

Possible effects (alienation, deterrence, intelligence loss) of measures against violent radical content

Tim Stevens¹

Consultant, IIEA Study on Non-Legislative Measures to Prevent the Dissemination of Violent Radical Content on the Internet

April 2010

Brief discussion note

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 Reference.²

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.

¹ The views presented in this draft note are not necessarily the view of the Institute of International & European Affairs.

² http://ec.europa.eu/justice_home/funding/tenders/2009_S041_058796/annex_1_en.pdf

Introduction

This document considers whether non-legislative measures (NLM) would have the same effects on internet users as those which member states set out to achieve. Would NLM, for example, minimise the ability and desire of prospective extremists to find and access violent radical content (VRC), or would they perhaps alienate internet users and motivate them to seek out proscribed materials elsewhere or, in a worst case scenario, to act in more aggressive and possibly violent fashion? Also, what are the likely impacts of non-legislative measures on the ability of security services to generate and gather intelligence from known internet sources such as web forums?

Section I: Impacts on the user base

The proposed non-legislative measures aim in part, via different mechanisms and structures, to deter persons from adopting and enacting types of behaviour deemed inappropriate or illegal by member states. Deterrence is a term normally associated with inter-state economic, diplomatic and military strategy and connotes one mechanism through which states aim to preserve the status quo or, in related fashion, coerce or compel others to change their actions in accordance with national aims. In recent years, increasing consideration has been given to the prospects of formulating deterrence strategies against non-state actors, especially Islamist terrorists such as al-Qaeda. It is recognised that it is not possible or even desirable to simply transfer inter-state deterrence models to terrorism and non-state activity, leading some observers to suggest that deterrence is not possible with respect to non-state and criminal actors. Other commentators are rather more hopeful that elements of deterrence can be brought to bear on a range of contemporary security and crime issues.³ In the context of the current discussion, how do deterrence and coercion theory view attempts to combat violent radical content on the internet?

Deterrence By Punishment: Notice-and-Takedowns and Three-Strikes Policies

'Notice-and-takedown' (NTD) and 'three-strikes' (3S) measures fall into the category of 'deterrence by punishment'. Deterrence by punishment involves threatening an actor with retaliatory actions should he pursue a particular activity, the effects of which are deemed costlier by the opponent than the benefits of the actions being deterred. In the cases of NTD and 3S, the threat of punitive action is aimed at deterring users from embarking on courses of action involving the production, dissemination and consumption of VRC. Both measures also have a coercive element, in that they aim to change actors' behaviours once activities have commenced in this case, the curtailment of the production and dissemination of VRC. The sanction available in NTD regimes is the removal of a given internet asset from the network. With 3S, the sanction is usually something like the throttling of domestic broadband, rendering it effectively useless for the purposes of file-sharing, streaming video, and gaming.

Deterrence By Denial: Content Filtering

By contrast, content filtering is a form of 'deterrence by denial'.⁴ Deterrence by denial is achieved by persuading an opponent that his desired outcomes will be unsuccessful on account of the capabilities possessed by the deterring entity. Content filtering is therefore an attempt to deter content producers from uploading material on the basis that it will not reach its desired audiences. It has a secondary deterrent effect in dissuading people from even looking for certain types of content on the basis that it will not be found. It does not have a coercive element because users cannot be forced to consciously change their behaviours to align with state aims the only change in behaviour that can be achieved is either a default one by restriction of access, or a detrimental one in that users elect to actively seek out this content by other means.

When Deterrence Breaks Down

At some point, deterrence and coercion regimes break down. That is, they cease to preserve

³ e.g. Wyn Q. Bowen (2004), 'Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism', *Contemporary Security Policy*, Vol.25, No.1, pp.54-70.

the status quo, or fail to change people's activity in line with national aims. The classic case of deterrence failure is that of the law. Legal prosecution with the prospect of conviction is generally considered a form of 'deterrence by punishment', in which custodial and other tariffs serve to dissuade would-be offenders from pursuing particular courses of criminal action. Given the global prevalence of judicial and penal systems, legal regimes clearly do not constitute perfect deterrents but they are generally considered worth pursuing for the many benefits the rule of law imparts to states and citizens alike. A similar approach is evident in states' willingness to experiment with non-legislative measures that lead to 'punishment' or 'denial' of various sorts, even if not backed by the full force of the legal and judicial systems. In the context of counterterrorism more broadly, we should perhaps take the view that deterrence 'often does not work' against non-state actors,⁵ but this is not *a priori* a reason to not pursue deterrence policies. The following sections examine what might happen when the deterrent and coercive aims of non-legislative measures are not met, first by looking at their effects on internet users, second by exploring their effects on intelligence agencies.

Non-Legislative Measures: Effects on Users

One of the most common forms of NLM is content filtering, which encompasses a wide range of technical measures implemented at network level, or on users' home computers in the case of parental control software.⁶ There are many barriers to the successful deployment of filtering, including accuracy, cost, stakeholder buy-in, ease of circumvention, and reverse-engineering of content blacklists.⁷ This has not prevented states from adopting or looking to adopt national-level filtering programs as means to control access to a wide range of content types, which generally fall into five main categories of political, pornographic, child sexual abuse, terrorist, and religious material.⁸ In 2010, Reporters Without Borders published a report in which they claimed that in 2009, 60 countries were actively censoring the internet, twice as many as in 2008.⁹ Such initiatives are not restricted to what Europeans would consider repressive regimes either. The Reporters Without Borders document lists Australia and South Korea as countries whose internet policies give cause for concern.¹⁰ Australia's controversial internet filtering scheme to restrict access to a wide range of 'refused classification' content has attracted substantial domestic opposition, as well as questions from the US State Department.¹¹ If filtering schemes were totally ineffective they would not attract such concern but they are likely outside of a very narrow range of content, e.g. child sexual abuse imagery, Holocaust denial material to cause more political problems than they solve. It is for these reasons that a 2009 King's College London study concluded that such 'negative measures' were generally 'crude, expensive and counterproductive'.¹²

⁵ Tore Bjørgo (2005), 'Conclusions', in Tore Bjørgo, ed., *Root Causes of Terrorism: Myths, Reality and Ways Forward* (London and New York: Routledge), pp.256-264.

⁶ See Johnny Ryan, Caitriona Heintz, Adrian Bannon, Oisín Suttle, Gilbert Ramsay, Tim Stevens, "RFC2 Initial (basic) overview of measures against illegal content on the Internet in all 27 EU Member States", 22 December 2009 (URL: <http://www.iiea.com/blogosphere/rfc2>).

⁷ Johnny Ryan (2007), *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web* (Dublin: Institute of International and European Affairs), pp 95-103.

⁸ Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, eds. (2008), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: The MIT Press)

⁹ Reporters Without Borders (2010), *Enemies of the Internet: Countries Under Surveillance* (Paris: Reporters Without Borders); available at http://www.rsf.org/IMG/pdf/Internet_enemies.pdf, accessed 6 April 2010.

¹⁰ See also <http://www.rsf.org/en-surveillance36674-Australia.html> and http://www.rsf.org/en-surveillance36667-South_Korea.html, accessed 7 April 2010.

¹¹ Associated Press, 'US Concerned by Australian Internet Filter Plan', 28 March 2010.

¹² Tim Stevens and Peter R. Neumann (2009), *Countering Online Radicalisation: A Strategy for Action* (London: International Centre for the Study of Radicalisation and Political Violence), p.49.

It is not just filtering that has attracted public and political concern. In the United States, the notice-and-takedown provisions of the Digital Millennium Copyright Act (1998) have been criticised for making it too easy for copyright owners to obtain takedowns in cases where no copyright infringement has occurred, and for stifling innovation and research. The Electronic Frontier Foundation claims that, 'In practice, the DMCA and DRM [Digital Rights Management] have done nothing to stop "Internet piracy." Yet the DMCA has become a serious threat that jeopardizes fair use, impedes competition and innovation, chills free expression and scientific research, and interferes with computer intrusion laws.'¹³ Although this is a disputed opinion, the DMCA has proven to be very problematic in its implementation, of which notice-and-takedown provisions are a major component. In the United Kingdom, there has been substantial public and parliamentary opposition to the Digital Economy Bill (2010), mainly from internet service providers who would be responsible for enforcing many of the quasi-legal provisions allowed by the legislation.¹⁴ These include three-strikes regulations leading to the suspension of consumers' broadband connections if they are thought to be filesharing illegally, and the blocking of copyright-infringing websites.¹⁵ A number of other countries, including New Zealand, France, Ireland, Italy and South Korea, have sought to introduce 'three strikes', or 'graduated response', policies for illegal file-sharing.¹⁶

Possible Impact 1: alienation of Muslim citizens

It is an uncontroversial assertion that in the current security environment, non-legislative measures within Europe would inevitably be weighted towards dealing with the presence of Islamist violent content on the internet. Although it is not a reason for non-deployment alone, it is very apparent that Muslim communities in several member-states feel aggrieved by what they perceive as unfair discrimination against Muslims in general, regardless of state attempts to mollify these concerns. For example, a UK parliamentary select committee in 2010 voiced the feeling of many British Muslims when it concluded that the Prevent domestic counterterrorism programme 'stigmatised' and 'alienated' British Muslims.¹⁷ Such findings were compounded by the subsequent release of a study of 'Islamic blogs' by the UK government's Research, Information and Communications Unit (RICU) which was criticised for including amongst its sample *Angry Arab*, the blog of As'ad Abukhalil, a secular California professor.¹⁸ This created the perception that non-Islamists were being treated as 'radical Islamic', which Abukhalil clearly is not.¹⁹ This is an iteration of the classic 'say-do' problem encountered so often in counterterrorism policy.²⁰ Reactions by Muslims in several European countries to the 'Danish cartoon affair' of 2005 frequently incorporated accusations of state

¹³ <http://www.eff.org/issues/dmca>, accessed 6 April 2010.

¹⁴ BBC News, 'Opposition Mounts to UK's Digital Economy Bill', 31 March 2010; available at <http://news.bbc.co.uk/1/hi/technology/8597007.stm>, accessed 7 April 2010.

¹⁵ BBC News, 'Anger About Digital "Stitch-Up"', 7 April 2010; available at http://news.bbc.co.uk/1/hi/uk_politics/election_2010/8608478.stm, accessed 8 April 2010.

¹⁶ Following a Swedish court's ruling against filesharing site Pirate Bay, the associated single-issue Pirate Party won 7.1% of the Swedish vote in the European Elections and a seat in the European Parliament. See BBC News, 'Swedish Pirates Capture EU Seat', 8 June 2009; available at <http://news.bbc.co.uk/1/hi/8089102.stm>, accessed 7 April 2010.

¹⁷ House of Commons Communities and Local Government Committee (2010), *Preventing Violent Extremism*, Sixth Report of Session 2009-10, HC65 (London: The Stationery Office)

¹⁸ *Estimating Network Size and Tracking Information Dissemination Amongst Islamic Blogs* (March 2010); available at <http://security.homeoffice.gov.uk/news-publications/publication-search/comms-with-public-and-partners/RICU-research/estimating-network-size2835.pdf>, accessed 6 April 2010.

¹⁹ Jillian C. York (2010), 'UK Study on Islamic Blogs "Flawed"', *Aljazeera.net*, 1 April 2010; available at <http://english.aljazeera.net/focus/2010/03/2010331142233983829.html>, accessed 6 April 2010.

²⁰ Bob de Graaf (2010), 'Redefining "Us" and "Them"', in E.J.A.M. Kessels, ed., *Countering Violent Extremism Narratives* (The Hague: National Coordinator for Counterterrorism), pp.36-45.

propaganda and institutional victimisation of Muslims, in which ‘a handful of humiliating images [became] a focal point for something much bigger than themselves.’²¹ There have been many other events that have strained the ability of states to communicate effectively with European Muslim communities. Some processes, such as the French and Dutch disputes over the public wearing of *hijab*, have deep cultural resonance, of which all parties seem to fall foul.²²

In the modern media environment, such perceptions are very hard to redress once activated and can easily be manipulated within the broader frame of Muslim victimisation that is an integral component of the global jihadist narrative of terrorist groups like al-Qaeda and their affiliates.²³ Measures that may bolster this narrative should be considered very carefully, particularly if their technical efficacy and practical utility is seriously disputed.²⁴ Collateral blocking of legitimate websites, for example, will not help to foster trust in government, and the private companies that will inevitably be charged with implementing filtering schemes (i.e. ISPs, web hosting services) will not wish to be embroiled in such politicised disputes.²⁵ One preliminary study in the United States suggests that government surveillance programs have had a ‘chilling effect’ on Muslim-American internet usage, defined as a situation in which ‘individuals otherwise interested in engaging in a lawful activity are deterred from doing so in light of perceived or actual government regulation of that activity.’²⁶ Although roughly 70% of the survey respondents believed, post-9/11, that the US government monitored their online behaviours, just under 10% actually changed their internet use patterns. However, this number is substantially larger than the number of potential extremists, and the report author reasonably concluded that ‘the net cast by the electronic monitoring is, in other words, over inclusive.’²⁷ Although the proposed NLM are not surveillance measures in the sense of the American example, they do all possess surveillance components, and member states must strive to ensure that the deterrent effects of NLM are limited as much as possible to their intended targets, rather than to the law-abiding public at large.

Possible Impact 2: removal of a venting space

On a different level, it has been argued that web forums, such as might be blocked by content filters or removed by notices against hosting companies, can have ‘a cathartic function, allowing audiences to vent their anger and frustration without resorting to violent means, similar to the role played by Al-Jazeera with Middle-Eastern audiences’.²⁸ Researchers at Royal Holloway University of London have documented the effects of the late 2008 jihadist

²¹ Tariq Modood (2006), ‘The Liberal Dilemma: Integration or Vilification?’, *International Migration*, Vol.44, No.5, pp.4-7.

²² Wasif Shadid and Pieter S. van Koningsveld (2005), ‘Muslim Dress in Europe: Debates on the Headscarf’, *Journal of Islamic Studies*, Vol.16, No.1, pp.35-61.

²³ See Alex P. Schmid (2010), ‘The Importance of Countering Al-Qaeda’s “Single Narrative”’, in E.J.A.M. Kessels, ed., *Countering Violent Extremism Narratives* (The Hague: National Coordinator for Counterterrorism), pp.46-57.

²⁴ Tim Stevens (2010), ‘New Media and Counter-Narrative Strategies’, in E.J.A.M. Kessels, ed., *Countering Violent Extremism Narratives* (The Hague: National Coordinator for Counterterrorism), pp.112-122.

²⁵ Richard Clayton (2000), ‘Judge and Jury? How “Notice and Take Down” Gives ISPs an Unwanted Role in Applying the Law to the Internet’, University of Cambridge research white paper, 26 July 2000; available at http://www.cl.cam.ac.uk/~rnc1/Judge_and_Jury.html, accessed 6 April 2010.

²⁶ Dawinder S. Sidhu (2007), ‘The Chilling Effect of Government Surveillance Programs on the Use of the Internet By Muslim-Americans’, *University of Maryland Law Journal of Race, Religion, Gender and Class*, Vol.7, No.2, pp.375-393.

²⁷ Ibid.

²⁸ Akil N. Awan (2007), ‘Virtual Jihadist Media: Function, Legitimacy and Radicalizing Efficacy’, *European Journal of Cultural Studies*, Vol.10, No.3, pp.389-408.

forum closures on the users of those forums and while it is not possible to extrapolate too much, the following statement is indicative of the feelings of some when online fora are removed:

For example, a posting on Shumookh Al-Islam ... lamented, 'with the closure of all our sites, you [the Crusaders and their agents] have left us with no choice but to physically join the caravan of jihad. With no jihadi sites through which we can support our brother Mujahideen, there is no point for us to stay behind. We shall join them.'²⁹

These sites are not usually removed from the internet as they are often 'mirrored' elsewhere but the disruption caused to users can be substantial and there will always be pushback from those who feel victimized by restricting access to them. This argument holds true for every type of content, online or offline, which someone will always interpret as censorship. Perhaps mindful of these arguments, there have been moves by member-states towards the facilitation, rather than the removal, of 'safe online spaces' for interaction between mainly young Muslims, such as the UK's Radical Middle Way internet platform.³⁰ This is partly a function of a genuine desire to foster 'moderate' debate but can also be read as an attempt to create visible bulwarks against 'extremist' content.

Possible Impact 3: failure to deter from seeking proscribed content

Filtering as a form of deterrence by denial works in theory by preventing access to VRC, and by making it pointless to disseminate this material as no-one will be able to access it. It is therefore aimed at both production and consumption, although the contemporary internet environment is uniquely characterised by users that are both producers and consumers of content. Some users will be deterred because material becomes more difficult to find; others will abide by the behavioural norms that filtering wishes to encourage as a secondary effect. The general behavioural approach is one that works with some success in repressive media regimes like China, where the intention of internet filtering is not just to prevent access but to engender self-censorship as a form of social engineering.³¹ However, as in China, those who wish to find this material by circumventing filtering mechanisms or resisting governmental normative projects will find a way to do so.

Despite the political will and resources that have been channelled into existing filtering regimes in dozens of countries, users with sufficient resolve will always find ways around the systems implemented by states and sub-state entities charged with implementing them. The old adage, 'the net interprets censorship as damage and routes around it', continues to be true if users and their social networks are considered as part of the network.³² Certainly, human intervention is required to circumvent most attempts at censorship like filtering, and there are many freely-available tools and methods for doing so. The simplest form of evasion is to switch network. This action is possible if the filters apply only to a sub-state network like a company intranet: the employee need only switch to a smartphone, for example, to access content not filtered by the employer. In this case, the deterrent in the absence of other behavioural control mechanisms, such as workplace bans on handheld devices has totally failed to act.

²⁹ Akil N. Awan and Mina al-Lami (2009), 'Al-Qa'ida's Virtual Crisis', *RUSI Journal*, Vol.154, No.1, pp.56-64.

³⁰ <http://www.radicalmiddleway.co.uk/>, accessed 6 April 2010.

³¹ Ronald J. Deibert (2002), 'Dark Guests and Great Firewalls: The Internet and Chinese Security Policy', *Journal of Social Issues*, Vol.58, No.1, pp.143-159.

³² John Gilmore, quoted in Philip Elmer-DeWitt, 'First Nation in Cyberspace', *Time*, 6 December 1993.

Tor software ('anonymity online') prevents surveillance systems from undertaking traffic analysis on a user's browsing habits, effectively making the user anonymous.³³ Copies of the many Tor variants have been downloaded hundreds of thousands of times from open source community hubs like SourceForge,³⁴ and activist groups like Global Voices Advocacy provide free guides to, for example, anonymous blogging with Tor and other free tools.³⁵ Other groups publish general 'how to' guides for avoiding 'censorware' of various types, specifically aimed at 'activists and users'³⁶ and acts as platforms for the development of their own open source anti-censorship software solutions.³⁷ Other solutions, such as VPNs (Virtual Private Networks) in combination with data encryption are more complex to set up but can also be purchased quite easily. Mobile VPNs can give secure anonymous access to networks across a range of devices. Instruction manuals are freely available on the web, including in video form on YouTube. Given, for example, that the US has vocally reaffirmed its commitment to Article 19 of the Universal Declaration of Human Rights³⁸ and is beginning to actively encourage the provision of circumvention software in media-repressive regimes,³⁹ it seems likely that content filtering of the type under consideration here will continue to come under significant exogenous as well as endogenous pressures, and will probably only bring short-term tactical gains at best.

The deterrence by punishment measures 3S and NTD work via a more explicit cost-benefit analysis in which the costs of embarking on or continuing a particular course of action outweigh the benefits of doing so. There is less information available on the possible effects of these measures as they have only begun to be deployed very recently. It is possible to say that overtures in these directions have met with stiff opposition from rights groups, legal NGOs, policymakers, and industry, particularly internet service providers. In the specific context of VRC, previous legal measures have not worked to deter or dissuade producers or consumers of this material, and it is likely that similar arguments apply here. We have noted the resolve of users circumventing filtering mechanisms and that too is likely to be a major factor with 3S and NTD. Legal provisions have not proven to be effective deterrent options against the production, dissemination and possession of VRC, even if they have increasingly been used to prosecute individuals. We may therefore wonder at the efficacy of measures located some distance upstream from the prospect of legal censure. Will 3S and NTD deter people from seeking out VRC? Probably not, because as long as the content remains accessible somewhere on the internet, people will seek it out if they so desire and feel entitled to do so on that basis. They may become more adept at using multiple channels, connections, and devices for doing so, but they are unlikely to totally change their usage patterns when the content remains available.

³³ <http://www.torproject.org/>, accessed 7 April 2010.

³⁴ <http://sourceforge.net/>, accessed 7 April 2010. Software enabling anonymous P2P (peer-to-peer) filesharing have been downloaded millions of times from sites like <http://download.cnet.com/windows/>, accessed 8 April 2010.

³⁵ Ethan Zuckerman (2009), *Anonymous Blogging with Wordpress and Tor* (Global Voices Online); available at <http://advocacy.globalvoicesonline.org/wp-content/uploads/anonymous-blogging-updated-Mars09.pdf>, accessed 7 April 2010.

³⁶ e.g. Civisec (2007), *Everyone's Guide to By-Passing Internet Censorship: For Citizens Worldwide* (Toronto: The Citizen Lab); available at <http://www.civisec.org/sites/all/themes/civisec/guides/everyone%27s-guide-english.pdf>, accessed 7 April 2010.

³⁷ <http://psiphon.ca/>.

³⁸ Hillary Clinton (2010), 'Remarks on Internet Freedom', speech, Washington, DC, 21 January 2010.

³⁹ US Department of the Treasury, 'Treasury Department Issues New General License to Boost Internet-Based Communication, Free Flow of Information in Iran, Sudan and Cuba', press release, 8 March 2010; available at <http://www.ustreas.gov/press/releases/tg577.htm>, accessed 6 April 2010.

A study by the University of Rennes may provide some indications of the unanticipated effects of copyright protection legislation on the usage patterns of persons seeking out copyrighted content on the internet.⁴⁰ The researchers found that amongst their French survey population, piracy levels rose rather than fell after the October 2009 introduction of the French 'HADOPI' laws. Users were indeed using peer-to-peer (P2P) services covered by the Hadopi legislation slightly less than before (17.1 to 14.6 per cent) in order to avoid the threat of three-strikes disconnection but switched instead to downloading services not covered by the new laws, or by the use of more complex technologies like virtual private networks (VPN). A quarter of respondents identified as in breach of copyright laws prior to Hadopi said they had changed their practices in these and similar ways since the introduction of the anti-piracy laws. Of those P2P users who downloaded copyrighted material, half also purchase legally downloadable material, suggesting that if the practical Hadopi measures were carried through to their logical conclusion, this would actually decrease the number of people downloading legal material, clearly not the intended consequence of the legislation.⁴¹ The researchers concluded that 'the deterrent effect of the law is for the time being relative', but expected the percentage of users abandoning P2P under Hadopi to further decrease.⁴² This decrease would however be accompanied by an increase in other forms of piracy not covered by Hadopi, as well as a general increase in piracy volume and the number of individuals criminalised under the laws.⁴³ They acknowledge the small scale of the survey (2000 respondents in Bretagne) but suggest that it 'raises some doubts about the effectiveness of web laws to curb digital piracy and promote the legitimate market for music and video on the internet.'⁴⁴ Hadopi as a deterrent may be working in some ways but has unexpected effects elsewhere that may actually be counterproductive.

As 3S and NTD measures do not involve the protection of, for example, copyright by a second party such as a media company, but rather represent attempts to regulate content from a third party, the system has rather less credibility than might be expected. At present, users are uncertain what the proposed punitive regimes are, how they will be implemented, what constitutes reasonable use, what material is illegal, and so on. This failure to communicate with users precludes a positive working relationship between states and citizens. This will be important should states decide to pursue 3S and NTD, as these measures have elicited significant negative reactions from a wide range of stakeholders in the context of copyright and piracy, where there is a demonstrable 'victim'. Where this 'victim' does not exist, as is the case with VRC, victimhood may be adopted by the internet user, accusations of censorship will be rife, and the initiatives would be unlikely to achieve the stakeholder buy-in they require for success. The courts cannot prosecute all offenders and users may decide that civil disobedience is a fruitful and forceful course of action.

Summary

It seems likely therefore that non-legislative measures will face significant difficulties in achieving total success in their stated aims, although they may have some utility if deployed in realistic fashion. They may also have the undesired effect of alienating not only potential extremists but also average internet users away from the intentions of the political

⁴⁰ Sylvain Dejean, Thierry Pénard and Raphaël Suire (2010), *Une Première Évaluation des Effets de la Loi Hadopi sur les Pratiques des Internautes Français* (Rennes: Université de Rennes); available at <http://recherche.telecom-bretagne.eu/marsouin/IMG/pdf/NoteHadopix.pdf>, accessed 12 April 2010.

⁴¹ Ibid, p.8.

⁴² Ibid, p.11.

⁴³ Ibid.

⁴⁴ Ibid, p.13.

mainstream and even, perhaps, into criminality. In this sense, we suggest that the stated deterrent and coercive aims of these policies can only partly be achieved and may create additional problems that may require different forms of legal and non-legal intervention.

Section II: Non-Legislative Measures: Effects on Security Agencies

It has been argued elsewhere that legislations and prosecutions 'may drive e-jihad further into the dark recesses of cyberspace, making observation and analysis more problematic' for government and their security agencies.⁴⁵ We must also ask what might be the effects of non-legislative measures on security agencies, specifically as regards the potential intelligence provided by online extremist activities. The cultivation by the containment of extremists' operating environments serves two main functions: it selectively manages incoming and outgoing links in a network to prevent it from replicating and propagating, whilst also keeping actors where one can see them. In a sense, this is a form of cultivation allowing for the controlled generation of intelligence and is gaining traction amongst security agencies as a preferred method of dealing with extremist networks. This can be achieved either by corralling individuals in pre-existing locations, such as well-known jihadi forums, or by enticing them via 'honeypot' sites to new locations set up specifically to allow monitoring and intelligence gathering. Honeypot sites can be deployed with other methods for attracting users away from genuine extremist sites. Malware can be used in the form of spyware trackers that provide user-specific data that can be fed back into analytical systems to provide further intelligence on usage patterns and network topologies.

As these activities are necessarily covert operations there are few details about them in the public domain. The technical feasibility of honeypots, for example, has been demonstrated in cybercrime mitigation and information security, where they are used to counteract unauthorised access to networked computer systems.⁴⁶ There is little public information about specific security agency actions in this field, although their use has long been theorised as a deception component of information warfare.⁴⁷ What little we know of such operations comes from American military intelligence. In 2006, the US Air Force authorised an operation 'to develop a website to identify and exploit foreign threats to [Department of Defense] equities'.⁴⁸ The project was suspended when it was found to have potentially breached regulations governing warrants for legal intercepts. The tensions between intelligence and other national security priorities are displayed in a story from the American press in early 2010. *The Washington Post* claimed that in 2008, the US Department of Defense shuttered a honeypot site created by the Central Intelligence Agency (CIA) and the Saudi Arabian government to attract and track Islamist extremists in Saudi Arabia.⁴⁹ In the eyes of the Pentagon, the site was a conduit for the exchange of operational information between extremists, and contributed to the influx of 'foreign fighters' into Iraq. It closed the site against the wishes of the CIA, who, in the words of a US counterterrorism official, 'understood that intelligence would be lost, and it was; that relationships with cooperating intelligence services would be damaged, and they were; and that terrorists would migrate to other sites, and they did.'⁵⁰

The forum in question is thought by many experts to have been al-Hesbah, long considered

⁴⁵ Gary Bunt (2009), *iMuslims: Rewiring the House of Islam* (London: Hurst & Company), p.240.

⁴⁶ See The Honeynet Project for resources on honeypots; available at <http://www.honeynet.org/>, accessed 6 April 2010.

⁴⁷ Lance Spitzner (2003), *Honeypots: Tracking Hackers* (Boston, MA: Addison-Wesley), p.34.

⁴⁸ *USAF Quarterly Report to the Intelligence Oversight Board (1 January-31 March 2008)*, p.1; available at http://www.eff.org/files/filenode/intel_oversight/20100202_dod_PT4.pdf, accessed 8 April 2010.

⁴⁹ Ellen Nakashima (2010), 'Pentagon's Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Policies', *The Washington Post*, 19 March 2010.

⁵⁰ *Ibid.*

one of the mainstays of the online jihad.⁵¹ In June and September 2008, three main jihadist forums al-Ikhlaas, al-Firdaws and al-Buraq went offline without warning, causing great consternation amongst the jihadist community, and leaving only al-Hesbah as 'Al-Qa'ida's official web presence.'⁵² Users transferred their activities to al-Hesbah where possible (its membership policies were too strict for some) and a range of smaller forums. Significant energy went into discussing how to respond to the closures, such as a 'Contingency Plan Presented to Maintain Internet Presence if Jihadist Sites are Hacked', which set out how to conduct 'guerrilla warfare' on the internet.⁵³ Some users began an 'Invasion of Facebook' as 'a new jihadi media tool' leveraging the opportunities of the global social networking site to disseminate propaganda.⁵⁴ However, 'Facebook lends itself to jihadist propaganda poorly for several reasons: administrators can easily close or remove controversial groups, intelligence agencies can see easily who accesses these groups and Facebook seems to attract a relatively liberal crowd'; the Facebook 'invasion' was therefore less successful than its proponents hoped.⁵⁵ In November 2008, al-Hesbah and a clutch of smaller forums also went offline, which may or may not be related to the alleged American military actions during this period. The forum closures cannot be definitively ascribed to one party or another, and states, vigilantes, and al-Qaeda itself have all been blamed.⁵⁶

Internet terrorism expert Aaron Weisburd commented on the CIA-Saudi story that 'there is no functional difference between a "real" jihadi forum and a "fake" jihadi forum, assuming the latter is accepted as legitimate by the community of activists.'⁵⁷ This assessment is correct and similar cost-benefit analyses are performed by intelligence and security agencies with respect to 'real' or 'fake' network assets' intelligence potential and security risks. How the proposed non-legislative measures might impact upon the intelligence functions of national security agencies would seem obvious: in the absence of negotiation between industry and government agencies with the power to take down sites, and intelligence services that might be monitoring them, there will be conflicts of interest. Political calculations are likely to result in takedowns, for example, whereas intelligence imperatives would almost always given appropriate technologies and robust oversight mechanisms prefer to see such sites remain online, whoever was responsible for their creation and maintenance.⁵⁸ This calculus applies to NTD and 3S measures but it is unclear how filtering would affect intelligence-gathering

⁵¹ Thomas Hegghammer (2010), 'Spy Forums', *Jihadica*, 19 March 2010; available at <http://www.jihadica.com/spy-forums/>, accessed 7 March 2010.

⁵² Awan and al-Lami, 'Al-Qa'ida's Virtual Crisis', pp.60-61.

⁵³ 'Portrait of Rats, Preparing to Drown', *Internet Haganah*, 10 October 2008; available at <http://internet-haganah.com/harchives/006420.html>, accessed 7 April 2010.

⁵⁴ Awan and al-Lami, 'Al-Qa'ida's Virtual Crisis', p.61.

⁵⁵ Thomas Hegghammer, summarised in Murad Batal al-Shishani (2010), 'Taking al-Qaeda's Jihad to Facebook', *Terrorism Monitor*, Vol.8, No.5, pp.3-4. In 2008, Daniel Kimmage noted that jihadist media was still principally text-based, which had implications for the web platforms utilised, see Daniel Kimmage (2008), *The Al-Qaeda Media Nexus* (Washington, DC: Radio Free Europe/Radio Liberty); available at http://docs.rferl.org/en-US/AQ_Media_Nexus.pdf, accessed 7 April 2010.

⁵⁶ e.g. Ian Black (2008), 'Cyber-Attack Theory as al-Qaida Websites Close', *The Guardian*, 22 October 2008; Steven R. Corman (2008), 'Did the Bad Guys Scuttle Their Own Forums?', *COMOPS Journal*, 18 October 2008, available at <http://comops.org/journal/2008/10/18/did-the-bad-guys-scuttle-their-own-forums/>, accessed 7 April 2008.

⁵⁷ 'Ah, the Pleasure of Waking Up in the Morning to Discover That...', *Internet Haganah*, 19 March 2010; available at <http://internet-haganah.com/harchives/006804.html>, accessed 7 April 2010. See also, 'Top Ten Jihadi Forums 11 April 2010', *Internet Haganah*, 11 April 2010; available at <http://internet-haganah.com/harchives/006821.html>, accessed 11 April 2010.

⁵⁸ UK intelligence agencies have reportedly expressed concerns that elements of the Digital Economy Bill (2010) will affect their abilities to conduct traffic analysis for national security purposes. See the analysis of Professor Richard Clayton (2010), 'What's Worrying the Spooks?', *Light Blue Touchpaper*, 13 March 2010; available at <http://www.lightbluetouchpaper.org/2010/03/13/whats-worrying-the-spooks/>, accessed 7 April 2010.

activities.

Conclusion

There are two principal aims of the proposed non-legislative measures. First, to degrade the ability of internet users to access illegal content. Second, to foster a behavioural regime in which persons no longer upload and publish illegal content on the internet. Both outcomes require that the deterrent and coercive aspects of the NLM act as they are intended. Our assessment suggests the following:

- NLM may deter less-committed individuals from the production, dissemination and access of VRC.
- NLM may coerce less-committed individuals into ceasing the production, dissemination and access of VRC.
- NLM will not deter committed individuals from the production, dissemination and access of VRC.
- NLM will not coerce committed individuals into ceasing the production, dissemination and access of VRC.
- NLM may motivate moderately-committed and committed individuals into finding and exploiting alternative outlets for the production, dissemination and access of VRC.
- NLM may cause significant disquiet amongst the general public, regardless of their attitudes to VRC, but borne of general ethical, moral and legal considerations of the proposed measures.
- NLM may alienate sectors of the internet using public, including those demographic elements that feel unfairly discriminated by them.
- NLM may cause problems with the intelligence functions of national security agencies.

One additional important consideration is the ability of the deterrer (state and proxies) to competently communicate the principles, processes and penalties associated with a given deterrent/coercive policy. In this formulation, we might conclude that the principles are problematic for ethical, legal and political reasons, the processes are imperfect at best, and the penalties may not be deliverable or might appear unduly and indiscriminately punitive.