statewatch

monitoring the state and civil liberties in Europe

Volume 21 no 4

"Tackling new threats upon which the security and prosperity of our free societies increasingly depend" : the EU-US Working Group on Cyber Security and Cyber crime

by Chris Jones

A trans-Atlantic working group has been created to share best practices, exchange information, and look at specific issues such as cyber incident management and child pornography. The group's activities promote increased internet regulation and the development of military capabilities for cyberspace, which invariably come at the expense of individual rights and freedoms.

The last year has seen significant developments in both national and European policies that attempt to address the issue of cyber security and cyber crime. One particularly significant move has been the establishment, following the November 2010 annual EU-US Summit, of a new transatlantic Working Group on Cyber Security and Cyber Crime. The statement announcing the group's formation noted the intention of the EU and US to "address a number of specific priority issues" - cyber incident management, public-private partnerships, awareness-raising, and cyber crime - and "report progress within a year".

While cyber crime covers issues such as fraud, the theft and misuse of personal data, phishing, the illicit distribution and sharing of copyrighted content, and other related issues, cyber security is a broader term. The EU apparently lacks its own definition of cyber security, although the European Organisation for Security ("the leading European organisation for the private security sector providers of technology solutions and services"0 [1]) defines it as:

> *The need to prevent from, prepare for, detect, respond to and recover from any hazard or illicit content in the cyberspace, covering networked infrastructures, including [the] Internet. [2]*

The definition used by the US Department of Homeland Security is a little more thorough:

> *[Cyber security is] the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. [3]*

Policies aimed at ensuring cyber security are therefore aimed not just at the information transmitted via digital networks, but also at the physical infrastructure facilitating that transmission. Network infrastructure such as servers and databanks permit the functioning of, for example, water and electricity supply systems.

The drive towards greater cyber security has led to a profusion of institutions, bodies, resolutions, statements, action plans, policies and legislation in the last decade or so. A number of EU measures have been geared towards cyber security, with a notable increase in the last year.

While there is undoubtedly a need to prevent malicious activity directed towards networked infrastructure, cyber security policy requires a balance between the powers of the state and the rights of individuals. Policies ostensibly aimed at 'securing' cyber space can have detrimental effects on individual rights, at the same time as opening new areas in which the state and other actors can exercise coercive power. This is illustrated most vividly by the ongoing debates surrounding intellectual property enforcement (for example, with the UK's Digital Economy Act), by which internet service providers would be obliged to adopt a police function in determining whether websites and internet users have broken the law.

Following an outline of the ideas, structure and working method of the EU-US Working Group (hereafter the WG), the four "priority issues" will be examined in the context of a "Concept Paper" (CP) that was issued in April 2011 for the Transatlantic Cyber Security Research Workshop held at the Hungarian Embassy in the United States. [4] This will be used to illustrate some of the potential issues that arise when states invoke the need for greater cyber security, and, more specifically,

Support for ACTA wanes following mass protests see page 5

State Trojans: Germany exports "spyware with badge" see page 8

Statewatch, PO Box 1516, London N16 0EW, UK

Tel: (00 44) 020 8802 1882 Fax: (00 44) 020 8880 1727 E-mail: office@statewatch.org Website: http://www.statewatch.org

some of the more problematic approaches taken by the United States, the EU, and the EU's Member States.

Structure and composition of the Working Group

The EU-US Working Group is composed of four 'Expert Sub-Groups' (ESG), in which most activities are conducted. The WG's main role is to "[take] stock of the progress of the ESG. It meets in ad hoc formats to manage activity at a senior level. It may also, "as appropriate, [get] the necessary political steering and guidance on the political level."

The four ESG deal with the "specific priority issues" noted above. Groups 1, 2 and 3 deal with cyber security-related issues (cyber incident management, public-private partnerships, and awareness-raising respectively), and are chaired by the same two individuals: Andrea Servida from the EU Directorate General on the Information Society and Media (DG INFSO) and an unnamed "US counterpart." ESG 4 (cyber crime) is co-chaired by Jakub Boratynski for the EU (head of the Commission's Directorate-General for Home Affairs' 'Fight against organised Crime' unit) and B. Shave for the US.

A number of heavyweight EU and US institutions are represented in the makeup of the ESG. EU representation will come from relevant Directorates-General (such as INFSO and HOME); the European External Action Service (EEAS); the Presidency of the Council; the Counter Terrorism Coordinator; the EU representation office to the US; EU agencies such as European Network and Information Security Agency (ENISA), Europol and Eurojust; and "experts from the EU Member States' competent national authorities". For the US, participants will come from the Department of Homeland Security (DHS); the US Secret Service (USSS); the Immigration and Customs Enforcement (ICE); the Department of Commerce (DoC); the National Telecommunications and Information Administration (NTIA); the National Institute of Standards and Technology (NIST); the Department of State (DoS); the White House and National Security Council (NSC); the Department of Justice (DoJ); and the Federal Bureau of Investigation (FBI). Furthermore, experts "selected on an ad hoc basis" may also be invited to participate.

Guidance to the Working Group itself will come, on the US side, from the Secretary of State; the Attorney General; the Secretary of Homeland Security; and the Special Assistant to the President and Cyber security Coordinator. For the EU, guidance will stem from the European Commission Vice-President for the Digital Agenda; the Commissioner for Home Affairs; the Presidency of the Council; the High Representative of the Union for Foreign Affairs and Security Policy; the office of the President of the European Council; and the office of the President of the European Commission.

Accountability and Activities

Any work undertaken by the Working Group or the Expert Sub Groups is subject to senior authority:

> *All configurations (WG, ESG) get their political guidance and high-level decisions formally approved from their respective political authorities, who shall in parallel maintain their EU-US bilateral contacts as appropriate.*

Given the number of different state agencies from both the EU and US involved in the WG, it seems that there is a keen interest from both parties in the potential benefits of cooperation. It is also alarming (but perhaps not surprising) that there is so little information available on the undertakings of the WG. So far there seem to have been two formal meetings of the group: the first on the 24th and 25th February 2011 on Internet governance; the second on 28th and 29th June 2011 on child pornography.

A number of questions submitted to the European Commission by Marietje Schaake MEP in May 2011 attempted to establish the necessity and aims of the WG. [5] An attempt was also made to ascertain information on the forthcoming EU cyber crime centre, the European information-sharing and alert system and the recently-established Computer Emergency Response Teams (CERTs). Nine separate questions covered topics such as the need for new institutions; means of monitoring data flows; the types of crime to be targeted; information-sharing between the EU and US; commercial relations; fundamental rights and democratic oversight.

The answer from Cecilia Malmström on behalf of the Commission was a paltry three short paragraphs. In response to Ms Schaake's question regarding public information on the WG, Ms Malmström noted that "the Commission does not share the Honourable Member's view that little information about [the WG] can be found", and mentioned three press releases – hardly a useful source of detailed information. The second paragraph merely restated, in briefer form, the official aims of the WG, which can itself be found in the press releases. The third and final paragraph rejected the notion that vested commercial interests have overplayed the threat from cyber crime, and suggested that the WG "is a timely and strategically highly significant response" to assessments from Europol, Interpol, and industry.

Issues identified by the Working Group

According to the Concept Paper, the WG was established in order to "tackle new threats to the global networks upon which the security and prosperity of our free societies increasingly depend". The increasing reliance of everyday life upon digital networks has led to an increasing recognition in recent years of the need to make those networks more secure, with a growing number of states developing their own cyber security strategies. The UK's Cabinet Office notes that society is "now almost completely dependent on cyber space," [6] therefore requiring robust efforts to deal with cyber crime and enhance security. Quite what this will mean in practice will become clearer as states develop and implement policies, although recent and current practice provides some indication.

Perhaps one of the most significant issues relates to the military use of cyber space. It is clear that the cyber security policies developed by states are far from being simply 'defensive'. The Pentagon has stated that "it is boosting efforts to build offensive cyber arms for possible keyboard-launched US military attacks", [7] with subsequent statements announcing that the "US military is now legally in the clear to launch offensive operations in cyberspace". [8] Such a statement may raise questions about the legality of previous computer network attacks by the US, as during the invasion of Iraq. [9] The UK is also working on the development of "an offensive capability to deal with cyber threats". [10] These developments cannot be considered just obvious extensions of traditional military practice. The increasing propensity of state and non-state actors to utilise digital networks in offensive military strategy blurs "traditional binaries of war and peace, the local and the global, the civil sphere and the military sphere, the inside and the outside of nation-states." [11]

As of yet, there is no indication that the EU and the US are cooperating on the development of offensive strategies. At least publicly, joint action geared towards dealing with cyber-attacks on critical infrastructure has been resolutely defensive. Nevertheless, the establishment of the WG certainly provides a forum in which such issues can be discussed.

Cyber Incident Management

The first of the four issues concerning the WG is Cyber Incident Management. The scope of activities to be organised under this heading includes the development of "broad scenarios", the sharing of "good practices for promoting the resilience and stability of networks", and the exchange of good practice on

"how to work and cooperate across sectors; engage with other countries; exchange information between Governments". The expected outcomes include a series of joint workshops in anticipation of joint cyber exercises, and an "alignment plan for developing country capacity-building on cyber security incident management". Expert Sub-Group 1 deals with these issues, and it is here that the more militaristic element of cyber security has been expressed. This is demonstrated by the first joint exercise undertaken by the two parties: "Cyber Atlantic 2011".

With the CP outlining the need for "a joint cyber exercise in the timeframe 2012-2013", Cyber Atlantic arrived somewhat ahead of schedule in November 2011. It was clearly an extensive project, with "security experts" from the US, the EU, and more than 20 EU Member States given the job of dealing with:

> *Simulated crises affecting national security. In the first scenario, a targeted attack burrowed into the network of an EU country and stole sensitive data there. In the second, an industrial control system used to manage machinery in a power plant was attacked, in an attempt to disrupt its operations. [12]*

The emphasis here is clearly on defensive capabilities. However, it would not be presumptuous to assume that offensive capabilities have at least been considered by the WG. As noted above, both the US and UK have recently publicly announced offensive cyber-warfare programmes. Germany too has "declared war on hackers" with a new Cyber Defence Centre, the job of which is to "spot and evaluate attacks, and to develop counter strategies". [13] The US Congressional Research Service as far back as 2001 listed the UK, France, Germany, Russia and China as states that are "incorporating cyberwarfare as a new part of their military doctrine". [14] One writer asserts that there are "more than 100 nation states that have set up military and intelligence cyberwarfare units". [15]

Whether the EU will be able to muscle in on Member States' cyber-warfare policies is questionable – most Member States remain strongly nationalistic when it comes to defence issues. A number of EU Member States – including the Czech Republic, France, Germany, the Netherlands and the UK – have, in the last year, launched their own national cyber security strategies. The EU has yet to adopt its own, but it has a number of institutions and policies geared towards, amongst other things, supporting those Member States that wish to develop their own policies and initiatives on cyber security.

The 'Trio' (the current Polish and future Danish and Cypriot Presidencies of the Council) have also made cyber security a priority, in light of "cyber attacks against the Commission and the EEAS in March 2011". A document from July 2011 states that the Trio will "explore possibilities to develop global and regional responses to the threats linked to cyber crime and to develop strategies on cyber security". [16] Any such work is likely to build on a Communication issued by the Commission in March 2011 on "Critical Information Infrastructure Protection – 'Achievements and next steps: towards global-security'." This document notes that there is a "trend towards using ICT [Information and Communication Technologies] for political, economic and military predominance, including through offensive capabilities." [17]

New institutions at EU level include:

- The Computer Emergency Response Team (CERT, a unit pulling together "existing IT security departments from the Commission, the Parliament and the Council to handle cyber attacks on all EU institutions"); [18]
- The European Network and Information Security Agency (ENISA, "Securing Europe's Information Society"); [19]
- A soon to be established "EU cyber crime centre", with which Europol is apparently keen to be involved. [20]

Related work is undertaken by the European Forum for Member States ("established to foster discussions and exchanges between relevant public authorities regarding good policy practices, with the aim of sharing policy objectives and priorities on the security and resilience of ICT infrastructures" [21]) and the European Public-Private Partnership for Resilience (EP3R), [22] itself established "within the framework of the initiative on Critical Information Infrastructure Protection", abbreviated to CIIP. [23] All three come under the remit of the Directorate-General for the Information Society, DG INFSO. Europol also has its own Cyber crime Task Force.

ENISA is currently the subject of a proposed Regulation of the European Parliament and Council that would "strengthen and modernise" the agency. Without mandating any operational tasks, the Commission has proposed that "ENISA should act as an interface between cyber security experts and public authorities involved in the fight against cyber crime". A "gradual increase" in "financial and human resources" will allow this. [24] The European Data Protection Supervisor has noted a number of problems with the proposed new tasks for ENISA including lack of clarity, legal uncertainty, and potential function creep amongst others. [25] A Parliament vote on the proposed Regulation is currently due in early 2012.

It is not only state and governmental institutions that are concerned with cyber security. The private sector also has enormous commercial interests in the use of digital networks. Any attempt by governments to protect digital networks from perceived "threats" must involve the private sector, as the majority of the infrastructure and equipment permitting the continued operation of such networks is in private hands.

Public Private Partnerships (PPP)

The Concept Paper makes clear that the WG is also expected to enable the development of "compatible approaches" to Public Private Partnerships (PPP), based on:

> *(a) key assets, resources and functions needed to ensure the continuity of electronic communications services;*
>
> *(b) good practises (including baseline requirements, if appropriate) for the security and resilience of vital ICT infrastructures based on risk management;*
>
> *(c) shared coordination and cooperation mechanisms to prevent, mitigate and react to cyber-disruptions and cyber-attacks.*

The mention in point (c) of the need to be able to react is a hint that offensive capabilities have not been side-lined by the WG. However, the section on PPP is broadly devoted to other issues.

It is expected that the group will produce reports on topics of mutual interest "including best practices and models to engage with the private sector"; national programmes for dealing with botnets; good practices on cyber security in the private sector; legislative development; an action plan intended to draw the private sector into "cooperative activities with governments, on selected areas"; and a set of "common principles and guidelines on the resilience and stability of the Internet as well as reliable access to it".

The questions submitted by Ms Schaake to the European Commission (noted earlier) on the issue of the WG asserted that the risks posed by cyber security and cyber crime required more analysis before the establishment of legislation and policy – "it is necessary to know facts and figures instead of basing policy on perceived risks" that have been asserted by "business interests." This may well be true. Nevertheless, "the cyber security market is witnessing an unprecedented growth in the next decade". [26] Many businesses will therefore likely be pleased with the WG's statement that:

> *While PPP represents a specific priority area, it also cuts across all other priority areas, and thus may be included in work in those areas as well.*

The UK's Cabinet Office commissioned a study on the cost of cyber crime to the UK economy, which was estimated by the study's authors to be in the realm of £27 billion. This figure has been dismissed as "meaningless" by Tyler Moore of the University of Cambridge, due to failings in its methodology and calculations. [27]

There is no indication that the WG has so far encouraged the formation of any particular public private partnership, although according to the CP, an analysis of good practice, initiatives, and models for national PPPs should have been completed in summer 2011.

Awareness-raising and cyber crime

As regards awareness-raising, the Working Group will seek to share best practice and exchange information:

> *In particular on how best to involve [ISPs] and technology providers in the delivery of messages to users about online behaviour and in the development of awareness raising materials.*

The first major crime issues for the WG is child pornography, for which a roadmap will be developed seeking to identify more effective ways to take down websites containing illegal content, as well as investigating effective channels for prosecution. There is also the technologically ambitious goal of examining "technological solutions to detect previously identified CP images from all locations on the internet". By June this had become more specific, with the US proposing to use "photo DNA software made by Microsoft and available for free for detecting and deleting child pornography pictures on internet". The EU was apparently "interested in the proposal." [28]

The Working Group will also develop a programme aimed at "eliminating illegal use of Internet resources, such as IP addresses and DNS (domain names)." Part of this process involves an attempt to have the Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) endorse "law enforcement recommendations", as well as to "collaborate, directly and through the GAC, with ICANN on [a] roadmap for [the] implementation of law enforcement recommendations".

ICANN is a "not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the internet secure, stable and interoperable." Its essential purpose is to ensure that the unique identifying numbers underlying internet addresses are globally coordinated. As the organisation's website goes on to note, it:

> *Doesn't control content on the internet. It cannot stop spam and it doesn't deal with access to the internet. But through its coordination of the internet's naming system, it does have an important impact on the expansion and evolution of the internet. [29]*

In May 2011, a bilateral meeting between the EU and US authorities announced that "reforms [to ICANN] are necessary" in order to:

> *[R]einforce the transparency and accountability of the internal corporate governance of ICANN, to enhance ICANN's responsiveness to governments raising public policy concerns in the GAC and to improve the way decisions affecting country-code Top Level Domains are made. [30]*

The Concept Paper also notes that the EU and US are seeking the implementation by ICANN of law enforcement recommendations, which includes the "implementation by DNS registrars and registries of Top Level Domain names". The specifics of these law enforcement recommendations remain unknown. Similarly cryptic is the statement that there will be coordination to ensure "IP addresses are allocated, assigned and recorded in the most secure and stable manner".

There are two final aspects of awareness raising to be undertaken by the EU-US Working Group. Firstly, attempts will be made to increase the number of states party to the Council of Europe Convention on Cyber crime. In a July 2011 meeting of EU-US JHA Senior Officials, the US "called again for full ratification by the remaining 9 EU Member States of the [convention]." Consideration will also be given to the possibility of taking joint approaches in international forums, such as the expert group on cyber crime of the UN Office on Drugs and Crime. On this issue, the minutes of the July 2011 meeting state that "the EU and the US should work together in the UN to avoid dilution" of the body of international law on cyber crime. [31]

Conclusions

The Concept Paper outlines a substantial base on which cooperation between the EU and US can proceed on the issues of cyber crime and cyber security. One year from the establishment of the Working Group, the EU and US met again for their annual official summit. Despite what the statement goes on to say, it is not necessarily the case that "respect for fundamental freedoms online, and joint efforts to strengthen security, are mutually reinforcing". Moves towards tighter regulation and even outright censorship of the internet and the development of military capabilities for cyberspace may strengthen the security of states and their corporate allies, but they potentially do so at the expense of individual rights and freedoms. If the work of the WG continues in its current, secretive fashion, then greater scrutiny and more pressing questions must accompany it.

Endnotes

1.European Organisation for Security, 'What is EOS?', http://www.eos-eu.com/AboutEOS/WhatisEOS/tabid/55/Default.aspx

2. European Organisation for Security, 'Towards a concerted EU approach to cyber security', September 2010, p.8

3. Department of Homeland Security, National Infrastructure Protection Plan, 2009, p.109, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

4. Transatlantic Cybersecurity Research Workshop at the Hungarian Embassy under the Presidency of the Council of the European Union, 22nd April 2011,

http://www.huembwas.org/News_Events/20110408_cyber_conf/summary_elemei/MD-018a-11-EU%20US%20WG%20-%20Concept%20paper%20-%20CL%20201110413_US.pdf

5. Marietje Schaake, Question for written answer to the Commission (E-004816/2011), 17th May 2011,

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-

004816+0+DOC+XML+V0//EN&language=BG

6. Cabinet Office, 'The cost of cyber crime',

http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

7. Jim Wolf, 'U.S. says will boost its cyber arsenal', Reuters, 7th November 2011, http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107

8. Brid-Aine Parnell, 'US general: 'We're cleared to cyber-bomb enemy hackers', The Reigster, 17th November 2011,

http://www.theregister.co.uk/2011/11/17/us_military_cyberspace/

9. Stephen Graham, 'Cities Under Siege', 2010. London: Verso, p.291

10. Duncan Gardham, 'Britain prepares cyber attacks on rogue states', The Telegraph, 26th November 2011,

http://www.telegraph.co.uk/news/uknews/defence/8916960/Britain-prepares-cyber-attacks-on-rogue-states.html

11. Stephen Graham, 'Cities Under Siege', 2010. London: Verso, p.294

12. Dan Goodin, 'US, Europe throw their very first joint cyber-war party', The Register, 4th November 2011

13. Matthias von Hein, 'Germany declares war on hackers with new cyber defence centre', Deutsche Welle, 1st April 2011 http://www.dw-world.de/dw/article/0,,14960339,00.html

14. Congressional Research Service, 'Cyberwarfare', 19th June 2001, p.2, http://www.fas.org/irp/crs/RL30735.pdf

15. Peter W. Singer & Noah Schachtman, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive', 15th August 2011, Brookings,

http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_schachtman.aspx

16. Note from: Polish, Danish and Cyprus Presidencies to: Delegations, 'JHA External Relations – Trio Programme', 4th July 2011, p.6 (EU doc. no. 12004/11),

http://register.consilium.europa.eu/pdf/en/11/st12/st12004.en11.pdf

17. Commission Communication, 'Critical Information Infrastructure Protection - 'Achievements and next steps: towards global-cyber security'', 31st March 2011, COM(2011) 163 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

18. Valentina Pop, 'EU institutions to create new cyber defence unit', EU Observer, 20th May 2011

19. European Network and Information Security Agency,

http://www.enisa.europa.eu

20. Valentina Pop, 'Europol wants to host EU cyber crime centre', EU Observer, 14th November 2011

21. CIIP – Implementation activities – Pillar 1,

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/pillar_1/index_en.htm

22. European Public-Private Partnership for resilience – EP3R, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm

23. Critical Information Infrastructure Protection,

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

24. Progress Report from: Presidency to: Council, 'Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)', 19th May 2011, p.1-2 (EU doc. no. 10296/11),

http://register.consilium.europa.eu/pdf/en/11/st10/st10296.en11.pdf

25. European Data Protection Supervisor, Opinion on the proposal for a Regulation concerning the European Network and Information Security Agency (ENISA), 1st April 2011, p.2 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:101:0020:0024:EN:PDF

26. Frost & Sullivan, 'Cyber Security – From Luxury to Necessity', February 2011, p.6, http://www.frost.com/prod/servlet/cio/225170443

27. Tyler Moore, 'Why the Cabinet Office's £27bn cyber crime cost estimate is meaningless', Light Blue Touchpaper, 17 February 2011, http://www.lightbluetouchpaper.org/2011/02/17/why-the-cabinet-offices-27bn-cyber-crime-cost-estimate-is-meaningless/

28. General Secretariat of the Council, 'Summary of conclusions of the meeting of the JHA-RELEX Working Party (JAIEX) on 9 September 2011', 14th September 2011 (EU doc. no. 14174/11), p.6, http://register.consilium.europa.eu/pdf/en/11/st14/st14174.en11.pdf

29. Internet Corporation for Assigned Names and Numbers, 'About', http://www.icann.org/en/about/

30. MEMO/11/298, 'Neelie Kroes discusses Internet governance with US Administration', 13th May 2011,

http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/298&format=HTML&aged=0&language=EN&guiLanguage=en

31. General Secretariat of the Council, 'Summary of conclusions of the EU-US JHA Informal Senior Officials Meeting, Cracow, 25-26 July 2011', 29th July 2011, p.3,

http://register.consilium.europa.eu/pdf/en/11/st13/st13228.en11.pdf

Support for ACTA wanes following mass protests

by Max Rowlands

The Agreement will require all signature countries to criminalise copyright infringement and grants private companies an inordinate amount of power to police the internet. A fierce public backlash in Europe has forced the European Commission to refer ACTA to the European Court of Justice

Ratification of the Anti-Counterfeiting Trade Agreement (ACTA) in Europe has been delayed indefinitely following widespread public protest. This highly secretive and undemocratic agreement, which has been much criticised for its damaging implications for individual privacy and freedom of expression over the internet, has now been referred by the European Commission to the European Court of Justice (ECJ) to rule on its compliance with EU law. ACTA is supposedly a trade agreement but it resembles an international treaty: it would substantially alter the criminal law of signatory countries by requiring them to introduce criminal sanctions for copyright infringement. ACTA's vague wording could lead to websites and internet users being unfairly punished. The agreement also places enormous pressure on internet service providers (ISPs) to monitor the downloading habits of their subscribers and to act in tandem with copyright holders (i.e. the entertainment industry) to prevent infringements. ACTA would thus bestow on private companies an inordinate degree of power to police the internet including "expeditious" enforcement procedures that would bypass legal due process. ACTA's critics have argued that the agreement is in breach of EU law, and its loss of political support following large scale public demonstrations across Europe and subsequent referral to the ECJ has been heralded as a major victory. However, the level of corporate lobbying behind the agreement is so strong that campaigning organisations such as European Digital Rights (EDRi) have been quick to warn that ACTA will not be easily defeated.

The drafting of ACTA

The creation of ACTA was first discussed by the US and Japan in mid-2006. Preliminary talks followed in late 2006 and 2007 and now included the European Union (represented by the European Commission, the EU Presidency and delegates from each of its member states), Canada and Switzerland. Formal negotiations began in June 2008 with the number of participating countries widening further to include Australia, New Zealand, Morocco, Mexico, South Korea and Singapore. Following ten further rounds of negotiations, a final version of ACTA open to signature was released by the European Commission on 27 May 2011.

ACTA's drafting process has been widely condemned for its lack of transparency and democratic legitimacy. National parliaments and civil society organisations were excluded and major international organisations working in relevant fields were bypassed, such as the World Trade Organisation, the World Intellectual Property Organisation and the Organisation for Economic Cooperation and Development. US diplomatic cables published by Wikileaks reveal how US negotiators deliberately avoided any form of collaboration with these bodies. [1] Instead ACTA will create its own governing body, the "ACTA committee," to monitor implementation, propose changes to the agreement - with no requirement for public consultation - and admit new countries. The European Parliament and US Senate were denied access to the details of ACTA negotiations and, like domestic law-makers and the general public, were forced to rely

on leaked documents for information. The Electronic Frontier Foundation concludes: "Both in substance and in process, ACTA embodies an outdated top-down, arbitrary approach to government that is out of step with modern notions of participatory democracy." [2]

It is striking that an Agreement intended to have a global impact was devised by only 38 countries. ACTA has been criticised as an example of powerful western countries dictating policy to the rest of the world. A diplomatic cable published by Wikileaks quotes a Japanese official as saying: "the intent of the agreement is to address the IPR [intellectual property rights] problems of third-nations such as China, Russia, and Brazil, not to negotiate the different interests of like-minded countries." [3] Yet none of these countries, nor India, were invited to attend or contribute to negotiations despite being the world's largest emerging economies as well as major sources of pirated merchandise. The digital rights advocacy group La Quadrature du Net believes that the US's priority has always been "to achieve the highest standards in sanctions and ensure that ACTA's scope is as broad as possible." [4] They argue that the inclusion of Mexico and Morocco – developing countries the US has had favourable dealings with in the past – was an attempt to lend legitimacy to the agreement.

ACTA was signed in October 2011 by the US, Japan, Canada, Australia, New Zealand, Morocco, Singapore and South Korea. In Europe, ACTA must be approved both by individual Member States and the EU because it contains criminal sanctions that fall outside the scope of EU law. Having received varying degrees of scrutiny - in the UK the House of Commons EU Committee deemed ACTA to be a "document not raising legal or political questions requiring a report to the House" - 22 EU Member States signed the agreement in Tokyo on 26 January 2012. [5] Only Cyprus, Estonia, Germany, Holland and Slovakia have yet to do so. The Council of the European Union had already adopted ACTA without prior notice or debate in December 2011 at an unrelated Council meeting on agriculture and fisheries. The European Parliament must now vote on whether to "consent" to the agreement and signature countries must ratify it. If ACTA is not approved by the European Parliament and signed and ratified by every member state it will not come into force anywhere in the EU. Domestic parliaments are responsible for ratification which means that ACTA will finally be in the hands of national parliaments and subjected to at least some degree of democratic due process (with the notable exception of the US where ACTA was signed by the President as an "executive agreement" without Senate approval). At this stage ACTA can only be accepted or rejected in its entirety; it is not open to amendment.

ACTA's impact on the digital world

ACTA requires all signature countries to alter their laws and introduce criminal sanctions for copyright infringement. For a supposed trade agreement this is virtually unprecedented, and makes ACTA's secretive and undemocratic origins all the more objectionable. Intellectual property rights are not covered by EU law because the only proposal to have been made was rejected, and ACTA's provisions are more extensive than those EU lawmakers had proposed. Section 4 states:

> *Each party shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright or related rights piracy on a commercial scale. For the purposes of this Section, acts carried out on a* ***commercial scale*** *include at least those carried out as commercial activities for direct or* ***indirect economic or commercial advantage****.[6] (emphasis added)*

This will apply to online activity in addition to counterfeited merchandise (such as fake watches, DVDs etc.). Section 5 stipulates that:

> *Each Party shall ensure that enforcement procedures...are available under its law so as to permit effective action against an act of infringement of intellectual property rights which takes place in the digital environment, including* ***expeditious remedies*** *to prevent infringement and remedies which constitute a deterrent to further infringements.[7] (emphasis added)*

EDRi has condemned the vague wording of these sections, arguing that poorly defined terms such as **commercial scale** and **indirect economic advantage** – with no mention of criminal intent - will result in extremely low thresholds for the imposition of criminal sanctions. "Such unclear wording is simply inappropriate in a key provision, on whose meaning the proportionality and the legality of the Agreement rests." [8] That ACTA's provisions are open to a wide degree of interpretation makes it difficult to predict precisely how they will be implemented by each signatory country.

Criminalising those who take **indirect economic advantage** from copyright infringement is likely to put enormous pressure on ISPs. Section 4 states specifically that each country "shall ensure that criminal liability for aiding and abetting is available under its law." This could include simply providing a copyright infringer with an internet connection, meaning that ISPs could be held accountable for the illegal downloads of their subscribers and thus would be incentivised to police their online behaviour. To this end ACTA stipulates that ISPs must work closely with copyright holders. Section 5 asserts that "each party shall endeavour to promote cooperative efforts within the business community to effectively address trademark and copyright or related rights infringement." Further:

> *A Party may provide, in accordance with its laws and regulations, its competent authorities with the authority to order an online service provider to disclose* ***expeditiously*** *to a right holder information sufficient to identify a subscriber whose account was allegedly used for infringement. (emphasis added)*

Copyright holders will therefore be afforded significant power over ISPs and their subscribers. La Quadrature Du Net denounced ACTA as a "bullying weapon for the entertainment industries" that is "incompatible with democratic imperatives and represents a real threat for fundamental freedoms." [9] Certainly it could have a chilling effect on internet growth and innovation and the free dissemination of information online. ACTA states that each country's enforcement procedures must cover "the unlawful use of means of widespread distribution for infringing purposes" which La Quadrature Du Net believes could lead to the indirect criminalisation of blogging platforms, free software and peer to peer networks. Further, new criminal sanctions for "aiding and abetting" copyright infringement mean that websites could face punitive measures should they link to or publicise another website that is unlawfully sharing copyrighted content. Simply hosting a copyrighted image without permission – with no intent to sell or redistribute it – could now be penalised for gaining **indirect economic advantage**. This will greatly affect websites that rely on user generated content because they could be held legally responsible for the subject matter of uploads made by their users. These sites may have little choice but to conduct pre-emptive censorship of user contributions, stifling creativity and freedom of expression in the process. New internet companies and websites are likely to have a harder time getting up and running; it is difficult to envisage how sites like YouTube and Flickr could have prospered had they been created under ACTA.

The prominent role afforded to private companies in policing the internet is also alarming, particularly because ACTA allows for **expeditious** enforcement procedures that are likely to bypass legal due process. The implications of this are deeply worrying

because establishing culpability in cases of online copyright infringement is typically a difficult process. As the European Data Protection Supervisor emphasises:

[ACTA's] monitoring is likely to trigger many cases of false positives. Copyright infringement is not a straight 'yes' or 'no' question. Often Courts have to examine a very significant quantity of technical and legal detail over dozens of pages in order to determine whether there is an infringement.[10]

ACTA fails to acknowledge these complexities and indeed makes little distinction between an internet file sharer and someone selling counterfeit goods. Expeditious punishment could lead to vast numbers of internet users being unfairly targeted and severely punished. Early drafts of ACTA demanded that persistent copyright offenders be disconnected from the internet and though this requirement has since been removed from the text, a private document published by the European Parliament obtained by EDRi indicates that this is the type of sanction that could be meted out. This power already exists in France under the three-strike HADOPI law and will be introduced in the UK if the Digital Economy Act comes into full effect.

Both of these laws, as well as the recently defeated Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) in the US, were lobbied for heavily by the entertainment industry. ACTA is no exception, with the Motion Picture Association of America one of its most vociferous advocates. Moreover, while the public and domestic parliaments of negotiating countries were denied access to the content of discussions, an advisory board of US-based multinational corporations was consulted frequently on draft versions of ACTA. [11] Freedom of information requests also revealed that companies including Google, eBay, Dell, Intel, the Business Software Alliance, Rupert Murdoch's News Corporation, Sony Pictures and Time Warner signed non-disclosure agreements and received copies of the text.

The level of corporate involvement in the drafting process and the subsequent power afforded to copyright holders in ACTA's final draft has led to accusations that the Agreement has been introduced in large part to protect the entertainment industry's outdated business model. ACTA's chapter on civil sanctions even goes so far as to substantiate the much discredited notion that an illegal download equates directly to a lost sale. Copyright holders have long used this flawed logic to estimate huge revenue losses and argue for harder sanctions against online copyright infringers. EDRi argues that the prioritisation of "private-sector repressive measures aimed at copyright protection over the fundamental rights to privacy and freedom of communication and association" violates both the European Convention on Human Rights and the EU Charter of Human Rights. Moreover, ACTA itself "is a clear violation of Article 21 of the TEU [Treaty of the European Union] which requires support for democracy and the rule of law in the Union's international relations." [12] An August 2011 report by Douwe Korff, Professor of international law at the London Metropolitan University, and Ian Brown, senior research fellow at the University of Oxford, reached a similar conclusion:

"Overall, ACTA tilts the balance of IPR protection manifestly unfairly towards one group of beneficiaries of the right to property, IP right holders, and unfairly against others. It equally disproportionately interferes with a range of other fundamental rights, and provides or allows for the determination of such rights in procedures that fail to allow for the taking into account of the different, competing interests, but rather, stack all the weight at one end.

This makes the entire Agreement, in our opinion, incompatible with fundamental European human rights instruments and standards." [13]

The backlash in Europe

The day after 22 EU Member States signed ACTA, the European Parliament's lead negotiator on the Agreement, Kader Arif, resigned in protest. He said:

"I want to denounce in the strongest possible manner the entire process that led to the signature of this agreement: no inclusion of civil society organisations, a lack of transparency from the start of the negotiations, repeated postponing of the signature of the text without an explanation being ever given, exclusion of the EU Parliament's demands that were expressed on several occasions in our assembly.

As rapporteur of this text, I have faced never-before-seen manoeuvres from the right wing of this Parliament to impose a rushed calendar before public opinion could be alerted, thus depriving the Parliament of its right to expression and of the tools at its disposal to convey citizens' legitimate demands.

This agreement might have major consequences on citizens' lives, and still, everything is being done to prevent the European Parliament from having its say in this matter. That is why today, as I release this report for which I was in charge, I want to send a strong signal and alert the public opinion about this unacceptable situation. I will not take part in this masquerade." [14]

In Poland, thousands of demonstrators quickly took to the streets to protest against their government's decision to sign the agreement. Government websites were subjected to denial of service attacks and Polish MEPs were sent over 100,000 emails urging them to reject ACTA. Poland's Prime Minister Donald Tusk responded on 3 February by suspending the country's ratification of the agreement pending wider consultation and more careful analysis. Buoyed by this success, protests soon followed across Europe. They were organised chiefly by civil society groups who, having been marginalised for so long, seized on the opportunity to have a direct influence on ACTA's ratification. On 11 February, demonstrations were held across four continents and in over 200 European cities. The largest protests were staged in Germany where over 100,000 people took to the streets. The German government had already backtracked a day earlier and agreed to postpone signing ACTA until the European Parliament had reached a decision on whether to consent to its implementation. Holland, another of the five EU countries yet to sign the agreement, quickly adopted the same position. Bulgaria followed Poland's lead and announced it would not ratify ACTA until Member States had formulated a unified position. The loss of support for the agreement has been dramatic. The Slovenian ambassador to Japan, who signed the agreement on behalf of his government, went so far as to issue a public apology:

I signed ACTA out of civic carelessness, because I did not pay enough attention. Quite simply, I did not clearly connect the agreement I had been instructed to sign with the agreement that, according to my own civic conviction, limits and withholds the freedom of engagement on the largest and most significant network in human history, and thus limits particularly the future of our children.[15]

The President of the European Parliament, Martin Schulz, publically criticised the agreement on German television: "I don't find it good in its current form." He also said that the balance between copyright protection and the individual rights of internet users was "inadequately anchored in this agreement." [16]

On 22 February the European Commission responded to growing pressure and referred the agreement to the European Court of Justice so that it could "assess whether ACTA is incompatible - in any way - with the EU's fundamental rights

and freedoms, such as freedom of expression and information or data protection and the right to property in case[s] of intellectual property." [17] One might ask why this was not done before the European Council and most Member States signed the agreement, but it is a welcome move nonetheless. The European Parliament vote on ACTA was originally intended to be held in June 2012, but given the ECJ typically takes 12 to 24 months to make a ruling it is likely to be pushed back until 2013 or 2014.

The prospect of the European Parliament or a Member State refusing to ratify and thus nullifying ACTA (in the EU at least) is stronger than ever. Member state governments and EU institutions alike were undoubtedly unprepared for the scale of public dissent directed towards the agreement. But while ACTA is floundering, EDRi has been quick to caution against complacency. [18] The now elongated timeframe for ratification could cause ACTA protests to lose momentum and gives lobbyists added time in which to manoeuvre. One strategy lobbyists could pursue would be to encourage the European Parliament to approve ACTA by "conditional consent" on the basis of assurances made by the European Commission of its proper implementation. EDRi also warns that it is by no means certain that the ECJ's judgement will be entirely favourable to those hoping to see ACTA scrapped and could instead be used to legitimise the agreement. The level of corporate lobbying for the agreement has been so intense that it is unlikely to go away quietly.

Endnotes

[1] WikiLeaks website:
http://wikileaks.ch/cable/2006/06/06TOKYO3567.html
[2] Electronic Frontier Foundation, 27.1.12:
https://www.eff.org/deeplinks/2012/01/we-have-every-right-be-furious-about-acta
[3] WikiLeaks website:
http://wikileaks.ch/cable/2006/07/06TOKYO4025.html
[4] La Quadrature du Net, 3.2.11:
http://www.laquadrature.net/en/wikileaks-cables-offer-new-insight-on-the-history-of-acta#footnote2_2w6l9ks
[5] Open Rights Group, 25.11.11:
http://www.openrightsgroup.org/blog/2011/acta:-time-for-a-democracy-catch-up
[6] Anti-Counterfeiting Trade Agreement, p. E-12:
http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf
[7] Ibid, p. E-15
[8] European Digital Rights analysis:
ttp://www.edri.org/files/EDRI_acta_series_2_20120117.pdf
[9] La Quadrature du Net, 9.12.10: http://www.laquadrature.net/en/acta-updated-analysis-of-the-final-version
[10] Opionion of the European Data Protection Supervisor, p. C 147/5: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf
[11] Knowledge Ecology International website, 13.3.09: http://www.keionline.org/blogs/2009/03/13/who-are-cleared-advisors
[12] European Digital Rights analysis:
http://www.edri.org/files/EDRI_acta_series_1_20120116.pdf
[13] Opinion on the compatibility of ACTA with the ECHR and the EU Charter of Fundamental Rights, p.53:
http://groenlinks.nl/files/ACTA%20and%20Fundamental%20Rights.pdf
[14] Open Rights Group, 27.1.12:
http://www.openrightsgroup.org/blog/2012/acta-rapporteur-resigns-over-masquerade
[15] Techdirt website, 2.2.12:
http://www.techdirt.com/articles/20120202/02305917633/full-text-slovenian-ambassadors-apology-signing-acta.shtml
[16] The Register, 13.2.12:
http://www.theregister.co.uk/2012/02/13/european_parliament_president_acta
[17] European Commission press release, 22.2.12:
http://trade.ec.europa.eu/doclib/press/index.cfm?id=778
[18] European Digital Rights, 5.3.12: http://www.edri.org/acta_revival

State Trojans: Germany exports "spyware with a badge"

by Kees Hudig

German police have been using software to surveil people's internet activity beyond what is allowed by the law. There has also been increased cross-border cooperation with the police forces of neighbouring countries, with an informal working group meeting twice a year without the knowledge of parliamentarians.

Since 2005 German police have been remote-spying on individuals and organisations by installing software (malware or Trojans) on their computers. [1] There was no legal base for these activities, and in February 2008 the Federal Constitutional Court (Bundesverfassungsgericht) ruled that the state of North-Rhine Westphalia (Nordrhein-Westfalen) was acting unconstitutionally and that 'remote searches' (online durchsuchung) are only allowed under very strict conditions. [2] Germany has a strong civic movement on the protection of 'digital privacy' and the disclosure has triggered heated public debate on state intelligence and security institutions intercepting private computers and mobile phones.

In October 2011, the computer watchdog Chaos Computer Club (CCC) published research conducted on data sent by people who had found Trojans installed on their computers (see Appendix)**.** According to the CCC, the malware was able to spy in ways that exceeded the limits set out by the Federal Constitutional Court in 2008. "The CCC's analysis showed that the Trojan can log keystrokes, take screenshots, record Skype conversations and even activate webcams or computer microphones to survey private events in a person's home." [3] The malware was also constructed in such a way that it could open a 'backdoor' in the targeted person's computer, allowing it to install software. The CCC said that the software, which was developed by the private company DigiTask based in the regional state of Hessen, was badly designed and "could allow the software to be used by third parties."

Following the CCC's disclosure, the Bavarian state acknowledged the existence of the Trojan and other states soon followed. The Minister of Justice, Sabine Leutheusser-Schnarrenberger (Liberal Party, Freie Demokratische Partei), initiated an investigation. The German news service *Deutsche Welle* reported on the extent of the known use of Trojans. [4]

The interior ministers of the states of Baden-Württemberg, Brandenburg, Schleswig-Holstein and Lower Saxony said that regional police had used the software within the parameters of the law. In Lower Saxony, the software had been in use for two years, according to the public broadcaster *NDR*.

Authorities in Brandenburg told the daily *Berliner Morgenpost* newspaper that they were using the spyware in a

single, on-going investigation. Baden-Württemberg had also used such software to investigate "individual cases," according to *Badische Zeitung*.

The interior ministry in the western state of North Rhine-Westphalia also admitted that police had used the software in two instances, both of which had been approved by a judge. The news agency *dpa* reported that both cases had involved serious drug crimes.

Officials in the southern German state of Bavaria confirmed that their agencies have been using a spyware program since 2009. It remains unclear whether all four states had been using the same software.

The president of the Federal Criminal Police Authority (Bundeskriminalamt), Jörg Ziercke, was quick to state that he had dissuaded the regional states' criminal police units from using the programme. What he did not say, and only became clear after parliamentary questions from the Left party Die Linke, was that it was not only police officers from Baden-Württemberg and Bavaria that had been meeting in an informal working group for DigiTask software users, but also officers from Belgium, the Netherlands and Switzerland. This working group had initially been called the DigiTask User Group and had been active for three years. It was later renamed the Remote Forensic Software User Group. The group met twice a year and parliamentarians were not aware of its existence. [5]

Before parliament was informed of the existence of this international working group, DigiTask had told German media that the software had been sold to other countries. The Dutch liberal party (D66) asked its Minister of Justice whether the software was being used in the Netherlands, but the answer is pending. [6]

Criminal prosecution cases have also disclosed information about these operations. At a court case involving two left-wing activists from Switzerland, who were using a server in Nürnberg to encrypt their communications, it was revealed that Swiss police used hardware and software for a so-called "deep packet inspection", which captures all communications made with the server. The legal file revealed that DigiTask software had been used and that the Swiss and Bavarian police forces, who had been arguing over who would foot the bill, shared the costs. [7] What remains unclear, however, is whether the informal working groups are also being used to coordinate joint international operations.

Informal groups rule

The EU has a long history of using informal rather than formal and transparent working groups to coordinate its police forces. [8] Heise reports that the European Cooperation Group on Undercover activities (ECG) "facilitate[s] cross border exchange of undercover investigators." This relatively informal group has countries participating from both inside and outside the EU. There is also a Cross-Border-Surveillance Working Group (CSW) that meets twice a year and is - according to the German government [9] - focused on "cross border observation and problems connected to that." It aims to "optimise the working results." The methods used for 'remote searches' by Europol are unknown.

One of the communication networks that concerns criminal investigators is Skype, which is more difficult to intercept than regular phones. The Trojan seems to be designed to be able to listen in to people communicating with this Voice over IP-system by capturing their key-logs, or sending a constant stream of images of the computer screen. After parliamentary questions on 19 October 2011, the German deputy interior minister, Ole Schröder, disclosed that some of the police collaboration with Italian forces was specifically around this issue. The Germans were concerned that Skype was giving more information to the Italians than to them (which later appeared to be untrue). Skype hands over information to every government that requests it, but the company checks whether the request is legitimate, following specific public guidelines. [10] For information requests, government institutions have to send a request to the organisation's head office in Luxembourg, and Skype advises the applicant not to send a notice to the phone-user that they are investigating. [11]

The 'Federal Trojan' scandal has had the positive side effect of revealing details about the way police and the secret services operate in the opaque area of 'cyber-espionage.' Sometimes the practice turns out to be very 'analogue,' because installing a Trojan on the computer of a targeted person is difficult. The common method of sending an email with an attachment in the hope the target person opens it, allowing its content to install itself on his or her computer, is increasingly unsuccessful because people are aware of the risk of infecting their computer with malware. The monthly newspaper *AK* writes that some Trojans had been installed by hand on peoples' computers. In one case, this happened when a person passed through customs at Munich airport. In another case, police installed it during a court-ordered house search.

The German news website *Heise.de* [12] reports that the Ministry of Interior acknowledges the existence of more informal working groups involving the German BKA and other countries' police authorities. In November 2007, the President of the European Commission issued a statement to "encourage" the practice of remotely searching computers and in September 2010 the EU Anti-Terrorism Coordinator called for the construction of a "common juridical framework for certain intelligence techniques" and pointed explicitly to remote searches. [13]

Endnotes

1 Geheimdienste spitzeln schon seit Jahren (Secret services spy since years already):http://www.stern.de/digital/online/online-durchsuchungen-geheimdienste-spitzeln-schon-seit-jahren-587865.html?nv=ct_mt

2 Press release Bundesverfassungsgericht

http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.html

3 Deutsche Welle 11/10/11 http://www.dw-world.de/dw/article/0,,15449054,00.html

4 See above

5 Kleine Anfrage der Linken enthüllt: Bundeskriminalamt treibt den Einsatz von Schadprogrammen der Firma DigiTask international voran http://www.jungewelt.de/2011/11-14/047.php

6 Gebruikt Nederlandse overheid ook spyware?

http://www.d66.nl/europa/nieuws/20111011/gebruikt_nederlandse_overheid_ook?ctx=vghpm7u9vdea

7 Matthias Monroy, Landeskriminalamt Bayern schnüffelt mit DigiTask für Schweizer Polizei http://www.heise.de/tp/artikel/35/35712/1.html

8 See, for example, Trevi, Europol and the European state by Tony Bunyan in Statewatching the New Europe, 1993/14

9 http://dipbt.bundestag.de/dip21/btd/17/056/1705677.pdf

10 http://cryptome.org/isp-spy/skype-spy.pdf

11 Matthias Monroy, Internationaler Trojaner-Stammtisch

http://www.heise.de/tp/artikel/35/35805/1.html

12 Internationaler Trojaner-Stammtisch

http://www.heise.de/tp/artikel/35/35805/1.html

13 http://register.consilium.europa.eu/pdf/de/10/st13/st13318-re01.de10.pdf

Background

Lemma Wikipedia on 'Online Durchsuchung in Germany'

http://de.wikipedia.org/wiki/Online-Durchsuchung_%28Deutschland%29

The tricky issue of spyware with a badge: meet 'policeware'

http://arstechnica.com/security/news/2007/07/will-security-firms-avoid-detecting-government-spyware.ars

APPENDIX

The announcement from the Chaos Computer Club

Chaos Computer Club analyses government malware http://www.ccc.de/en/updates/2011/staatstrojaner (08/10/11)

The largest European hacker club, "Chaos Computer Club" (CCC), has reverse engineered and analyzed a "lawful interception" malware program used by German police forces. It has been found in the wild and submitted to the CCC anonymously. The malware can not only siphon away intimate data but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the internet.

Even before the German constitutional court ("Bundesverfassungsgericht") on February 27 2008 forbade the use of malware to manipulate German citizen's PCs, the German government introduced a less conspicuous newspeak variant of the term spy software: "Quellen-TKÜ" (the term means "source wiretapping" or lawful interception at the source). This Quellen-TKÜ can by definition only be used for wiretapping internet telephony. The court also said that this has to be enforced through technical and legal means.

The CCC now published the extracted binary files [0] of the government malware that was used for "Quellen-TKÜ", together with a report about the functionality found and our conclusions about these findings [1]. During this analysis, the CCC wrote its own remote control software for the trojan.

The CCC analysis reveals functionality in the "Bundestrojaner light" (Bundestrojaner meaning "federal trojan" and is the colloquial German term for the original government malware concept) concealed as "Quellen-TKÜ" that go much further than to just observe and intercept internet based telecommunication, and thus violates the terms set by the constitutional court. The trojan can, for example, receive uploads of arbitrary programs from the Internet and execute them remotely. This means, an "upgrade path" from Quellen-TKÜ to the full Bundestrojaner's functionality is built-in right from the start. Activation of the computer's hardware like microphone or camera can be used for room surveillance.

The analysis concludes, that the trojan's developers never even tried to put in technical safeguards to make sure the malware can exclusively be used for wiretapping internet telephony, as set forth by the constitution court. On the contrary, the design included functionality to clandestinely add more components over the network right from the start, making it a bridge-head to further infiltrate the computer.

"This refutes the claim that an effective separation of just wiretapping internet telephony and a full-blown trojan is possible in practice – or even desired," commented a CCC speaker. "Our analysis revealed once again that law enforcement agencies will overstep their authority if not watched carefully. In this case functions clearly intended for breaking the law were implemented in this malware: they were meant for uploading and executing arbitrary code on the targeted system."

The government malware can, unchecked by a judge, load extensions by remote control, to use the trojan for other functions, including but not limited to eavesdropping. This complete control over the infected PC – owing to the poor craftsmanship that went into this trojan – is open not just to the agency that put it there, but to everyone. It could even be used to upload falsified "evidence" against the PC's owner, or to delete files, which puts the whole rationale for this method of investigation into question.

But the trojan's built-in functions are scary enough, even without extending it by new moduls. For the analysis, the CCC wrote its own control terminal software, that can be used to remotely control infected PCs over the internet. With its help it is possible to watch screenshots of the web browser on the infected PC – including private notices, emails or texts in web based cloud services.

The official claim of a strict separation of lawful interception of internet telephony and the digital sphere of privacy has no basis in reality. [NB: The German constitutional court ruled that there is a sphere of privacy that is afforded total protection and can never be breached, no matter for what reason, for example keeping a diary or husband and wife talking in the bedroom. Government officials in Germany argued that it is possible to avoid listening in on this part but still eavesdrop electronically. The constitutional court has created the concept of "Kernbereich privater Lebensgestaltung", core area of private life. The CCC is basically arguing that nowadays a person's laptop is intrinsically part of this core area because people put private notes there and keep a diary on it] The fact that a judge has to sign the warrant does not protect the privacy, because the data are being taken directly from the core area of private life.

The legislator should put an end to the ever growing expansion of computer spying that has been getting out of hand in recent years, and finally come up with an unambiguous definition for the digital privacy sphere and with a way to protect it effectively. Unfortunately, for too long the legislator has been guided by demands for technical surveillance, not by values like freedom or the question of how to protect our values in a digital world. It is now obvious that he is no longer able to oversee the technology, let alone control it.

The analysis also revealed serious security holes that the trojan is tearing into infected systems. The screenshots and audio files it sends out are encrypted in an incompetent way, the commands from the control software to the trojan are even completely unencrypted. Neither the commands to the trojan nor its replies are authenticated or have their integrity protected. Not only can unauthorized third parties assume control of the infected system, but even attackers of mediocre skill level can connect to the authorities, claim to be a specific instance of the trojan, and upload fake data. It is even conceivable that the law enforcement agencies' IT infrastructure could be attacked through this channel. The CCC has not yet performed a penetration test on the server side of the trojan infrastructure.

"We were surprised and shocked by the lack of even elementary security in the code. Any attacker could assume control of a computer infiltrated by the German law enforcement authorities", commented a speaker of the CCC. "The security level this trojan leaves the infected systems in is comparable to it setting all passwords to '1234'".

To avoid revealing the location of the command and control server, all data is redirected through a rented dedicated server in a data center in the USA. The control of this malware is only partially within the borders of its jurisdiction. The instrument could therefore violate the fundamental principle of national sovereignty. Considering the incompetent encryption and the

missing digital signatures on the command channel, this poses an unacceptable and incalculable risk. It also poses the question how a citizen is supposed to get their right of legal redress in the case the wiretapping data get lost outside Germany, or the command channel is misused.

According to our hacker ethics and to avoid tipping off criminals who are being investigated, the CCC has informed the German ministry of the interior. They have had enough time to activate the existing self destruct function of the trojan.

When arguing about the government authorized infiltration of computers and secretly scanning suspects' hard drives, the former minister of the interior Wolfgang Schäuble and Jörg Ziercke, BKA's president (BKA, German federal policy agency), have always claimed that the population should not worry because there would only be "a handful" of cases where the trojan would be used at all. Either almost the complete set of government malware has found their way in brown envelopes to the CCC's mailbox, or the truth has been leapfrogged once again by the reality of eavesdropping and "lawful interception".

The other promises made by the officials also are not basis in reality. In 2008 the CCC was told that all versions of the "Quellen-TKÜ" software would manually be hand-crafted for the specifics of each case. The CCC now has access to several software versions of the trojan, and they all use the same hard-coded cryptographic key and do not look hand-crafted at all.

Another promise has been that the trojan would be subject to exceptionally strict quality control to make sure the rules set forth by the constitutional court would not be violated. In reality this exceptionally strict quality control has neither found that the key is hard coded, nor that the "encryption" is uni-directional only, nor that there is a back door for uploading and executing further malware. The CCC expressed hope that this farce is not representative for exceptionally strict quality control in federal agencies.

The CCC demands: The clandestine infiltration of IT systems by government agencies must stop. At the same time we would like to call on all hackers and people interested in technology to further analyze the malware, so that at least some benefit can be reaped from this embarrassing eavesdropping attempt. Also, we will gladly continue to receive copies of other versions of government malware off your hands. [4]

Links:

[0] Binaries
[1] Analysis of the government malware (German)
http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf
[4] BigBrotherAwards 2009, Category Business: companies selling internet and phone surveillance technology
http://www.bigbrotherawards.de/2009/.com
[5] 0zapftis (at) ccc.de use the PGP key below

The comparative study of forced return monitoring in Europe by Matrix/ICMPD

by Marie Martin

Forced return monitoring mechanisms vary widely throughout the EU and the rights of irregular migrants are not safeguarded consistently. This study was an opportunity to make a strong case for improved practices in all Member States, but its scope and recommendations are very limited from a human rights perspective.

In 2009, the European Commission launched a call for tender for the purpose of a comparative study on forced-return monitoring systems in place in the different EU Member States. In 2008, the Returns Directive, regulating return procedures for third country nationals irregularly staying in the EU, was adopted. It gave Member States two years starting from its entry into force (January 2009) to transpose the directive into their respective national laws, including the obligation to "provide for an effective forced-return monitoring system" (article 8(6)).

The comparative study aimed at providing an audit of current measures to allow for the sharing of best practice and putting in place mechanisms for ensuring an EU-compliant monitoring system of forced returns. The study, which started in June 2010, was completed a year later, (i.e. after the deadline for the directive's transposition in December 2010).

The Returns Directive

In 2004, the European Council agreed at The Hague on harmonising return and removal procedures among EU member states according to EU standards [2] and created the European Return Fund (ERF) to this end. Since then, legal harmonisation has been underway since the adoption of "Directive 2008/115/EC of the European Parliament and of the Council on common standards and procedures in Member States for returning illegally staying third-country nationals" [3], commonly known as the Returns Directive (which the UK is not part of).

The directive is described by the Commission as:

> *clear, transparent and fair common rules concerning return, removal, use of coercive measures, detention and re-entry, which fully take into account the respect for human rights and fundamental freedoms of the persons concerned. The "Return Directive" creates a common understanding amongst Member States of the most important elements of return and limits Member States' discretion to follow different national approaches on each of these issues.[4]*

Return, as understood in the directive, comprises forced as well as voluntary return.

However, the Returns Directive has been subject to much criticism in the past few years, with some human rights organisations calling it the "shameful" or "outrageous directive" arguing that the new legal framework merely legitimated the expulsion of migrants that Member States considered undesirable. They also expressed concern at removal procedures and standards in the directive, which, for many civil society organisations, did not sufficiently safeguard the rights of those who were subject to return. [5]

Part of the European Return Fund (7%) may be used to finance transnational projects or projects of interest to the European Community (rather than projects in single Member States applying for the ERF), and the Commission decided to fund a comparative study on practices and legislation in Member States in relation to forced return monitoring, so that best practice may be shared.

Considering the criticism mentioned above, the ERF study could have been an opportunity to suggest improving the directive, which had been accused of "not go[ing] far enough to ensure that minimum standards of proportionality, fairness and humanity are satisfied".[6] As the Returns Directive aims at limiting "Member States' discretion" in how to return irregular migrants, the study could have been an opportunity for identifying insufficiencies in the scope of these limits and ways to upgrade standards, notably safeguards for the rights of irregular migrants facing return.

The study: main findings

The call for tender was won by a consultancy firm based in London, Matrix Insight, which conducted the study in cooperation with the International Centre for Migration Policy and Development (ICMPD) between June 2010 and June 2011. According to the methodology required by the European Commission, the study should be based on existing literature, on reviewing the legal frameworks, and on information collected through interviews with the authorities of nine EU Member States, with representatives of NGOs working on forced return, research institutes and people subjected to return procedures. Case studies and field data took precedent over academic research because "very little has been written specifically on forced return monitoring".

The study was submitted to the Commission in July 2011 and made public in November 2011. It covers the whole EU (except Ireland) and EEA countries (Iceland, Lichtenstein, Norway and Switzerland – who are members of the Schengen group) with an in-depth analysis of best practice in nine countries: Austria, Belgium, France, Germany, Latvia, Luxembourg, Norway, Poland and Switzerland The inclusion of EEA countries seems fair as they are participating in some aspects of the EU return policy (in particular in Frontex operations). The case studies are presented as helping "gain an insight as to the difficulties which may occur in the process of setting up an effective and transparent monitoring system...and to provide illuminating examples of best practice."

As regards the monitoring of forced return, the study reveals that:

- Based on the country profile sheets, 20 countries had a monitoring system in place (or one is imminent) while four countries were in the legislative process of putting one in place. Six countries therefore do not have any monitoring system so far, including some countries at the EU's external borders where the rate of successful applications is very low and from where irregular migrants are likely to be returned under the Dublin II Regulation (cf. Bulgaria, Greece, Iceland, Italy, Malta, Slovakia and Sweden).

- Forced return monitoring systems generally place more emphasis on the pre-return than on the post-return phase.

- In the majority of cases, civil society organisations, law enforcement bodies and ombudspersons are involved in the monitoring system

- The study reflects the opinion that a real difference exists between monitoring actors (simply monitoring forced return) and interventionist actors (organisations empowered to expose misbehaviour when it happens). It is argued that monitoring organisations are more likely to communicate with the returnees and to report on the situation than "intervention powers" for which a mixed role of monitoring and intervention may be "confusing".

Regarding effectiveness (ensuring that returnees are treated in accordance with human rights standards) and transparency of forced return monitoring systems, the study concludes that:

1. Monitoring organisations/authorities should be "different from the enforcement authorities"

2. "Monitors should be immediately informed of impending return operations" in countries where such mechanisms are in place. This is not the case in Denmark, Lichtenstein, Lithuania and Romania (the country profile states: "to be decided"), or is left to the discretion of the authorities (Ministry of Interior in Estonia; Prosecution Service in Hungary)

3. Sufficient funding is necessary to ensure proper forced return monitoring

4. Cooperation between all stakeholders is desirable

5. Monitoring should cover the whole return process, including pre-departure, return and arrival

6. "Monitors should be able to decide which cases to monitor"

7. Observation duties may be extended, under strict conditions, to other tasks (a review of medical files is suggested)

8. Monitors should endeavour to facilitate cooperation and "constructive work relationships" with enforcement authorities especially when there is a risk of confrontation between them and the returnee

9.Monitoring reports should be taken into account in a systematic manner by the authorities

10. A special recommendation regarding Frontex joint return flights is made: a monitor should be designated by the country hosting the operation (or the country returning the biggest group) and common monitoring reports on all operations should be submitted to Frontex. It is suggested that Frontex reports annually on these monitoring observations to the European Parliament.

Analysis

Some of the points raised in this study give a useful insight into forced return monitoring mechanisms in Europe. Systems vary widely depending on the country, especially regarding the nature of the organisations involved in the monitoring and the tasks they carry out. The independence of monitors and their capacity to act differ from one country to another. The comparative study was an opportunity to point out these differences and make recommendations to improve forced-return monitoring mechanisms. Regrettably, the recommendations are unsatisfactory from a human rights perspective – this problem may well have been due to the lack of detailed data being made available to the study.

Blurred definitions

The scope of the definitions lacks clarity regarding other aspects of the study. The definition of "forced return" is obviously of particular importance in this case. The study presents in detail the different positions adopted by various organisations regarding the criteria adopted to decide whether a return is forced or voluntary. In particular, there is no clarification as to whether the controversial notion of "forced return without compulsion" used by the International Organisation of Migration (IOM) is taken into account in the final definition of voluntary or forced return. Similarly, people issued with a deportation order but given time to leave the country by themselves are defined by the IOM as being "voluntary under compulsion", as being "voluntary" by the European Migration Network, and as "mandatory returns" by the European Council of Refugee and Exiles (ECRE). Here again, no common definition is provided in the study.

It must be assumed that the questionnaires have been filled in by the different stakeholders following different definitions. Differences as to whether a return is forced or voluntary are crucial, not least when evaluating monitoring systems.

Non-comprehensive study

As mentioned above, the study is based much more on field research than on desk review, due to the absence of relevant literature on mechanisms to monitor forced returns. While this may be true, it seems legitimate to expect from field studies that they detail in the most comprehensive way the mechanisms in place in the different countries under survey.

Moreover, the list of stakeholders interviewed for the purpose of the study lacks consistency. The methodology requirement for officials, civil society organisations operating in the field of forced return, and returnees to be contacted, only applies to "case studies". The list provided in Appendix G reflects that in many cases, only officials were interviewed for the country not shortlisted for the case study (i.e. 21 out of 30 countries), giving only a partial picture of the reality.

As a result, the study does not seem comprehensive enough to allow for a real comparison of practices. For example, in a number of cases, no information is given as to when monitors are informed about impending return operations (Cyprus, the Netherlands, Portugal, Slovenia, Spain, Switzerland and the UK).

Monitors different but not independent from authorities

According to the study, monitors should be different from enforcement authorities. Such a principle would help ensure a clear distinction in the tasks of each actor involved in the return process and limit conflicts of interest. Yet, this recommendation does not go far enough to ensure the independence of monitors other than recommending that "safeguards [are] in place which allow the monitor to perform the monitoring tasks in an independent way".

In fact, "financial independence from the State is not necessarily required" (p.19), and "a public body would qualify as monitor" (p.19). While the example given of a public body is that of the national ombudsman, the recommendation may be interpreted as not being limited to such body; for example, in Belgium, it is the General Inspectorate of the General Federal Police and the local Police force (*Inspection générale de la Police fédérale et de la Police locale*) which is in charge of monitoring forced returns (p.24).

Another recommendation made about cooperation between monitoring and enforcement bodies entails a similar risk of collusion, if not conflict of interest in the monitoring process. Sharing feedback with all stakeholders after monitoring so that "lessons learnt are incorporated into practice" may be valuable, but doubts remain as to the lifting of "any barrier to effective and respectful cooperation 'on the ground' between monitors and executing authorities" (p.8).

Based on the study's recommendations, situations where monitors would partly depend on public funding and would therefore be strongly inclined to cooperate with enforcement authorities, i.e. where monitors would not be entirely independent in their capacity to act, cannot be excluded.

The absence of systematic monitoring of forced returns

As pointed out in the study, "third country nationals do not have a subjective right to be monitored" (p.20). Moreover, it is recalled that the Commission does not consider "the mere existence of judicial remedies in individual cases" as a transposition of the obligation to set up a forced return monitoring mechanism (p.20). In the absence of a subjective right to be monitored, it seems reasonable to expect that forced return monitoring mechanisms are compliant with European standards in ensuring that all forced returns are respectful of human rights and fundamental freedoms. In the absence of automatic monitoring, the risk exists that some people are wrongfully returned because no preventive mechanism is in place.

Frontex Joint Return Operations

The identification of a need for a monitoring mechanism for Frontex operations fits the general consensus reflected in the amended Regulation 2004/2007 on the Agency, which foresees such mechanism in Article 9(1)b. [7] It is recommended that host countries should nominate a monitor for each joint return operation, but the study does not reach a conclusion on the submission of the report before national bodies in charge of monitoring forced return.

The unexplored potential of the study

An evaluation such as the Matrix and ICMPD study could have been used to improve practices in all EU countries where international standards apply. The death of Jimmy Mubenga and the alleged disproportionate use of force during his forced deportation emphasises the need for common standards and monitoring mechanisms applicable to all return operations, not only in response to misconduct, but also to prevent improper practices which may put lives at risk. The growing involvement of private companies in removal operations and the issues of accountability and monitoring are not addressed in the Matrix/ICMPD study either. [8]

The recent publication by Justice First [9] on the unsafe return of Congolese asylum seekers from the UK is a good example of the importance of proper return monitoring mechanisms, not only to assist decision-making when a return takes place, but also to ensure the safety of the people removed. This report documented the experiences of 17 asylum seekers returned to the Democratic republic of Congo, nine of whom alleged that they had been the victim of ill-treatment upon arrival in Kinshasa, and/or had been arrested, and faced imprisonment after information on their asylum case was passed on from the UK to the Congolese authorities.

Conclusion

While differences between Member States reflect their sovereignty in the field of immigration and asylum, the aim of a European immigration and asylum policy is the adoption of "minimum rules". Yet, in practice, much has been debated as to whether these "minimum rules" should act as the lowest common denominator or should improve the standards in accordance with the European Union's values. The state of play of monitoring mechanisms in Member States shows that, depending on where migrants are returned from, their rights will not necessarily be safeguarded in a consistent way across the EU.

The information available helps to identify best practices, some of which are a step in the right direction (e.g. mechanisms involving independent monitors, or extending the scope of monitoring to the post-return phase and reintegration in the country of origin). Nevertheless, in the general context of the promotion of EU standards in the field of immigration and asylum which are compliant with the respect of fundamental rights and freedoms, the recommendations submitted in the study do not reflect the need for improvement in some practices that have been criticised: breaches of returnees' rights and developments such as the accountability of private companies in charge of removal operations.

Endnotes

[1] Matric/ICMPD (2011) Comparative Study on Best Practices in the Field of Forced Return Monitoring JLS/2009/RFXX/CA/1001, European Commission Directorate-General Justice, Freedom and Security,

http://ec.europa.eu/home-affairs/doc_centre/immigration/docs/studies/Forced%20Return%20Monitoring%20Study%20Final%20Report.pdf

[2] Peers (2005) The "Hague Programme": Annotation of final version, approved 5.11.2004, p.16,

http://www.statewatch.org/news/2004/nov/hague-annotated-final.pdf

[3] Directive accessible at

http://www.statewatch.org/semdoc/assets/files/council/DIR-2008-115.pdf

[4] European Commission (2009), Invitation to tender No. JLS/2009/RFXX/CA/1001 concerning a comparative study on best practices in the field of forced-return monitoring, p.7,

http://ec.europa.eu/justice/tenders/2009/338746/tender_en.pdf

[5] The Council of Ministers of the European Union must not adopt the outrageous directive!, Joint communique (Anafé, APDHA, Arci, ATMF, La Cimade , Gisti, IPAM, LDH-Belgique, Migreurop, Statewatch), 2008, http://www.migreurop.org/article1333.html

[6] Peers (2008a) The Returns Directive - 9 June 2008, p.10,

http://www.statewatch.org/news/2008/jun/eu-analysis-returns-directive-june-2008-final.pdf

[7] REGULATION (EU) No 1168/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union,

http://database.statewatch.org/article.asp?aid=31086

[8] The death of Jimmy Mubenga: "Securing your world" through "privatised manslaughter", by Statewatch Journal Volume 21 no 1 January-March 2011

[9] Justice First (November 2011)Unsafe return: Refoulement of Congolese Asylum Seekers. A report compiled by Catherine Ramos,

http://justicefirst.org.uk/wp-content/uploads/UNSAFE-RETURN-DECEMBER-5TH-2011.pdf

The EU's accession to the European Convention on Human Rights: a cause for celebration or concern?

by Chris Jones

Internal negotiations over whether to accede to the ECHR have been mired by problems and highlight fundamental shortcomings with the EU's decision making process. An insistence on secrecy and an emphasis on "strategic priorities" have come to take precedence over individual rights.

For nearly 40 years, there have been plans for the European Union (or its predecessor, the European Community) to accede to the European Convention on Human Rights, and thus submit the actions of its institutions to the jurisdiction of the European Court of Human Rights. In December 2009, when the Lisbon Treaty came into force, Article 6(2) of the Treaty finally provided a legal basis for this accession.

Negotiations between the EU and the Council of Europe for the purpose of formulating a legal instrument for accession took place between June 2010 and June 2011, although they were not entirely successful. Disagreement between EU Member States over the minutiae of the legal instrument seems to be the primary cause of the delay.

Following a brief outline of the current situation for judicial human rights protection in the EU the substance of the accession agreement is covered; this is followed by a discussion of the EU's need to accede to the ECHR and its current relationship with human rights; elements of the accession agreement that will lead to discussions over whether the EU can yet be considered a state; and the fact that the accession procedure, on the EU side, has been marred by a lack of transparency.

Human rights protection in the EU

It is a common mistake that the European Court of Human Rights is an organ of the European Union. It was in fact established by the Council of Europe in 1953, and has 47 signatory states, 27 of which are EU Member States. This will rise to 28 with the accession of Croatia to the EU.

Individuals are able to submit a case to the European Court, located in Strasbourg, only after the exhaustion of all domestic remedies. It therefore functions as a court of 'last resort' for those dissatisfied with the final decisions of the highest national courts. While all EU Member States are required to be party to the European Convention, its provisions are frequently undermined or flouted by the actions of those states – the purpose of the European Court is to try and provide external scrutiny of state action.

The EU's own high court is the European Court of Justice of the EU, which "settles legal disputes between EU governments and EU institutions". It is also possible for "individuals, companies or organisations [to] bring cases before the Court if they feel their rights have been infringed by an EU institution." [1]

Until the EU accedes to the European Convention on Human Rights it will remain impossible to submit the actions of EU institutions to the scrutiny of the European Court of Human Rights.

The substance of the accession agreement

The legal instrument to be agreed between the EU and the Council of Europe will cover a number of issues. There are 12 articles in the most recent (but not finalised) version of the *Draft legal instruments on the accession of the European Union to the European Convention on Human Rights*, covering:

- *Article 1: Scope of the accession and amendments to Article 59 of the Convention*
- *Article 2: Reservations to the Convention and its Protocols*
- *Article 3: Co-respondent mechanism*
- *Article 4: Inter-Party cases*
- *Article 5: Interpretation of Articles 35 and 55 of the Convention*
- *Article 6: Election of Judges*
- *Article 7: Participating of the European Union in the*

Committee of Ministers of the Council of Europe

- Article 8: Participation of the European Union in the expenditure related to the Convention

- Article 9: Relations with other Agreements

- Article 10: Signature and entry into force

- Article 11: Reservations

- Article 12: Notifications

Negotiations between the EU and Council of Europe Member States within the *Informal Group on Accession of the EU to the Convention* (CDDH-UE) led to the production of a 'final version' of the *Draft legal instruments* in July 2011. However, EU Member States have still not managed to agree upon their position, and negotiations look set to continue well into 2012.

The implications of Article 1 are discussed at some length below (under the heading 'A distinct legal entity'). Article 2 of the *Draft legal instruments* modifies Article 57 of the Convention, in order to allow the EU to make reservations to particular provisions of the ECHR "to the extent that any law of the European Union then in force is not in conformity with the provision." However, laws passed following accession must conform with the provision that is subject to reservation, and reservations have to be specific, "preferably restricted to a particular right" and not be general in nature. [2] There is no indication that the EU is intending to make reservations to any of the Convention's articles.

Article 2 also deals with the issue of the Protocols to the Convention. There are only two Protocols to which every EU Member State is a signatory – 'the Protocol', concerning property, education and elections, and Protocol number 6, concerning the abolition of the death penalty, except in times of war or "imminent war". The other protocols deal with the issues of civil imprisonment, free movement and expulsion (Protocol 4); criminal matters (procedure, appeals, compensation, double jeopardy - Protocol 4) and family; discrimination (Protocol 12); and the total abolition of the death penalty (Protocol 13).

As it is only the Protocol (i.e. the first Protocol, to which a number was not given) and Protocol 6 that all Member States have both signed and ratified, it is only the provisions of these Protocols that will apply to the EU upon its accession.

The co-respondent (or 'co-defendant') mechanism dealt with in Article 3 concerns the possibility of joint participation of both the EU and concerned Member States in a court case, in order "to avoid the situation where Member States alone bear the duty to defend the EU law's conformity with the ECHR". [3]

A submission by Amnesty International and the AIRE (Advice on Individual Rights in Europe) Centre to the CDDH-UE highlighted some of the issues surrounding the co-respondent mechanism, their main concern being that depending on the wording of Article 3, the mechanism may be overused and lead to the over-complication of cases, and the unnecessary involvement of the EU where fundamental principles of EU law may not be the primary issue at stake. [4]

A submission to the CDDH-UE from national human rights institutions also raised the concern that in cases where the EU and a Member State or Member States are acting as co-respondents, "the gulf between the legal resources at the disposal of applicants and...State and EU legal experts will likely render it more difficult for applicants to overcome admissibility criteria and be successful in their application". In such a situation, applicants would require an extended timeframe to prepare and submit their applications. Such extensions "should not be excessive but should be reasonable...Overtly stringent requirements would frustrate the equality of arms requirement enshrined in the Convention". [5]

Judging from discussions that took place in the EU's Working Party on Fundamental Rights, Citizen's Rights and Free Movement (FREMP) in November, there is some way to go before agreement is reached on the specificities of this article. Further discussion was deemed necessary on at least two of the sub-articles. [6]

It appears there is no dispute amongst EU Member States on the substance of Articles 4, 5 and 6 as they appear in the Draft agreement. Article 7, however, saw both the UK and French delegations in FREMP raise "strong objections". Article 7 deals with the voting rights of the EU and its Member States within the Council of Europe's Committee of Ministers, the body responsible for supervising the execution by parties to the ECHR of the judgements of the European Court of Human Rights.

It seems that most ire was reserved for a proposed amendment to the Committee of Ministers' rules that would limit the voting rights of the EU and its Member States when supervising "judgements in which the EU, on its own, or along with one or more Member States, has been found in breach of the Convention." Bloc voting is of course undertaken by the EU Member States in a number of international fora, and the UK and French delegations felt that the proposed Draft agreement put this principle under threat. Currently the EU does participate in the Committee of Ministers, but has no voting rights.

One concern is that were the EU and its Member States to coordinate positions within the Committee, it could affect the execution of judgements handed down against the EU or its Member States. The UK and France seem to favour "a procedural safeguard mechanism whereby High Contracting Parties which are not EU Member States may question judgements concerning the correct execution of a judgement." [7] This proposal was questioned by a number of the other delegations. As with other issues, further discussions were considered necessary.

The remaining articles deal with expenditure by the EU related to the Convention, and the implementation of the agreement. It would however seem that the UK's enthusiasm for austerity has reached the negotiations, with its delegation "insisting on further clarification of the financial implications...this was to be considered as a precondition for its assent to the draft Accession Agreement."

The provisional agenda for Council meetings under the Danish Presidency foresees an "Orientation debate with a view to concluding the accession agreement" taking place during the JHA Council on the 8 and 9 March 2012.

The need for accession

Article 6(2) of the Lisbon Treaty states that the EU "shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms," and that the provisions of the ECHR shall therefore "constitute general principles of the Union's law." (*Lisbon Treaty*)

The Stockholm Programme states that accession should be "rapid", and invites the Commission "to submit a proposal on the accession of the EU to the ECHR *as a matter of urgency*," (emphasis in original) due to the fact that it will "reinforce the obligation of the Union, including its institutions, to ensure that in all areas of its activity, fundamental rights are actively promoted." (It may of course be noted that promotion and protection are entirely different concepts.)

The Spanish presidency of the EU noted that the issue of accession "ranks amongst the highest priorities". Work on accession continued under the Belgian presidency during the second half of 2010, with the subsequent Hungarian presidency also stating that the issue would be "a top priority."

Clearly, there is a significant impetus within the EU's institutions for accession to the ECHR. One reason for this is certainly to do with the global image of the EU as a promoter and protector of human rights standards. In March 2010, as the EU

Member States were attempting to coordinate their approach to negotiations with the Council of Europe, Viviane Reding (at the time Vice-President of the European Commission for Justice, Fundamental Rights and Citizenship) made a speech to the European Parliament's Constitutional Affairs Committee, stating that becoming a signatory to the ECHR would "enhance the credibility both internally and externally of the EU's strong commitment to fundamental rights."

"An ambitious and comprehensive rights policy"

Of course, accession is not merely a propaganda exercise; its political and legal implications are significant. Joining the Convention system of rights protection is "one out of four key components of an ambitious and comprehensive EU fundamental rights policy."

The other three components are the Charter of Fundamental Rights becoming legally binding following the entry into force of the Lisbon Treaty; the Stockholm Programme's priority of "promotion of fundamental rights...setting the strategic guidelines for developing an area of freedom, security and justice in Europe"; and "the creation of the new 'Justice, Fundamental Rights and Citizenship' portfolio" which "shows the importance that President Barroso attaches to strengthening this area of the Commission's action."

Quite how seriously the EU's human rights obligations are taken by its policy-makers is open to question. A damning report from Human Rights Watch [9] discussing "Europe's own human rights crisis" suggests that, moving beyond "the fine words...human rights in Europe are in trouble." Intolerance towards minorities (in particular Muslims); the persecution of the Roma and an increase in policies that trade rights for 'security' is indicative of failure's by European governments and EU institutions to respond effectively to human rights issues.

In May 2011, FREMP produced *Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council's preparatory bodies.* [10] These were produced in order to try and ensure that fundamental rights (as laid out in the EU Charter) were taken into account during preparatory work undertaken in the Council's numerous working parties and preparatory bodies. The *Guidelines* provide advice on checking whether proposals affect fundamental rights; thinking "from a fundamental rights perspective"; examining legislative proposals in relation to jurisprudence, and so on. Unfortunately, the first sentence of the *Guidelines* states that they "should be considered as non-binding advice."

"A distinct legal entity"

Perhaps the most significant political effect of accession will be the recognition of "the Union's specificity as a distinct legal entity vested with autonomous powers." The ability of individuals to take legal proceedings against EU institutions makes necessary the representation of the EU as a specific legal entity. It will be represented at the Court by its own representative judge, and will be able to participate in the Committee of Ministers (the Council of Europe body responsible for, amongst other things, supervising the execution of judgements).

It should be noted that the accession agreement negotiated between the EU and the Council of Europe will make clear that the EU is not considered a state. Whether it will be defined in anything more than the negative is currently unknown. In October 2011, the informal working group established between the EU and the Council of Europe (CDDH-UE) discontinued its work. Despite a year of negotiations, "given the political implications of some of the pending problems, they could not be solved at this stage by the CDDH or the CDDH-UE." The CDDH therefore considered "it had done all it could, as a steering committee," and transmitted its report and the draft legal instruments "to the Committee of Ministers for consideration and further guidance."

Reading the final version of *Draft legal instruments on the accession of the European Union to the ECHR* produced by the CDDH-UE, the potential political implications become apparent. The 'final version' of the document, produced in July 2011, refers to the fact that the "specific legal order of the European Union" means that the Convention system "requires certain adjustments." These adjustments, according to the July 2011 *Draft legal instruments,* include making applicable to the EU the terms 'State', 'State Party', 'States' or 'States Parties' where they appear in the Convention.

The same applies to the terms 'national security', 'national law', 'national laws', 'national authority', 'life of the nation', 'country', 'administration of the State', 'territorial integrity', 'territory of a State' or 'domestic', which "shall be understood as relating also, *mutatis mutandis* [the necessary changes having been made], to the European Union." [11]

Unsurprisingly, the possibility of interpreting this as meaning that the EU should be considered a state was considered unacceptable by EU Member States' delegations. Discussions on the CDDH-UE draft in the EU's Working Party on Fundamental Rights, Citizens' Rights and Free Movement of Persons (FREMP) saw the UK in particular seeking more specificity. Its delegation was successful in having an amendment made to the Preamble so that it would read "having regard to the specific legal order of the EU, which is not a state." [12]

Furthermore, following "informal discussions and by way of compromise" the Presidency suggested further changes to both the sections referred to above. The proposed compromise was to have any reference to 'State', 'State Party', 'States' or 'States Parties' within the Convention as "referring also to the European Union as a non-State party to this Convention." It was further proposed that references to 'national security' etc. be qualified with that statement that "they shall be understood as relating also, *mutatis mutandis*, to the European Union, insofar as they relate to matters falling within the competence of the European Union." (p.4)

A further series of suggestions were made by the Presidency in order to allay the disquiet of Member States about further potential references to the EU as constituting a country, having a State administration, or being able to refer to its 'national security', the 'economic well-being of the country', or its 'territorial integrity'.

It seems that on these issues, and on many others, Member States' disagreements will not be resolved any time soon. Nevertheless, the very fact that the EU is deemed able to accede to the European Convention will be enough for some to consider it as now constituting a state. Following the UN General Assembly's resolution on the participation of the EU in the work of the UN (permitting EU representatives the right to present the General Assembly common European positions; the right to present proposals and amendments; and the right of reply regarding positions of the EU) [13] it was suggested by a UK Conservative MEP, Daniel Hannan, that according to the 1933 Montevideo Convention on the Rights and Duties of States, the EU could be considered as a state. [14] Accession to the ECHR is likely to lead to significant further debate on the issue, regardless of the wording of the accession agreement itself.

"Too nutty for Monty Python"

The 'story so far' of the EU's accession to the ECHR has been marred by problems other than those of disagreement between the Member States. One particular instance of refusal to make public documents related to the negotiation procedure has been described as "even too nutty for Monty Python," by the applicant.

Frank Schmidt-Hullmann, head of the international

department for the German trade union *IG Bauen-Agrar-Umwelt*, applied to the Council of the European Union for access to a document outlining the negotiating mandate decided upon by the Council. Access was refused on the basis that "full release" of the requested documents:

> *Would reveal the Union's strategic objectives to be achieved in the international negotiations...[enabling] the Union's negotiating partners to assess the measure of the Union's willingness to compromise.[15]*

Mr Schmidt-Hullmann argued against the Council's refusal to publish the document, noting that:

> *A Danish version of the full document – which coincidentally, also happens to be the mother tongue of the other party's chief negotiator – was, for many months, freely available to download from the Internet. The other party in the negotiations should therefore already have the text and hence there is no longer any need to maintain confidentiality.[16]*

A subsequent investigation by the Council found that it was in fact a later version of the requested document that had been released in full on the internet, containing the final version of the negotiating directives – nevertheless, the principle of Mr Schmidt-Hullman's request continued to apply.

The final response of the Council was to remove the document from the internet – stating that publication of its full contents "had occurred only due to human error" – and to re-classify the document. This unintentional act required "a correction in order to safeguard the public interest in the Union's international relations as described above." [17]

This position could not, however, be agreed upon by all Member States delegations to the Working Party on Information, which considered Mr Schmidt-Hullman's application. Denmark, Estonia, Finland and Sweden took the view that:

> *The remaining parts of the documents do not, at least entirely, come under the said exception [protection of the EU's negotiating position]. The Convention is of a special nature and EU's objectives in the negotiation process are largely based on the text of the Treaty and/or the protocol attached to it, and access to the documents should be extended at least on these parts.[18]*

Non-governmental organisations that were occasionally party to negotiations within the CDDH-UE seem to share a similar view. In the final report of the CDDH-UE, they:

> *Emphasised that the people whose human rights are at issue in this process should be kept at the centre of the debate and that there was a need for greater transparency in the proceedings in the EU. [19]*

Another, unnamed, applicant seeking access to the documents outlining the EU's negotiating mandate was also refused access following their initial request. They argued that the very point of the negotiations was to improve the EU's mechanisms for the protection of human rights, and thus should be released:

> *Clearly, and until proven otherwise, negotiation of a treaty EXCLUSIVELY designed to protect the fundamental rights of citizens is by definition a process of fundamental importance (and great relevance in terms of both Community law and Member States' constitutional law) and great interest to the citizens whose rights are at issue.(...)*
>
> *Ensuring that the negotiations are public should be a factor for raising awareness of the fundamental human rights guaranteed by the Convention and the Union Treaties, and therefore would be fully in line with the obligations to promote and protect human rights to which the Union itself has subscribed. [20]*

Again, the Danish, Finnish and Swedish delegations argued for the release of at least some portions of the negotiating mandate. Other delegations decided that disclosure was not in the public interest and would harm the EU's negotiating position.

It should be noted that over a period of just over a year (from July 2010 to September 2011), an increasing number of sections of a copy of the *Draft Council Decision authorising the Commission to negotiate the Accession Agreement* (10602/10) were released. However, not one line of the negotiating mandate included within the document was ever made public.

Summary

Europe is able to boast one of the most extensive judicial systems of rights protection in the world, and the accession of the EU to the ECHR will certainly reinforce this. However, the character of the EU's internal negotiations highlights some of the problems with the EU's decision making process – an insistence on secrecy and an emphasis on 'strategic priorities' above the consideration of the rights of individuals.

Endnotes

1. http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm

2. http://www.liberty-human-rights.org.uk/pdfs/policy02/interventions-dec-2002.pdf, p.2-3

3.http://afsj.wordpress.com/2010/02/24/the-first-eu-steps-towards-the-accession-to-the-european-convention-of-human-rights/

4.(http://www.coe.int/t/dghl/standardsetting/hrpolicy/cddh-ue/CDDH-UE_documents/AIRE&AI_comments_March2011.pdf

5.(http://www.coe.int/t/dghl/standardsetting/hrpolicy/cddh-ue/CDDH-UE_documents/CDDH-UE_EG_NHRI_Submission_9_March_2011.pdf

6. DS1675/11, p.6-8

7. DS1675/11, p.8

8. DS1675/11, p.9

9. http://www.hrw.org/sites/default/files/related_material/eucrisis_2012.pdf

10. http://register.consilium.europa.eu/pdf/en/11/st10/st10140.en11.pdf

11. (http://www.coe.int/t/dghl/standardsetting/hrpolicy/cddh-ue/CDDH-UE_MeetingReports/CDDH_2011_009_en.pdf

12. DS1675/11

13.

http://www.un.org/apps/news/story.asp?NewsID=38261&Cr=general+assembly&Cr1

14. http://blogs.telegraph.co.uk/news/danielhannan/100053681/the-eu-wants-to-be-treated-as-a-state-by-the-united-nations/

15. 13725/11, p.5

16. 13723/11, p.7

17. 13725/11, p.6

18. 13725/11, p.1

19.http://www.coe.int/t/dghl/standardsetting/hrpolicy/cddh-ue/CDDH-UE_MeetingReports/CDDH_2011_009_en.pdf, p.4-5

20. 12676/10, p.6

Book Reviews

Black for a Cause...Not Just Because...The Case of the 'Oval 4' and the Story of Black Power in 1970s Britain, Winston N. Trew. The Derwent Press 2010, 310 pages (ISBN 10: 1-84667-039-1) Reviewed by Trevor Hemmings

Black for A Cause...Not Just Because tells the story of four young black men - Winston Trew, Sterling Christie, Constantine Boucher and George Griffiths – who became known as the Oval 4 after being assaulted by the police, arrested and falsely convicted of robbery in 1972. The book is the eyewitness account of one of the men who was falsely accused, and as such it is a unique historical document bearing testimony to the endemic police racism inflicted on the everyday lives of black British working class communities. It is also the record of a generation of movements that emerged to defend their communities in the early 1970s. The activism that arose to resist state (as well as non-state) violence was redefined by the media in terms of a breakdown of law and order and by the criminal justice system as lawlessness, defined by the emotive – but legally meaningless – US term "mugging." In many respects the mugging scandal was a direct attack on the "investment made by Caribbean parents in their young, who were seen by Black organisations as representing the hopes and future of black settlement and development in Britain." Indeed, the police war on mugging, just as with the war on terror in the twenty-first century, was mainly successful in criminalising many innocent young black men, removing any prospect of their employment or a future.

Winston Trew was one of a group of young Fasimbas (Swahili for Young Lion), members of a black youth organisation that provided educational, cultural and political support to their local south-east London community. The group embraced Malcolm X's ideas on political community self-defence, self-organisation and self-reliance combined with the ideas of Marcus Garvey. Trew describes and analyses the experiences of growing up in south London as a young black man: the racism that blighted his education and his growing political and cultural consciousness set within the context of a putative British Black Power movement. He discusses his role in forming the South East London Parents Organisation (SELPO), and in so doing offers the first inside account of this historically important organisation. SELPO played a key role in establishing education classes to combat the racism of the British education system which regularly assigned black children an ESN (educationally sub-normal) status. The Fasimbas comprised the younger generation whose programme envisaged an education - and politicisation - to correct an education system in which black history had no place. These organisations forged links with like-minded social, cultural and political organisations in west London (Black Liberation Front, BLF) and north London (Youth Forces for National Liberation, YFNL). The period is evoked through the use of contemporary reggae and soul lyrics, that are suffused with protest and raise philosophical questions about the meaning of being black.

Trew describes in evocative detail the police ambush that led to the arrest of the Oval 4 after they left a political meeting and arrived at Oval tube station in south London in March 1972. The youths were set on by a gang of white men as they reached the top of an escalator and manhandled and abused by them. These plain clothes police officers accused Trew and his comrades of stealing handbags (no evidence was ever produced) but refused to show them any identification. Trew and his friends were arrested and subsequently imprisoned; Trew, who was sentenced to two years, was eventually released on appeal in July 1973. Like the case of Mangrove 9, who had successfully defended themselves against riot charges a few months previously, the Oval 4 convictions marked another turning point in the criminalisation of black youth by racist police officers who labelled them as "muggers", a rebranding of robbery that was marketed as synonymous with violent black crime. Like the use of "sus" (stop and search based on racial profiling and stereotyping) before it, it necessitated the organisation of militant community-based organisation to counter abuses of police powers and the injustices of a compliant legal system.

In May 1978, some six years the trail of the Oval 4, the main police protagonist, Detective Sergeant Derek Ridgewell, was arrested and exposed as a "corrupt policeman." The instigator of the framing of the Oval 4 was convicted of conspiracy to steal – ironically, one of the charges that the Oval 4 defendants had been convicted of – and sentenced to seven years imprisonment. Transferred from anti-mugging duties, Ridgewell had been tasked to investigate large scale robberies from goods depots and rapidly became a lynchpin in a lucrative "police escort" service for escalating thefts. In December 1982 Ridgewell was found dead in his prison cell after suffering a heart attack.

This autobiography is an important historical work that, on one level, documents the wrongful arrest and imprisonment of a young black man for crimes that he did not commit. However, it is much more than this for it places the racist treatment black youth by the police in the early 1970s within the context of the media "mugging scare" which was utilised by the criminal justice system to criminalise black communities. The militant black organisations that emerged as a consequence, SELPO, The Fasimbas, and others, highlighted the racism that blighted the education system and in attempting to illuminate black history and culture found themselves targeted by an institutionally racist police force. This institutional racism remains to this day, as is manifested in the massively disproportionate imprisonment of young black men, the use of joint enterprise laws and the return of stop and search and racial profiling. But so, importantly, does the resistance of black communities that was born out of the struggles of the 1970s.

The Crises of Multiculturalism, Racism in a Neoliberal Age, Alana Lentin and Gavin Tilley. Zed Books (London) pp.285 (ISBN 9781848135819). Reviewed by Chris Jones

A sizeable book concerned "with the insistent sense of multiculturalism as a unitary idea, philosophy, 'failed experiment' or era...[S]ince 11 September 2001 commentators, politicians and media coverage have increasingly drawn on narratives of the 'crisis of multiculturalism' to make sense of a broad range of events and political developments, and to justify political initiatives in relation to integration, security and immigration." However, as the authors are keen to stress, "multiculturalism has rarely amounted to more than a patchwork of initiatives, rhetoric and aspirations in any given context". With this as a starting point, the authors work their way through chapters covering the idea of multiculturalism and its discursive functions; the persistence of racism via its replacement by the idea of 'culture'; the complicated and frequently racist content of contemporary liberalism as shaped by concerns over 'multiculturalism'; the nature of public debates on immigration and integration; the "post-racial logics of 'diversity politics' in [Europe]" and the ways in which discussions of diversity serve to mask racist assumptions and attitudes; and finally with an examination of "how partial and inconsistent visions of already achieved equality and freedom are at the nexus of new forms of racialised exclusions being elaborated by state and civil society actors". Seeking to provide critical analysis and information of

contemporary racial and racist politics, the transnational scope of The Crises of Multiculturalism provides a wide-ranging interrogation of the numerous ways in which racism has been re-packaged and re-invented in the contemporary era.

Maurice Punch ***Shoot to Kill: police accountability, firearms and fatal force*** (The Policy Press, UK) 2010, 264 pages, ISBN 9781847424723. Reviewed by Dick Muskett

In the aftermath of the shooting of Mark Duggan in Tottenham, you can feel a certain trepidation picking up a book with the dramatic title 'Shoot to Kill' and a sub-heading of 'police accountability, firearms and fatal force'. Is it going to be a justification of tragedies such as the shooting of an innocent electrician in a train at Stockwell, or a full-on denunciation of a trigger happy out-of-control culture that dominates the Met? Interestingly it is neither of these two things, but rather a well-written analysis of the evolution of firearms policy in the police, that sets out, with considerable success, to understand how Jean Charles de Menezes was killed in 2005 and what can be done to diminish the chances of such an event happening again.

Maurice Punch is not a police officer but he knows the organisational structures and tactics of the police well, not just in the UK, but also in the Netherlands and the USA and has written extensively on the subject. He acknowledges the advice and collaboration he has had from senior police officers here and abroad, which for some commentators may mean that he is irrevocably suspect. I'd suggest that this would be a pity as the book provides a fascinating insight into the drift into the current situation and highlights the fudging of the chain of command and the role played by ACPO, an unelected and unaccountable body, in formulating firearms policies for the police.

Punch sets the scene by tracking the history of the arming of police in the UK, from Robert Peel's first police force. Although Peel's force held a small number of pistols, cutlasses were more frequently issued to patrols in times of disturbances, with the policy being to bring in troops if it became necessary. Punch makes the point that although Peel and the Tory administration in 1829 were anything but liberal, they made a clear government decision that the police should not be an armed gendarmerie on the continental model but a civil force.

This can partly be attributed to the ongoing concerns about revolutionary ideas but also reflected the lessons the Government had learned from the deaths and injuries in Manchester in 1819, when a detachment of (probably) semi-drunken Yeomanry charged a peaceful rally in St Peter's Field with sabres drawn, killing between a dozen and twenty people and injuring many more. Known sardonically as the battle of Peterloo, it influenced Ministers to avoid using Yeomanry in crowd control situations if possible.

Yeomanry were volunteer units, usually drawn from the sons of local industrialists and merchants, usually fond of designing fancy uniforms for themselves and riding around looking for an opportunity to break a few working class heads. Ten years after Peterloo, when the surge in membership of the Grand National Consolidated Union took off, the then Home Secretary, Lord Melbourne, wrote on more than one occasion to magistrates concerned about militant trade union activity, urging them not to use Yeomanry but to call on regular army units who were considered to be more disciplined. I think it's likely that a generally reactionary ruling class were not at all averse to the odd exemplary shooting, hanging or transportation of troublesome individuals, but general massacres of radicals risked a backlash they didn't need.

The author's account takes a broad sweep across policing history, including the siege of Sidney Street in 1911, and amateurish approach to firearms in the 1950s and 60's, with stories of how, following reports of armed criminals, cardboard boxes of elderly revolvers, sometimes still in their factory grease, were dug out of lockers. Constables recalled going out with a revolver in one raincoat pocket and a handful of rounds in the other, with a Sergeant's instruction not to load the gun unless they really needed to. A long way from the Heckler & Koch semi-automatic carbines seen in public places today.

The author uses the narrative to highlight several factors that seem central to the story of police and guns. First are the recurring mistakes and cock-ups whenever guns are used, a few ending in tragedy but more as farce. Then there are the interesting statistics: Punch states that in the overwhelming number of cases where firearms are issued, no shots are fired; one of the experienced officers who took part in the Stockwell operation that resulted in Jean de Menezes death had previously taken part in over 2000 firearms incidents but had never before fired at a person; a senior officer had in his career granted around 4000 authorisations for the use of firearms but in none of them had the police opened fire; in the rare cases when police have fired, at least half the rounds have missed their targets, and on the very few occasions that a person has been hit by a police bullet, over half survive.

Punch correlates these figures to similar statistics from both the USA and Holland and finds the same picture. For example, in New York, a city with over 30,000 police officers, the vast majority will never fire a weapon in anger in their entire career. The author's argument is that in general police officers avoid opening fire and when they do, they will try to avoid shooting to kill, despite that fact that all training insists that if the weapon is fired, it must be aimed at the centre of the torso.

What Punch does stress over and again is the dislike of firearms and an unwillingness by most operational police to use them if it could be avoided. This seems partly because of the tradition of an unarmed force, partly because it was thought by some that more armed police would lead to more armed robbers but primarily because of an organisational feature that few of us have heard of. Police Officers in the UK are sworn in as Constables, and although this is generally assumed to be a rank, like Private, it is also a post under the Crown and as such police officers, whatever rank they may rise to in their career, are utterly different from any other uniformed public servant, whether a soldier, a firefighter or a traffic warden.

The common law assumption about the role of a constable is that their authority is original, not delegated, and the holder of the office is accountable to the law, not to another person, exercising 'his' power at 'his' discretion. This could be interpreted to mean that it was the constable's responsibility whether they opened fire and they could not in theory be ordered to fire by their superior. This culture, certainly until the last twenty or so years, was about resolution of a situation by de-escalation, of the use of minimal and proportionate force, of justifying every round fired and the personal responsibility of each individual officer. Punch's thesis is that by and large this worked reasonably effectively so long as the armed officer was dealing with either a bank robber armed with a handgun or an armed individual suffering from acute mental stress, and behaving with complete irrationality. Terrorism, and to a lesser extent the acquisition of powerful automatic weapons by some criminal gangs, have made that old school approach as archaic as the elderly Webley revolvers it depended upon.

From the 1970s, conflict in both the Middle East and Ireland started to spill into Europe and UK police forces started to re-think their response to an entirely new situation. The picture that emerges is a spike in the acquisition of new and much more powerful weapons and the training that their use required. This was patchy and relatively uncoordinated, due probably to the differing approaches of the Police Authorities and a resistance to the need for heavy weaponry by many senior police officers. Special firearms units had to be formed, with selected officers

undergoing a radically different type of training but alongside most of their colleagues adhering to the concept of an unarmed police for all normal duties.

What didn't match the 'mission creep' of increasingly sophisticated firearms were the command structures to oversee the tactical deployment of the weapons. The authorisation system to deploy weapons on the ground, probably adequate when the threat was a villain with a sawn-off shotgun, proved to be clumsy and painfully slow in the face of the new threat. Punch describes instances when the only officer in an area who could authorise the deployment of firearms was away for the weekend, and so on. Inevitably, the newly trained firearms teams grew to see themselves as an elite who were hampered by their commanders caution and equivocation. Punch does however note that however special the new firearms teams saw themselves, they were not in any sense on par with regular army SAS units, in training or experience.

Central Government had reacted to growing public concerns over a range of issues, from police corruption to miscarriages of justice and public disorder, by deluging forth a stream of legislation covering all manner of police and criminal justice issues, but as Punch observes, studiously avoiding the subject of firearms use and fatal force. The pressure on Chief Constables to bring coherence to the use of firearms did not diminish however. For instance, Justice Rafferty's statement following the trial of the individual police officer who fired a fatal shot that killed an unarmed man in a police raid in Hastings in 1998 was pointed. She made it clear that there had to be a line of institutional responsibility running back to senior officers who should also be held to account when things went wrong. But the policy vacuum on the use of firearms remained until it was filled by an organisation that had no statutory role and no public accountability – ACPO, the Association of Chief Police Officers.

With hindsight, it's possible to see that the Police's long tradition of resisting centralisation and of clinging fiercely to local autonomy created an open goal and ACPO took advantage. It may also be that Chief Constables who might be bitterly opposed to a policy being formed by civil servants felt much happier knowing that potentially contentious policies were being developed by individuals they knew well, in an organisation that they were part of.

In any event, it appears that ACPO were responsible for significant changes in the way that police in the UK used firearms. Punch sets out the long standing ground rules for opening fire, and then contrasts them with the very different approach after the Kratos policy was adopted. Kratos was seemingly formulated by ACPO to deal with an admittedly entirely new situation, where a suicide bomber would be likely if apprehended to detonate the device he or she was carrying. From an approach that was based on firing only as a last resort, after due warning and then with the aim of preventing the individual from harming someone, Kratos instead set out a strategy of shooting the potential suicide bomber in the head, at once, without warning and to continue firing until the target was incapable of taking any further action, in other words, dead. Moreover, the thinking that produced Kratos overturned nearly two hundred years of policing practice by laying down that a senior officer could order an armed officer to take this action.

Maurice Punch takes the reader through the aftermath of the fatal tube bombings on the 7 July 2005, followed by the failed bombings a fortnight later. His account of the 24 hours following those attempts, as the suspected perpetrators were tracked is riveting and I found its recounting of the succession of errors and cock-ups had a familiarity that sounds real. The circumstances of operating in a city where a fortnight ago over 50 people died in suicide blasts, and where the previous day a repeat had only been avoided by chance created a tension that made a violent climax almost inevitable. The awful death of Jean Charles de Menezes was the result.

There will be many people who will believe that a Kratos policy is never acceptable under any circumstances. There will be very many more who despair of it but will ask what else can be done? If there are grounds for believing that a suicide bomber is about to detonate themselves, what do you do? That's a question that each of us has to decide for ourselves but the State is certain to reserve that right to kill if it seems it is justified.

What we can usefully do is to focus on demanding that if ACPO is to be the chosen body to create policy on the use of firearms by the police, then ACPO has to be publicly accountable and its policy proposals must be scrutinised. The procedures for taking the ultimate action of killing need to be very much more coherent than they appear to be at present and senior police officers need to spend a considerable time examining what went wrong at Stockwell and thinking hard about how each little glitch could be avoided.

Accidents will always happen but steps can and must be taken to reduce the chances of them happening to infinitesimal numbers. Maurice Blunt's book is a good enough place to start that process.

Policy Press: http://www.policypress.co.uk/

Steadfast in Protest – Annual report 2011, *Observatory for the Protection of Human Rights Defenders (FIDH-OMCT),* November 2011, 617p. **Regional Analysis on Western Europe,** pp.396-412. Reviewed by Marie Martin

The Observatory for the Protection of Human Rights Defenders was created in 1997 as a joint initiative by the International Federation of Human Rights (FIDH) and the World Organisation Against Torture (OMCT). For the past 14 years, the Observatory has been reporting on cases of "persons at risk or victim of retaliation, harassment or violation due to their involvement individually or as a group, in favour of the promotion and the implementation of rights enshrined in the Universal Declaration of Human Rights and safeguarded by various international mechanisms". While this year is obviously marked by the uprising in the Middle East and in North Africa, the report is an occasion to recall that, in a number of countries "no wind of change [has been witnessed] but a great deal of continuity or even an exacerbation of threats and assaults on human rights defenders". Despite Europe having one of the most developed and comprehensive legal frameworks protecting fundamental rights and freedoms, many people face threats, violence or harassment in Western European countries as a result of them taking positions in favour of human rights. The EU has appointed "human rights defenders' focal points" in over 80 countries, but appear to fall short of implementing its own guidance when it comes to internal social and political challenges. Growing discrimination against migrants, LGBT people and minority groups such as Roma, restrictions to press freedom and trade-union activities, along with judicial, administrative and financial restrictions to non-governmental organisations directly impacted on the environment in which human rights defenders were operating. Whether cases happened in EU or non-EU countries, a worrying trend towards the restriction of civil liberties, e.g. through the storage of personal data, and freedom of speech through arbitrary arrests and threats, is perceptible. Disturbing cases revealing total impunity and the disproportionate use of force against human rights defenders are not limited to "developing countries", as this report sadly documents: See: http://www.fidh.org/IMG/pdf/obs_2011_uk-complet.pdf

New material and sources

Civil Liberties

Good Muslim, Bad Muslim: a response to the revised *Prevent* strategy, Jahangir Mohammed & Dr Adnan Siddiqui. *Cageprisoners* 2011, 26 pages. This report is Cageprisoners response to the UK government's revised 'Prevent' strategy after the original proved to be "counterproductive both in terms of its strategy and its implementation." It finds that the "revised formulation only seeks to further alienate Muslims from the mainstream of society" because of an "overemphasis on the ideological challenges relating to political violence, and very little recognition of other factors. Indeed, the title of report was chosen precisely because the government's latest position signals to Muslims in the UK that it is the government that will decide what is acceptable religious practice and belief, and not the communities themselves." Among the main features of the report are analyses relating to: the profiling of Muslims; the root causes of political violence; secrecy and spying; the problem of definitions and the law; extremism in other communities; equality, discrimination, sectarianism and human rights; the healthcare sector and the Channel programme: http://www.cageprisoners.com/our-work/reports/item/1873-good-muslim-bad-muslim-a-response-to-the-revised-prevent-strategy

Global Burden of Armed Violence 2011, Keith Krause, Robert Muggah and Elisabeth Gilgen (eds.)**.** *Geneva Declaration on Armed Violence and Development Secretariat*, 2011. Following the 2008 report of the same title, this extensive study provides "a global overview of violent death across different forms of violence". Eschewing the more traditional distinctions drawn between organised and interpersonal violence, and conflict and criminal violence, it seeks to provide a more nuanced approach that recognises not all forms of violence can be so neatly distinguished from one another. Chapters provide a general overview; statistical trends and patterns; geographical and situational differences; femicide (the intentional killing of women); and the relationship between armed violence and development: http://www.genevadeclaration.org/measurability/global-burden-of-armed-violence/global-burden-of-armed-violence-2011.html

Immigration and asylum

Almost 700 children detained in three months and **Why are so many children being detained at out ports?** *The Children's Society* Press releases, October 2011. These news releases ask why so many children are being detained after travelling to the UK. Some children are held at Heathrow Airport and ports in the south-east in conditions described as "degrading" by the Independent Monitoring Board; they lack places to sleep and "even decent washing facilities." The 697 children held in Greater London and the south-east, could indicate that "as many as 2,000 children are detained annually, but shockingly, the Home Office is not collecting information on the length of detention or reasons why the children have been detained." This is after the government promised 18 months ago that it would end the immigration detention of children, with deputy prime minister Nick Clegg making an impassioned plea for an end to this "shameful practice." The Children's Society website: http://www.childrenssociety.org.uk/

Ways of celebrating 18-D. *Mugak*, no. 57 December 2011. The following introduction by the editorial team of *Mugak* in its December issue focuses on visits by migrant support groups in four of Spain's nine CIEs (Centros de Internamiento de Extranjeros, detention centres for foreigners), on racial profiling and stop-and-search operations in Spanish cities, on the construction of racist discourse and on stereotypes, prejudices and attitudes towards people from the Muslim faith. "When ephemeralities are set in the international calendar, like 10 December, anniversary of the Universal Declaration of Human Rights, or 18 December, International Migrants' Day, it appears that the institutions also need to highlight respect for the rights that are commemorated, at least on these dates. Well, on 15 December organised a joint removal flight for migrants to Dakar in Senegal. To do so, it set to work increasing identity checks on the streets to look for people from Senegal whose status is irregular, and concentrated Senegalese people held in CIEs (detention centres) around Spain in the CIE in Aluche [in southern Madrid, not far from Barajas airport] to make chartering the flight cost-effective.Among those to be expelled on this flight were people with detention orders issued by judges who are clearly settled, who have been recorded in the municipal residents' register [padrón] for four years, who have a stable residence and all the other criteria for applying [to be regularised] on this basis and which, according to the legislation, make detention and expulsion a disproportionate measure. This forms part of a policy of internment and expulsion of citizens who have not committed any other irregularity than that of looking to make a living wherever they can, even if they do not have the relevant administrative authorisation. And, to do this, Centros de Internamiento de Extranjeros, whose very existence and what happens in them is unknown to a large majority of the population, are used.The organisations that form part of the Migreurop network in the Spanish state have just released a report on the visits that they have undertaken in four CIEs in their attempt to throw light on the existence of this prison-like reality, and as part of its demand for both the closure of these centres and the requirement that the rights of people who are detained there be respected. This is certainly another way of celebrating 18-D." Available from: *Mugak*, Peña y Goñi, 13-1° 20002 San Sebastián.

Unsafe Return: Refoulement of Congolese Asylum Seekers, Catherine Ramos (compiler). *Justice First*, November 2011, pp. 36. The introduction to this briefing says: "This report has been prepared in response to a growing concern for the plight of Congolese nationals who have sought asylum in the UK, whose appeals have been refused and who have been forcibly removed to the Democratic Republic of the Congo between 2006 and 2011. During this period, first hand reports which were received from nine people who had been living in the Tees Valley area alleged inhuman and degrading treatment at the hands of the Congolese authorities." The need for the report arose because the "United Kingdom has no monitoring mechanism in place to test the UKBA hypothesis of safety on return for rejected asylum seekers". See: http://no-racism.net/upload/172818438.pdf

Law

The new SOCPA, Christina Dey. *Peace News*, No 2538 (October) 2011 and **SOCPAvistas, sleep on,** *Peace News*, No 2359, (November) 2011. The first article outlines the fact that although the Serious Organised Crime and Policing Act (SOCPA, which contains provisions restricting protest near parliament) was repealed on 15 September, it effectively has a replacement in the forthcoming (and highly controversial) Police and Social Responsibility Bill. According to the article, the new Bill "appears to prohibit 24-hour protests in Parliament Square". The article in the November issue contains slightly more detail. The Police Reform and Social Responsibility Act 2011 (PRSRA) does repeal sections of SOCPA that "required police authorisation for political protest and banned the use of loudspeakers in an area including Parliament Square". The new act does not do away with repression altogether, however. It contains retrospective provisions that apply to "public assemblies" that began before the act came into force: this is intended to target long-term, tent-based protests in Parliament Square. Part 3 of PRSRA applies specifically to the grassy island at the centre of the square and bans the use of amplified equipment, as well as the erection of a tent or structure on the central island that is "adapted...for the purpose of facilitating sleeping or staying...for any period". The police are able to seize any equipment that appears to be in breach of these provisions, with a maximum penalty for the offender of £5,000. The article notes, rather optimistically, that permanent protests in the square will be able to continue as long as "participants are willing to forgo any structure facilitating them staying in the square or any sleeping equipment". Peace News website: http://peacenews.info/

The state gets heavy – part 1, Tom Holness. *The Chartist*, September/October 2011. An article by one of 145 people arrested at a

sit-in inside luxury food shop Fortnum & Mason on 26 March 2011, during protests against the government's austerity measures. The author notes the political nature of the cases, the majority of which are based on accusations that anyone in the shop holding leaflets or making speeches was part of the organisation of the protest. A number of those whose cases have since been dropped have received threats from the Crown Prosecution Service that, should they be arrested again, their cases will be re-opened and the attempt to prosecute will begin again. Further comparisons are drawn with the nature of the sentencing in cases related to the recent riots. The Chartist website: http://www.chartist.org.uk/

Military

The Report of the Baha Mousa Inquiry. The Rt. Hon. Sir William Gage, Chair *The Stationery Office*, London, £155, 8.9.11, 3 Volumes. This is the official report into the torture and eventual killing by British soldiers of Iraqi civilian, Baha Moussa, in Basra in a case that has been described by Phil Shiner of Public Interest Lawyers as the "tip of an iceberg" of civilian abuse and murder by the British Army. The Iraqi hotel receptionist, and eight of his colleagues, were hooded and beaten for nearly 24 hours before Moussa died at the hands of the 1st Battalion the Queen's Lancashire Regiment. The post-mortem into Mousa's death found that he suffered more than 90 injuries, including broken ribs, a fractured nose and smashed wrists among many others. He had been subjected to sleep deprivation and had been used in kickboxing "games," where soldiers competed to see how far detainees could be kicked. Although a large number of soldiers were involved in kicking Moussa to death only one, Corporal Donald Payne, was found guilty of involvement in the violence, and that was only because he pleaded guilty before the hearing. Instead the army has suspended 14 soldiers from duty and said that there may be disciplinary action taken. see: http://www.bahamousainquiry.org/report/index.htm and Public Interest Lawyers website: http://www.publicinterestlawyers.co.uk/

We mustn't ignore the fact that British drones kill too, Chris Cole. *The Guardian* 13.5.11. This article, by the founder of Drone Wars UK, is a response to an earlier article by Ken Macdonald ("The Predator Paradox" in *The Guardian* 6.5.11, see *Statewatch* Volume 21 no. 3) that acknowledges that veracity of questioning the "morality and legality of US drone strikes in Pakistan", but points to the "wall of silence" surrounding Britain's use of unarmed aerial vehicles. Cole reports that "between June 2008 and December 2010, more than 124 people were killed by British drones. We know this not because of any ministerial statement, parliamentary question, or Freedom of Information (FoI) request, but because of a boastful, off-the-cuff remark to journalists by the prime minister during his last visit to Afghanistan." Cole argues that "without accountability and scrutiny, without proper information about the circumstances of these strikes, we cannot pretend to be legally or ethically superior to the US in this matter". He calls for the Defence secretary to issue "a full statement to the House of Commons, giving as much detail as possible about Britain's drone strikes. In particular we need to know whether those killed in the strikes were directly participating in hostilities at the time; whether the UK has or would use drones for assassinations of so-called high-value targets; and whether any civilians are known to have been killed or injured by UK drones."

Ground the Drones. *Drone Campaign Network,* 2011, pp. The Drones Campaign Network (DCN) is a UK-based network of organisations, academics and individuals working together in collective action in relation to military drones. This pamphlet documents "the increasing use of unmanned aerial vehicles, commonly known as drones, to undertake armed attacks around the globe. Iraq, Afghanistan, Pakistan, Libya, Yemen and Somalia have all been subject to drone strikes by US or British drones controlled from many thousands of miles away. Palestine is also subjected to drone strikes from Israel." The DCN website: http://www.dronecampaignnetwork.org.uk/

X-ray vision now a possibility for soldiers. *FT Weekend Magazine*, 29.10.11. Researchers at MIT have developed a prototype of a radar system that can see through walls – "which could give soldiers in urban warfare the equivalent of x-ray vision". Although currently very limited in its scope (the system can detect people moving behind eight inches of concrete from 20 feet away), "researchers expect soon to have a more user-friendly display that will show recognisable images". The leader of the university's project is quoted as saying that the technology has been developed "primarily with military applications in mind".

Policing

"Notre vie est en suspens:" Les familles des personnes mortes aux mains de la police attendent que justice soit faite ("Our lives are left hanging:" families of victims of deaths in police custody wait for justice to be done). *Amnesty International,* November 2011, pp. 28. This report casts light on five cases of people from ethnic minority groups who died in police custody in France between 2004 and 2007. These cases illustrate the frequent miscarriages of justice and the impunity enjoyed by the police force, leaving families in despair and with a strong feeling of mistrust against the police and the judicial system. To date, no police officer has been found guilty of misconduct or disproportionate use of force, despite the National Committee on Security Ethics having asked for disciplinary procedures to be taken against some of them. It confirms the discrimination and racial profiling faced by minority groups in France, and documented by research centres as well as Human Rights Watch (see: "*The Root of Humiliation": Abusive Identity Checks in France*, released in January 2012 and available on Human Rights Watch's website). Link to Amnesty International's report: http://www.amnesty.org/en/library/info/EUR21/003/2011/en and http://www.amnesty.org/en/library/asset/EUR21/003/2011/en/9073e684-86cc-4e39-9951-fefbe67d6ce1/eur210032011fr.pdf

Brief History. *I'm a Photographer not a Terrorist* 2011, pp. 24. The I'm a Photographer not a Terrorist (Phnat) network grew from a small group of London-based photographers who covered political protests and found themselves under surveillance by Metropolitan police Forward Intelligence Teams (FIT). This pamphlet documents Phnat's collective response to FIT harassment and the birth of a campaign to defend photographer's rights. The campaign is supported by the National Union of Journalists, The Campaign for Press and Broadcasting Freedom, the British Press Photographer's Association and the London Photographer's Branch. Phnat's website: http://photographernotaterrorist.org/

The Voices of Tottenham are being Marginalised, Stafford Scott. *The Guardian* 17.10.11. Stafford Scott was a co-founder of the Broadwater Farm Defence Campaign, launched in the wake of the 1985 riots on the Tottenham estate, which were provoked by the death of Cynthia Jarrett during a provocative police search of her home in 1985. Scott looks back to the role of former Tottenham MP, Bernie Grant, in preventing further disturbances through working openly with the local community, unlike the "kneejerk reactions from today's politicians." Citing Martin Luther King, saying that riots gave a voice to the voiceless, Scott observes that the voices of those who felt moved to take to the streets following the police shooting of Mark Duggan in August "are still very much unheard." The Tottenham Defence Campaign was launched in October to provide legal support for those who have been arrested and the campaign has a website at: http://tottenhamdefencecampaign.co.uk/

*European Police Science & Research Bulletin***,** Issue 5 (Summer) 2011. This issue of the Bulletin contains an editorial, two research reports, an essay, a conference report, and a selection of upcoming events. Perhaps of most interest is the essay, by Eduardo Ferreira from the *Escola de Polícia Judiciára* in Portugal, entitled 'European Police Cooperation in the future – Reflections from the present'. It is concerned with two main issues – the presumption that "Europe is facing and will continue to face growing common transnational risks or threats", and that "no one is 100% sure" how police cooperation in Europe can or will develop in order to deal with these. Three major obstacles are identified as standing in the way of European police cooperation: judicial issues, judicial-operational issues, and "the (apparent) irrelevance of international police cooperation results to a successful national police career". It will be necessary to overcome these obstacles in order to deal with disasters, threats, risks and horrors – terrorism, crime, trafficking, smuggling, war, natural disasters, industrial accidents, epidemics, and so on. The author concludes tackling this long list of threats and risks will only be done successfully if rewards for successful international cooperation are more integral to the success of police officers in their careers. The article does provide a useful overview of the legal instruments that exist,

and those that are under development, that are intended to enhance police cooperation in Europe. Issue 5 of the bulletin is available at: (http://www.cepol.europa.eu)

Prisons

Traumatization and Mental Distress in Long-term Prisoners in Europe, Manuela Dudeck, Kirstin Drenkhahn, Carsten Spitzer, Sven Barnow, Daniel Kopp, Philipp Kuwert, Harold J. Freyberger and Frieder Dunkel. *Punishment and Society* Volume 13 no. 4 (October) 2011**,** pp. 403-423. The article examines the traumatisation and mental distress of 1,055 male European long-term prisoners from Belgium, Croatia, Denmark, England, Finland, France, Germany, Lithuania, Poland, Spain and Sweden. "In each national sample, more than 50 per cent of the participants were in need of treatment because of psychological symptoms and nearly one third had attempted suicide."

Solitary Confinement must Stop. Scotland Against Criminalising Communities *Press release* 28.11.11. The human rights group Scotland Against Criminalising Communities (SACC) will contact the governments of Britain, USA, France, Germany, Turkey and Australia to ask them to "eliminate long-term solitary confinement and isolation of prisoners." Citing the examples of Babar Ahmad, Talha Ahsan and others, the campaign expresses its opposition to Britain's extradition arrangements with the USA, which provides for "evidence-free extradition to the USA, where prisoner isolation is commonplace." http://www.sacc.org.uk/index.php?option=content&task=view&id=867&catid=27

No way out: a briefing paper on foreign national women in prison in England and Wales. *Prison Reform Trust* (January) 2012, pp. 16. "Foreign national women, many of whom are known to have been trafficked or coerced into offending, represent around one in seven of all the women held in custody in England and Wales. Yet comparatively little information has been produced about these women, their particular circumstances and needs, the offences for which they have been imprisoned and about ways to respond to them justly and effectively." This briefing draws on the work of the charity FPWP Hibiscus, the Female Prisoners Welfare Project to redress the balance. It offers findings and recommendations which could be used to inform a strategy for the management of foreign national women in the justice system.

Review of the medical theories and research relating to restraint related deaths. *Caring Solutions (UK) University of Central Lancashire*, pp. 94, 2011. This report was commissioned by the Independent Advisory Panel on Deaths in Custody and considers research from national and international literature to "ascertain common findings in order to provide guidance for staff on safe and effective restraint techniques in the management of violent and aggressive individuals." The report concludes: "Six of the thirty eight deaths noted in this report involved individuals with pre-existing conditions that may have increased the risk of cardiac arrest: e.g. ischaemic heart disease, diabetes and four people suffered from epilepsy. Sixteen cases had a history of mental illness, specifically psychosis. Positional asphyxia appears to be implicated in at least twenty six deaths (whether or not given as a verdict) because of struggle/physical stressors prior to restraint, number of staff involved and, in particular, because of the length of time of the restraint and position of the individual." Available: http://iapdeathsincustody.independent.gov.uk/wp-content/uploads/2011/11/Caring-Solutions-UK-Ltd-Review-of-Medical-Theories-of-Restraint-Deaths.pdf

Racism and fascism

Razzismo di stato. Stati Uniti, Europa, Italia, Piero Basso (dir.) La Società, Franco Angeli, *Milan*, 2010, pp. 630, €38. A collection of essays that analyses the rise of what it terms "state racism" in the West, with a special emphasis on the situation in Italy. The essays report key developments in the United States, Germany, Great Britain and France, with case studies including the situation in the Calais region, in the Spanish north African enclaves of Ceuta and Melilla, the treatment of Roma people in eastern Europe and the Swiss referendum against minarets. Basso argues that it is mistaken to merely accuse institutions of not doing enough to counter hostility and contempt for migrants or of fomenting these attitudes through incautious initiatives or acts. "Rather, the book's central thesis is that the first propellant for the racist revival that is underway is institutional racism, and its first protagonists are precisely states, governments and parliaments: with their special laws and their public speeches, their arbitrary administrative practices, the racial selection between 'good' nationalities and dangerous ones, obsessive police operations and camps for internment".

Inside the EDL: populist politics in a digital age, Jamie Bartlett and Mark Littler. *Demos* (November) 2011, 54 pages. Unlike the investigative journalism and political actions that undermined the violence and lies spread by the National Front and British National Party in an earlier period, this report surveys the English Defence League (EDL) by examining their supporters' Facebook pages. This "new methodology" eschews the multi-disciplinary practices of anti-fascist activists who successfully acted with and within communities to confront the far-right and drive them from the streets. In this study, Facebook pages are perused and statistically analysed, allowing the authors' to reach the conclusion that: "Although their demonstrations have often involved violence and racist chants, many [EDL] members are democrats who are committed to peaceful protest and other forms of activism."

Security and intelligence

Libyan victims of MI6, CIA rendition to Gaddafi file criminal complaint with British police. Reprieve *Press Release* 17.11.11. Sami al-Saudi, an opponent of the Gaddafi regime who was rendered to the country in 2004 by British intelligence, acting jointly with the CIA and Libya has, along with his family asked London's Metropolitan Police to investigate charges of conspiracy to torture. The press release says: "Evidence of the mistreatment of Mr al-Saadi, his wife, and four children all aged 12 or under at the time emerged earlier this year after documents were found in the wake of the Libyan revolution, showing the UK's key organisational role in the case. Letters were also found showing a close relationship between Moussa Koussa and 'Mark in London', thought to be MI6's Mark Allen.": http://www.reprieve.org.uk/investigations/ukcomplicity/history

Designing for Counter-Terrorism, Dr Jurek J A Tolloczko**.** *Info 4 Security*, 21.9.11. Outlines "the security challenges facing the UK" and "best practice to protect against terrorist attack". Tolloczko, the business manager for defence and security at Tata Steel, notes that the last decade has seen significant focus on ensuring that crowded places are "better protected" from terrorists, often due to the work of government bodies such as the Centre for the Protection of National Infrastructure (CPNI) and the National Counter Terrorism Security Office (NaCTSO), both of whom "provide essential guidance on protecting the UK's most vulnerable and valuable sites and assets, enhancing the UK's resilience to terrorist attack and generally raising awareness of the terrorist threat and how we can prepare for, and protect ourselves, in the event of an attack taking place". Reveals some of the ways in which 'counter-terrorism' ideas have been embedded, to varying degrees, into architecture and construction. Apparently, this is done in part by "Counter Terror Security Advisors (CTSAs) – a nationwide team of police security experts whose purpose is to advise on how best to protect against terrorist, and criminal, attacks." http://www.info4security.com/story.asp?sectioncode=10&storycode=4128108&c=1

The CIA tried to gag me following its 9/11 failures. *FT Weekend* Magazine, 29.10.11. Ali Soufan was an FBI agent who has recently released a book about his time hunting Al Qaeda operatives following the 11 September attacks. The main thrust of the article is that Soufan may have been able to prevent the attacks from taking place, had the CIA been willing to share with the FBI numerous pieces of information it held on suspected Al Qaeda operatives. As a former agent, Soufan was legally obliged to let the FBI and CIA read his manuscript before publication – the CIA "redacted long passages. In the end, it was published with sections blacked out".

CONTENTS

Now Free access to Statewatch European Monitoring and Documentation Centre (SEMDOC):

h*ttp://www.statewatch.org/semdoc*

and Statewatch database: *http://database.statewatch.org/search.asp*

***Statewatch* bulletin is a quarterly Journal.**

It carries features, analyses and viewpoints plus New material - reviews and sources.

Statewatch's work is supported by:

Joseph Rowntree Charitable Trust, Zennstrom Philanthropies, Garden Court Chambers, Friends of Statewatch

and through an operating grant for 2011 from the Education, Audiovisual and Culture Executive Agency.

Statewatch website

http://www.statewatch.org

Contributors

Statewatch, was founded in 1991, and is an independent group of journalists, researchers, lawyers, lecturers and community activists. Statewatch's European network of contributors is drawn from 17 countries.

Statewatch journal
Subscription rates: 4 issues a year: UK and Europe: Individuals and voluntary groups £16.00 pa; Institutions and libraries: £40.00 pa (outside Europe add £4 to the rate)

Published by Statewatch and printed by Russell Press, Russell House, Bulwell Lane, Basford, Nottingham NG6 0BT

Statewatch, PO Box 1516,
London N16 0EW,UK.
Tel: (00 44) 020 8802 1882
Fax: (00 44) 020 8880 1727
e-mail: office@statewatch.org