decision:

- (a) "child" shall mean any person below the age of 18 years;
- (b) "child pornography" shall mean pornographic material that visually depicts or represents:
 - (i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or
 - (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or
 - (iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i);
- (c) "computer system" shall mean any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, perform automatic processing of data;
- (d) "legal person" shall mean any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations.

Article 3 – Offences concerning child pornography

1. Each Member State shall take the necessary measures to ensure that the following intentional conduct whether undertaken by means of a computer system or not, when committed without right is punishable:

- (a) production of child pornography;
- (b) distribution, dissemination or transmission of child pornography;
- (c) supplying or making available child pornography;
- (d) acquisition or possession of child pornography.

2. A Member State may exclude from criminal liability conduct relating to child pornography:

(a) referred to in Article 1(b)(ii) where a real person appearing to be a child was in fact 18 years of age or older at the time of the depiction;

(b) referred to in Article 1(b)(i) and (ii) where, in the case of production and possession, images of children having reached the age of sexual consent are produced and possessed with their consent and solely for their own private use. Even where the existence of consent has been established, it shall not be considered valid, if for example superior age, maturity, position, status, experience or the victim's dependency on the perpetrator has been abused in achieving the consent;

(c) referred to in Article 1(b)(iii), where it is established that the pornographic material is produced and possessed by the producer solely for his or her own private use, as far as no pornographic material as referred to in Article 1(b)(i) and (ii) has been used for the purpose of its production, and provided that the act involves no risk for the dissemination of the material.

Article 4 – Instigation, aiding, abetting and attempt

1. Each Member State shall take the necessary measures to ensure that the instigation of, or aiding or abetting in the commission of an offence referred to in Articles 2 and 3 is punishable.

2. Each Member State shall take the necessary measures to ensure that attempts to commit the conduct referred to in Article 2 and Article 3(1)(a) and (b), are punishable.

Article 8 – Jurisdiction and prosecution

1. Each Member State shall take the necessary measures to establish its jurisdiction over the offences referred to in Articles 2, 3 and 4 where:

(a) the offence is committed in whole or in part within its territory;

(b) the offender is one of its nationals; or

(c) the offence is committed for the benefit of a legal person established in the territory of that Member State.

2. A Member State may decide that it will not apply, or that it will apply only in specific cases or circumstances, the jurisdiction rules set out in paragraphs 1(b) and 1(c) where the offence is committed outside its territory.

3. A Member State which, under its laws, does not extradite its own nationals shall take the necessary measures to establish its jurisdiction over and to

prosecute, where appropriate, an offence referred to in Articles 2, 3 and 4 when it is committed by one of its own nationals outside its territory.

4. Member States shall inform the General Secretariat of the Council and the Commission accordingly where they decide to apply paragraph 2, where appropriate with an indication of the specific cases or circumstances in which the decision applies.

5. Each Member State shall ensure that its jurisdiction includes situations where an offence under Article 3 and, insofar as it is relevant, under Article 4, is committed by means of a computer system accessed from its territory, whether or not the computer system is on its territory.

6. Each Member State shall take the necessary measures to enable the prosecution, in accordance with national law, of at least the most serious of the offences referred to in Article 2 after the victim has reached the age of majority.

Annex 5 – Proposed Framework Decision COM(2009)135 Final

Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (Brussels, 25.3.2009, COM(2009)135 final)(SEC(2009) 355)(SEC(2009) 356)

Relevant Provisions

Article 1 – Definitions

For the purposes of this Framework Decision:

- (a) ‘child’ shall mean any person below the age of 18 years;
- (b) ‘child pornography’ shall mean
 - (i) any material that visually depicts a child, or any person appearing to be a child, or realistic images of a non-existent child, engaged in real or simulated sexually explicit conduct; or
 - (ii) any depiction for primarily sexual purposes of the sexual organs of a child, or of any person appearing to be a child, or of realistic images of a non-existent child;
- (c) ‘child prostitution’ shall mean the use of a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment in exchange for the child engaging in sexual activities, regardless of whether this payment, promise or consideration is made to the child or to a third person;
- (d) ‘pornographic performance’ shall mean the exhibition in front of a live audience:
 - (i) of a child engaged in real or simulated sexually explicit conduct; or
 - (ii) of the sexual organs of a child for primarily sexual purposes;
- (e) ‘information system’ shall mean any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, perform automatic processing of data.

Article 4 – Offences concerning child pornography

Each Member State shall take the necessary measures to ensure that the following intentional conduct whether undertaken by means of an information system or not, when committed without right is punishable:

- (a) production of child pornography;
- (b) distribution, dissemination or transmission of child pornography;
- (c) offering, supplying or making available child pornography;
- (d) acquisition or possession of child pornography;
- (e) knowingly obtaining access, by means of an information system, to child pornography.

Article 18 – Blocking access to websites containing child pornography

Each Member State shall take the necessary measures to enable the competent judicial or police authorities to order or similarly obtain the blocking of access by internet users to internet pages containing or disseminating child pornography, subject to adequate safeguards, in particular to ensure that the blocking is limited to what is necessary, that users are informed of the reason for the blocking and that content providers are informed of the possibility of challenging it.

Annex 6 – Framework Decision 2002/475/JHA

Council Framework Decision of 13 June 2002 on combating terrorism

Relevant Provisions

Article 1 – Terrorist offences and fundamental rights and principles

1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:

- seriously intimidating a population, or
- unduly compelling a Government or international organisation to perform or abstain from performing any act, or
- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation,

shall be deemed to be terrorist offences:

- (a) attacks upon a person's life which may cause death;
- (b) attacks upon the physical integrity of a person;
- (c) kidnapping or hostage taking;
- (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
- (e) seizure of aircraft, ships or other means of public or goods transport;
- (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
- (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;
- (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;
- (i) threatening to commit any of the acts listed in (a) to (h).

2. This Framework Decision shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.

Article 2 – Offences relating to a terrorist group

1. For the purposes of this Framework Decision, "terrorist group" shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

2. Each Member State shall take the necessary measures to ensure that the following intentional acts are punishable:

(a) directing a terrorist group;

(b) participating 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.

Article 3 – Offences linked to terrorist activities

Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following acts:

(a) aggravated theft with a view to committing one of the acts listed in Article 1(1);

(b) extortion with a view to the perpetration of one of the acts listed in Article 1(1);

(c) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).

Article 4 – Inciting, aiding or abetting, and attempting

1. Each Member State shall take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.

2. Each Member State shall take the necessary measures to ensure that attempting to commit an offence referred to in Article 1(1) and Article 3, with the exception of possession as provided for in Article 1(1)(f) and the offence referred to in Article 1(1)(i), is made punishable.

Annex 7 – Framework Decision 2008/919/JHA

Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism

Relevant Provisions

Article 1 – Amendments

Framework Decision 2002/475/JHA shall be amended as follows:

1. Article 3 shall be replaced by the following:

"Article 3 – Offences linked to terrorist activities

1. For the purposes of this Framework Decision:

(a) "public provocation to commit a terrorist offence" shall mean the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed;

(b) "recruitment for terrorism" shall mean soliciting another person to commit one of the offences listed in Article 1(1)(a) to (h), or in Article 2(2);

(c) "training for terrorism" shall mean providing instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the offences listed in Article 1(1)(a) to (h), knowing that the skills provided are intended to be used for this purpose.

2. Each Member State shall take the necessary measures to ensure that offences linked to terrorist activities include the following intentional acts:

(a) public provocation to commit a terrorist offence;

(b) recruitment for terrorism;

(c) training for terrorism;

(d) aggravated theft with a view to committing one of the offences listed in Article 1(1);

(e) extortion with a view to the perpetration of one of the offences listed in Article 1(1);

(f) drawing up false administrative documents with a view to committing one of the offences listed in Article 1(1)(a) to (h) and Article 2(2)(b).

3. For an act as set out in paragraph 2 to be punishable, it shall not be necessary that a terrorist offence be actually committed."

2. Article 4 shall be replaced by the following:

"Article 4 – Aiding or abetting, inciting and attempting

1. Each Member State shall take the necessary measures to ensure that aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.

2. Each Member State shall take the necessary measures to ensure that inciting an offence referred to in Article 1(1), Article 2 or Article 3(2)(d) to (f) is made punishable.

3. Each Member State shall take the necessary measures to ensure that attempting to commit an offence referred to in Article 1(1) and Article 3(2)(d) to (f), with the exception of possession as provided for in Article 1(1)(f) and the offence referred to in Article 1(1)(i), is made punishable.

4. Each Member State may decide to take the necessary measures to ensure that attempting to commit an offence referred to in Article 3(2)(b) and (c) is made punishable."

Article 2 – Fundamental principles relating to freedom of expression

This Framework Decision shall not have the effect of requiring Member States to take measures in contradiction of fundamental principles relating to freedom of expression, in particular freedom of the press and the freedom of expression in other media as they result from constitutional traditions or rules governing the rights and responsibilities of, and the procedural guarantees for, the press or other media where these rules relate to the determination or limitation of liability.

Annex 7 – European Convention on Human Rights

Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950

Relevant Provisions

Article 8 - Privacy

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 10 – Freedom of Expression

1. Everyone has the right to freedom of expression. this right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 6 – Fair Trial

In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgement shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

