

CHAPTER 1

What role for what rule of law in EU-US counterterrorism cooperation?

Thorsten Wetzling

The default approach of assuming probity, good faith, constant self-discipline, and deference to formally accepted legal limits on the part of officials acting in secrecy undermines basic democratic principles, defies experience, and mocks the notion of human rights accountability.

Philip Alston

Introduction

Solemn celebrations and expressions of solidarity marked the tenth anniversary of 9/11. The terrorist attacks that occurred on that day killed nearly 3,000 innocent civilians and embodied a grave assault on the fabric of America's democratic life, notably, in the words of Jerzy Bucek, the 'respect for fundamental liberties, human dignity, religious pluralism and justice.'¹ The United States, the European Union and its Member States reacted swiftly to the challenge. 9/11 became a catalyst for the creation of vast homeland security infrastructures in the US and extensive counterterrorism cooperation practices across the Atlantic.

The tenth anniversary of 9/11 calls for a critical review of the anti-terrorist toolkit. This chapter focuses on the compatibility of EU-US counterterrorism practice with the rule of law. The chapter begins with a brief elaboration of the concept and the key norms, institutions and procedures commonly associated with it. It then sketches the current scope and organisation of transatlantic counterterrorism cooperation before arguing that the impressive web of security agencies and institutions now carries an increased risk of 'blowback': as various different actors now connect the dots across different jurisdictions, violations of the rule of law may also entangle a greater number of actors and thus cause greater total damage to the joint counterterrorism effort. Knowing how bureaucratic obstacles to transatlantic intelligence and data-sharing have been overcome or significantly reduced over the past ten years

1. Jerzy Bucek, President of the European Parliament, statement on tenth anniversary of the 9/11 attacks.

also means that the compatibility of EU-US counterterrorism with the rule of law can no longer be solely examined on the basis of the bilateral exchanges between these two entities. Hence, the analysis extends to counterterrorism efforts at the domestic, bilateral and multilateral levels. More concretely, the chapter provides three miniature case studies on selected rule-of-law concerns in current transatlantic counterterrorism practice. Each account documents the general incompatibility of a recent counterterrorism practice with the rule of law and discusses the negative repercussions that it either has already caused or will soon cause on both sides of the Atlantic. It also provides recommendations on the steps necessary to improve the actors' compliance with the rule of law.

What is the rule of law and how does it pertain to counterterrorism?

The term 'rule of law' remains essentially contested in theory and practice.² This chapter cannot account for, let alone debate, the salience of the various different interpretations of the term. Instead, it draws on the work of scholars who have studied the evolution of the term across different political contexts and who have managed to discern what may be called *sine-qua-non* conditions for the rule of law from this process. Important differences notwithstanding, notably between the traditional Anglo-American use of the term which emphasises the judicial process and the traditional continental European tradition which focuses more on the nature of the state,³ three criteria are commonly invoked as the basic ontological foundation of the rule of law concept: a government of laws, the supremacy of the law and equality before the law.⁴

The following definition puts flesh on the bone of these basic criteria without adding unnecessary or contested ideological baggage. It defines the rule of law as:

a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.⁵

The mere existence of fair laws does, of course, not guarantee the rule of law. A specific set of institutions and procedures are also required

2. For an interesting overview, see Simon Chesterman, 'An International Rule of Law?', *American Journal of Comparative Law*, vol. 56, no. 2, Spring 2008, pp. 331-61.

3. *Ibid.*, p. 336.

4. *Ibid.*, p. 342.

5. 'The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies', Report of the UN Secretary-General, doc. S/2004/1616, 3 August 2004.

to monitor adherence to the rule of law in political practice and the provision of effective remedy in case of its violation. The next paragraph summarises the basic processes and institutional architecture that this requires.⁶

First, the counterterrorism agencies ought to engage in internal control procedures themselves (e.g. through intra-agency abuse reporting mechanisms, *ad hoc* inquiries, legal training for individual agents in domestic constitutional law, international humanitarian law and international human rights law). Second, the executive's direction of individual counterterrorism agencies should include control instruments such as oversight boards and the allocation of sufficient funds and human resources for inspector general institutions and regular civil liberties outreach efforts. Third, parliament should consistently exercise independent oversight of counterterrorism practice (e.g. through the passing of laws that define and regulate each actor and its control, by adopting the corresponding budgetary appropriations, by questioning decision-makers on the legality and effectiveness of specific activities and by publishing regular accounts of its oversight activities and findings). Fourth, the judicative branch monitors the use of the special powers (such as surveillance and interrogation practices) of counterterrorism agencies and adjudicates wrongdoing and potential disputes between the different branches of government. Fifth, civil society organisations provide alternative views, disclose scandals and initiate complaints about alleged government malfeasance.

No single layer or institution can bear the sole responsibility for the rule of law in established democracies. Instead, all five layers ought to work simultaneously and proactively towards the defence of the rule of law.

On the scope of counterterrorism cooperation among the US, the EU and its Member States

Following the mantra that 'networked threats require a networked response',⁷ the US, the EU Member States and the supporting EU institutions simultaneously pursue various modes of cooperation across different administrative levels throughout the transatlantic space. Many efforts are thoroughly institutionalised and codified in written agreements, others are more *ad hoc* in character and yet another set of activities hardly register on the public's radar screen. This chapter can only

6. See Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Parliament of Norway, 2005) for further details.

7. Anne-Marie Slaughter, 'Disaggregated Sovereignty: Towards the Public Accountability of Global Government Networks', *Government and Opposition*, vol. 39, no. 2, Spring 2004, pp. 159-90 (p. 160).

sketch the basic contours of present-day transatlantic counterterrorism cooperation.

The 2011 US National Strategy for Counterterrorism calls for ‘a multidepartmental and multinational effort’.⁸ Current transatlantic counterterrorism practice reflects this rather well. The following account is by no means exhaustive but it hopes to further illustrate the wide-ranging and profound levels of interaction across different sectors and jurisdictions.

The primary activity consists of data- and intelligence-sharing among law enforcement agencies,⁹ internal security and intelligence agencies,¹⁰ judicial authorities,¹¹ treasury and trade authorities,¹² border security and transportation authorities.¹³ In addition, one could list regular consultations among diplomatic services to prepare and re-negotiate transatlantic agreements, resolve potential conflict of interests and the mutual exchange of seconded officers to their respective partner agencies on the other side of the Atlantic.¹⁴ Next to the exchange of intelligence and human resources, transatlantic counterterrorism also includes joint operations aimed at the pursuit of identified terrorist networks. Here one can list the coordinated freezing of financial assets and the surveillance and partial or total disruption of their means of online communication.

Given that the main responsibility for the security of EU citizens still lies with the EU Member States and not with the EU’s supporting agencies, whose *de facto* efficiency often ‘depend[s] on the willingness of national services to provide it with information’,¹⁵ the bulk of transatlantic counterterrorism practice still evolves around the ‘good existing bilateral relations between the FBI and CIA (among other agencies) and national police and intelligence services in EU member states’.¹⁶ The current web of transatlantic counterterrorism practice may not constitute a full-blown network but the law enforcement, judicial, intelligence, diplomatic, financial and border security agencies of the US and EU Member States and its supporting EU agencies have come a long way to make joint operations and information sharing less cumbersome.

As documented in the next section, a more seamless interaction across different administrative levels and jurisdictions can also imply negative ramifications for a greater number of actors in case of serious deviations from the rule of law.

8. The document is available online at www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.

9. For example, on the movements, assets, contacts of individuals and networks known to have perpetrated or assisted in terrorist attacks.

10. For example, on the movements, contacts, strategies and assets of a greater number of suspected terrorists and radicals.

11. For example, on information relevant for Mutual Legal Assistance (MLA) and extradition requests.

12. For example, on financial transactions, individual account numbers in accordance with the EU-US Agreement on the Terrorist Finance Tracking Programme (TFTP).

13. On passenger name records.

14. In addition, one could mention peer-review sessions and regular consultations with a broader group of academic and civil society experts to improve existing schemes, for example, on the de-radicalisation initiatives for at-risk youth and lessons for cybersecurity.

15. Kristin Archick, *US-EU Cooperation Against Terrorism*, US Congressional Research Service Report RS 22030, July 2011.

16. *Ibid.*, p. 5.

Sources of concern for the rule of law

It is beyond the scope of this chapter to evaluate the quality of all pertinent counterterrorism laws and to assess the performance of the principal actors in each constitutive layer of the rule-of-law protection in the US, the EU Member States and the EU. Instead, the remainder of this chapter concentrates on three specific ‘problem children’ for rule-of-law protection in transatlantic counterterrorism. Naturally, given this selective focus, the text may only draw limited inferences from these specific cases to the broader spectrum of EU-US counterterrorism cooperation.

Having said this, it is instructive to recall David Cole’s observation that ‘the rule of law may be tenacious when it is supported, but violations of it that go unaccounted corrode its very foundation’.¹⁷ Thus, while a more balanced depiction of ‘compatible’ and ‘incompatible’ counterterrorism practices may be required to substantiate broader claims, it is also true that a few severely misguided counterterrorism practices suffice to discredit the ever-present promise of ‘full respect for our obligations under applicable international and domestic constitutional law’.¹⁸ In the light of the potentially contagious effect of individual rule-of-law deviations on the entire collaborative effort, the actual percentage of incompatible practices among the grand total of transatlantic counterterrorism activities appears secondary.

Each selected case (see the overview table on the next page) focuses on one particular counterterrorism practice and highlights the most pressing rule-of-law issues commonly associated with it. Knowing that laws and conventions can only go so far to ensure the compatibility of political practice with the rule of law, the focus then extends to parliamentary oversight and judicial review. Each miniature study also briefly outlines a transatlantic partner’s reaction to the rule-of-law defence or its forbearance across the pond.

17. David Cole, ‘After September 11: What We Still Don’t Know’, *New York Review of Books*, 29 September 2011.

18. ‘EU-US and Member States 2010 Declaration on Counterterrorism’, 3 June 2010. Available online at: http://www.eu-un.europa.eu/articles/fr/article_9814_fr.htm.

Table 1: Overview of miniature case studies

Level	Practice	Issue	Rule of Law Defender Focus	Cooperation Partner Focus
EU – US CT	Exchange of European SWIFT data to US TFTP	Data Privacy	Europol JSB/ European Parliament	US Congress
EU MS – US CT	Extraordinary rendition	Prohibition of torture	British Parliament & High Court	US Govt
US CT	Capture-or-kill raids	Due Process Right to life	US Congress & US Courts	German Govt

Suppressing terrorist financing through the transmission of SWIFT data

This section concentrates on EU-US cooperation to suppress terrorist financing. More specifically, it looks at the implementation of the June 2010 agreement between the EU and the US on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (hereafter: TFTP Agreement). The TFTP agreement foresees that ‘financial payment messaging and related data stored in the territory of the European Union by providers of international financial payment messaging services [...] are provided to the US Treasury Department for the exclusive purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing’.¹⁹ The agreement attributes a specific role to Europol, namely to check whether requests from the US Treasury Department for SWIFT data comply with the terms of agreement.²⁰

The transmission of sensitive financial data of individuals to foreign governments clearly constitutes an infringement of the right to privacy (Art. 8.1 ECHR and Art. 17.1 ICCPR). Domestic and international law permit derogations from this right only in exceptional circumstances. This may be justified, for example, in the interests of national security and public order. However, this presupposes safeguards to prevent situations where unsubstantiated national security concerns suffice to permit sweeping human right infringements. When drafting a law or contractual agreement, the contracting parties are advised to apply

19. Art. 1.a of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

20. This pertains especially to Art. 4.2 of the TFTP agreement: ‘In particular, the requests [from the US Treasury Department] together with any supplemental documentation, shall: – identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; clearly substantiate the necessity of the data; be tailored as narrowly as possible in order to minimise the amount of data requested [...]’.

the ‘quality of law test’.²¹ In case safeguards are not part of the law or agreement itself, then the text ‘must at least set up the conditions and procedures for interference’.²²

The TFTP agreement entails provisions on ‘safeguards applicable to the processing of data’ (Art. 5), the ‘monitoring of safeguards and controls’ (Art. 12), ‘joint review’ (Art. 13) and ‘redress’ (Art. 18) but the conditions and procedures for interference remain somewhat nebulous. Yet, as indicated, the rule of law cannot be guaranteed through laws only. The focus turns, therefore, to the institutions and procedures that monitor political practice. At the EU level, one such institution is Europol’s Joint Supervisory Board (JSB). It is tasked to review ‘the activities of Europol in order to ensure that the rights of the individual are not violated’ (Art. 34.1 Europol Council Decision).²³

In November 2010, the JSB carried out (with advance notice) an *in situ* inspection to ‘check Europol’s implementation of the TFTP Agreement’.²⁴ While the individual findings of the inspection and the JSB evaluation are classified, it is clear from the public summary of this report that the JSB criticised both the US Treasury Department for making SWIFT data requests that do not fully comply with the terms of the TFTP agreement (criticising especially its insistence on oral instead of written demands for data which precludes any meaningful audit) and Europol’s apparent failure to insist on written requests. The transmittal of European SWIFT data to the US Treasury Department under such conditions is not commensurate with the rule of law.

It is due to the important work of the JSB (executive control) that Europol may soon have better policies in place to ensure that its verification of data requests comply with the terms of the TFTP agreement. The European Parliament (EP) should also be commended for its proactive oversight owing to which better privacy protections were included in the TFTP agreement. The EP first rejected the agreement in February 2010 and only agreed to a revised version, which among other additional caveats gave ‘Europol the authority to approve or reject US Treasury Department requests for SWIFT data’.²⁵ In so doing, the EP has contributed to the defence of the rule of law in the fight against terrorism.

Whether or not Europeans can obtain effective judicial remedy in the US for unlawful infringements of their right to privacy following an unwarranted transmission of SWIFT data remains contested. ‘The US government has long maintained that EU citizens may seek redress concerning US government handling of personal information through agency administrative redress or judicial redress through the US Freedom of Information Act’,²⁶ but given the rather fervent application of the state secret privilege in comparable US proceedings, doubts can be raised about their likely success.

21. Using the case law of the European Court of Human Rights, the quality of a law can be determined by using the following criteria: laws ‘must be adequately accessible and formulated with sufficient precision’ (Sunday Times v UK, 2 EHRR 245, para 47), ‘possess the essential characteristics of foreseeability’ (Silvers and Others v UK, 5 EHRR 347, para 85) and ‘the scope of a discretion must be indicated with reasonable certainty’ (Ibid). See Ian Cameron, *National Security and the European Convention on Human Rights* (Stockholm: Iustus Forlag, 2000).

22. *Klaas v FRG*, No 5029/71, cited also in Born and Leigh, *op. cit.* in note 6, p. 20.

23. Available online at: <http://ec.europa.eu/dgs/olaf/data/doc/Europol.pdf>.

24. A short public version of the report is available online at: www.idpc.gov.mt/dbfile.aspx/TFTP2.pdf.

25. Kristin Archick, *op. cit.* in note 15, p. 7.

26. *Ibid.*

EU Member State complicity in US-led extraordinary rendition

Europol, Eurojust or Frontex are just one of several European counterterrorism partners for the US. Their effectiveness depends largely on the willingness of national European services to provide them with relevant information. The Treaty of Lisbon makes it also 'very clear that Member States of the European Union still have the main responsibility for the security of their citizens; the EU is only supporting its member states'.²⁷ Not surprisingly, several US decision-makers continue to hold the more established and more flexible security partnerships between the US and individual EU Member States in higher esteem.

Much ink has already been spilt over Europe's entanglement in the US-led practice of extraordinary rendition and secret detention of terrorist suspects.²⁸ Despite credible and egregious complicity allegations, few countries felt compelled to honour the rule-of-law principle through rigorous parliamentary and judicial scrutiny. While some countries have thus far failed altogether to formally address grave allegations of government malfeasance, even the more earnest parliamentary inquiries (e.g. Germany's *ad hoc* inquiry committee)²⁹ experienced incapacitating secrecy protection. Most overseers were also unduly credulous in their handling of government reporting and lacked the political will to ask probing questions. The performance of the British Intelligence and Security Committee (ISC) during its *ad hoc* renditions investigation helps to illustrate this point further.

The ISC investigated, among other cases, the allegations made by Binyam Mohamed against the British Security Service. Mr. Mohamed claims that 'he was held by the Pakistani authorities for a period of three months, during which time he was mistreated. He says he was interrogated by British officials'.³⁰ The question arose whether the British authorities knew about this UK resident's torture and whether they failed to come to this man's assistance. The ISC took evidence from the Director General of the British Secret Service and reported that when Mr. Mohamed was interrogated by a British officer in Karachi, the latter 'did not observe any abuse and no instances of abuse were mentioned by [Mr. Mohamed]'.³¹ The report concluded that 'in the cases we have reviewed, the Agencies have taken action consistent with the policy of minimising the risks of torture or CIDT (and therefore "Extraordinary Rendition") based upon their knowledge and awareness of the CIA rendition programme at that time'.³²

By contrast, consider the British High Court's finding on this matter: the Court held, *inter alia*, that Binyam Mohamed 'was transferred to a detention facility in which he was held incommunicado and without

27. Lisa Ginsborg, Martin Scheinin, Mathias Vermeulen, 'European and United States Counterterrorism policies, the rule of law and human rights', *Policy Brief* 2011/2 of the European University Institute's Global Governance Programme.

28. For an important recent contribution, see the Council of Europe's Parliamentary Assembly's Draft Report and Conclusion, *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, 7 September 2011. Available online at: www.assembly.coe.int/CommitteeDocs/2011/State%20secrecy_MartyE.pdf.

29. The Bundestag's *ad hoc* inquiry committee's report (1430 pages) is available in German at: <http://dipbt.bundestag.de/dip21/btd/16/134/1613400.pdf>.

30. Renditions Report of the Intelligence and Security Committee. Available at <http://isc.independent.gov.uk/committee-reports/special-reports>.

31. *Ibid.*

32. *Ibid.*

access to a lawyer, or review by a court or tribunal; that the UK Security Services were aware of this situation; that they continued to facilitate interviews by or on behalf of the United States despite being aware of this situation and that this involvement was far beyond that of a bystander or witness to the alleged wrongdoing'.³³

Reviewing the instruments and mechanisms in defence of the rule of law, it is instructive to know why the British High Court (judicial review) and the British Intelligence and Security Committee (parliamentary oversight) came to such different conclusions. Interestingly, in defence of the unique structure of British intelligence oversight,³⁴ it is often emphasised that the committee's direct access to the intelligence community allows them to 'earn the trust of the agencies' and that this 'enables us to pursue our work more effectively'.³⁵ Redactions in the public version of the ISC report, it has been argued, show that 'we have seen the evidence, are looking at all the information and reaching our conclusion based on the full facts'.³⁶

The Binyam Mohamed case reveals a systemic flaw in an oversight system that relies heavily on trust in the information holder's good faith. The ISC was effectively misled by the British intelligence community when it inquired about their knowledge about Binyam Mohamed's detention in Pakistan. The High Court, on the other hand, was able to establish that the security services were in possession of 42 classified US intelligence documents 'which made clear to anyone reading them that BM was being subjected to the treatment that we have described'.³⁷ Furthermore, it informed the general public about the fact 'that the 42 documents disclosed as a result of these proceedings were not made available to the ISC'.³⁸ Clearly, the ISC had every need to see these documents but failed to be sufficiently probing in terms of the questions it put to its interlocutors in this case. Philip Alston's warning (see the quotation at the beginning of this chapter) thus seems to apply to a broader set of rule-of-law defence mechanisms. Partly influenced by the new information that has come to light about the BM case, the UK government decided to pay him (and 15 other individuals) a considerable amount of compensation. In doing so, it did not admit liability but its assertion that 'there simply is no truth in the claims that the United Kingdom has been involved in rendition' appears even less convincing.³⁹

In this case, the High Court stood up against considerable political pressures from the UK and US government (the latter threatening to review the special relationship between the two countries' intelligence communities) in its rightful defence of the rule of law.⁴⁰ The focus of this case study fell on the United Kingdom yet it is undeniable that other European executives 'permitted, protected and participated in CIA operations which violated fundamental tenets of our systems of

33. R (on the application of Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs [2008] EWHC 2048 (Admin) (21 August 2008), paragraphs 87-88.
34. See, for example, Peter Gill, 'Evaluating Intelligence Oversight Committees: the UK Intelligence and Security Committee and the "War on Terror"', *Intelligence and National Security*, vol. 22, no. 1, pp. 14-37 for a good introduction.
35. Personal interview with an ISC member.
36. Statement made by former UK Foreign Secretary and former Chair of the ISC, Margaret Beckett, during a parliamentary session on 17 July 2008 (Hansard: HC Deb, 17 July 2008, c467).
37. 'The treatment reported, if had been administered on behalf of the United Kingdom, would clearly have been in breach of the undertakings given by the United Kingdom in 1972 [i.e. the UN Torture Convention]. Although it is not necessary for us to categorise the treatment reported, it could readily be contended to be at the very least cruel, inhuman and degrading treatment by the United States authorities.' R v. Foreign Secretary, op. cit. in note 33.
38. *Ibid.*
39. Statement made by former Foreign Secretary Jack Straw before the House of Commons foreign affairs committee in December 2005.
40. According to the diplomatic cables released by Wikileaks, the US government politely asked the German, Italian and Spanish governments to consider the potential negative consequences that too vigorous national rule-of-law defences could have for their respective bilateral relations. See, for example: 'El Masri: CIA drohte dem Kanzleramt', *Berliner Zeitung*, 10 December 2010.

justice and human rights protection'.⁴¹ Unfortunately, 'darkness still enshrouds those who authorised and ran the Black Sites on European territories'.⁴²

The Obama administration 'looks forward and not backward' and faces hardly any credible opposition from the legislative or judicative branch.

Capture-or-kill raids and drone strikes

Most European counterterrorism partners rejoiced when the Obama administration abandoned the term 'war on terrorism'. The fight against terrorism, it seemed, would now be brought into closer proximity with the rule of law. Terrorists suspects are better 'investigated, prosecuted and convicted according to the rules of criminal law'⁴³ than captured, detained, tortured and killed according to unilateral interpretations of the law of war.

While President Obama deserves credit for having abolished the most controversial counterterrorism practice to date (i.e. the 'enhanced interrogation techniques' and the extraordinary rendition of terrorist suspects to secret and indefinite detention), his administration currently relies heavily on two practices that also bode rather poorly for the rule of law: capture-or-kill raids and drone strikes against suspected terrorists by poorly overseen CIA and JSOC operatives in various hotspots around the globe.

'The individuals targeted are alleged terrorists or others deemed dangerous, and their inclusion on what are known as kill-or-capture lists is based on undisclosed intelligence applied against secretive criteria.'⁴⁴

This practice⁴⁵ raises severe doubts on the US's 'full respect for our obligations under applicable [...] domestic constitutional law'.⁴⁶ Philip Alston argues convincingly that the convergence of the CIA (intelligence) and JSOC (military) activities in these raids clearly undermines the effectiveness of the two separate oversight regimes for 'traditional military activities' (Title 10 US Code) and covert intelligence activities (Title 50 US code) in the US constitution. The 'extensive fluidity between the JSOC (DOD) special forces and their CIA counterparts' makes it 'virtually impossible for anyone outside the two agencies to know who is in fact responsible in any given context'.⁴⁷ While there is no room here to spell out the separate oversight regimes for the military and the intelligence services, it should be noted, however, that this intentional double-hatting of CIA and JSOC forces creates *de facto* accountability gaps. These activities often 'escape the scrutiny of the intelligence committees, and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction'.⁴⁸

41. Thomas Hammarberg (Council of Europe Commissioner), 'Ten years of "global war on terror" undermined human rights – also in Europe'. See: http://commissioner.cws.coe.int/tiki-view_blog_post.php?postId=172.

42. Thomas Hammarberg, 'Europeans must account for their complicity in CIA secret detention and torture'. See: http://commissioner.cws.coe.int/tiki-view_blog_post.php?postId=175.

43. Gilles de Kerchove, '10 years – 10 lessons: What our experiences since 9/11 can teach us for the future', *The Hill*, 8 September 2011.

44. Philip Alston, 'The CIA and Targeted Killings Beyond Borders', *Havard National Security Journal* (forthcoming), p. 3.

45. See Greg Miller and Julie Tate, 'CIA Shifts Focus to Killing Targets', *The Washington Post*, 1 September 2011; Charlie Savage, 'Secret US Memo Made Legal Case to Kill a Citizen', *The New York Times*, 8 October 2011; Eric Schmitt and Thom Shanker, *Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda* (New York: MacMillan, 2011).

46. EU-US and Member States 2010 Declaration on Counterterrorism, op. cit. in note 18.

47. Philip Alston, op. cit. in note 44, p. 52.

48. Alfred Cumming, 'Covert Action: Legislative Background and Possible Policy Questions', *Congressional Research Service Report RL33715*, p. 9. See also: Marcy Wheeler, *The Gang of Four Doesn't Have Access to the Kill List*. See: www.emptywheel.net.

A ranking member of the US House of Representatives Permanent Select Committee on Intelligence, Dutch Ruppersberger, recently admitted that he did not ‘really have access to that list’⁴⁹ (in fact, there are several different lists) of individuals, including American citizens, doomed to be ‘taken out’ by US special forces. The enormous secrecy surrounding the raids and their preparatory proceedings in the National Security Council not only debilitates effective oversight, it is also doubtful whether the inclusion of individuals on those capture/kill lists can be legally challenged and whether any effective judicial remedy can be obtained *ex post facto* (refer to Alston’s concrete list of judicial obstacles). In short, this practice raises numerous questions as regards its compatibility with the basic transparency and accountability requirements required by both domestic and international law.

Naturally, this affects the broader practice of transatlantic counterterrorism, too. Following the lethal drone strike against a German citizen in Pakistan, the

‘German Interior Ministry has issued new, more restrictive rules and has instructed the BfV [Bundesverfassungsschutz – Germany’s domestic intelligence agency] to stop providing the Americans with current information that would make it possible to determine the location of German citizens in geographical contexts that may not be successfully defined as armed conflicts or war. [e.g. the current night raids and drone strikes in Pakistan, Yemen and Somalia]’⁵⁰

Conclusion

Good laws do not suffice to guarantee the adherence to the rule of law in political practice. The three miniature case studies of this chapter cast doubt on the proposition that the respect for the rule of law is ‘fundamental in the national and international effort in the fight against terrorism’.⁵¹ The 2010 EU-US Declaration on Counterterrorism acknowledged ‘the need to adopt measures to address [...] the absence of the rule of law’⁵² but the unchallenged insistence on oral communications (first case), credulous deference to the security establishment (second case), and double-hatting practice (last case) demonstrate that good intentions will not suffice. At times even severe violations of the rule of law remain unchallenged.

Naturally, this poses a dilemma for the EU and its Member States. On the one hand, the EU benefits tremendously from its extensive counterterrorism cooperation with the US and wishes to secure the smooth continuation of this cooperation. On the other hand, it has committed itself to a robust defence of the rule of law and knows that its power

49. Quoted in Marcy Wheeler, *ibid.*

50. Robert Chesney, ‘Der Spiegel Claims Germany Withholds Intel on Militants Who Might Be Drone Strike Targets’. Available at: www.lawfareblog.com/2011/05/der-spiegel-claims-germany-withholds-intel-on-militants-who-might-be-drone-strike-targets.

51. EU-US and Member States 2010 Declaration on Counterterrorism, *op. cit.* in note 18.

52. *Ibid.*

stems largely from the credibility of this defence. The latter is not a mere legal obligation, it also ensures vital support from domestic and international partners and helps to erode the ideological foundation of terrorist networks.

The dilemma is, of course, not entirely new but honest discussions about the conflicting interests and how to best address them in concrete political practice are rare.⁵³ The severity of rule-of-law violations that some transatlantic counterterrorism practices entail are seldom the subject of formal discussions, let alone official policy documents.

As the EU and the US move into another decade of intense counterterrorism cooperation, they are well advised to pay greater attention to the potentially grave negative ramifications that some of their misguided policies might have. For example, the current JSOC/CIA night raids and drone strike campaign outside of declared zones of conflict defies hard-earned provisions of international law and may thus cause a universal regression of this important international tool of conflict resolution. A thin-skinned or lukewarm defence of the rule of law by European national parliaments and courts can also have grave negative ramifications for the credibility of European Security Sector assistance in other parts of the world. Rather than apologising for the more assertive oversight role of the European parliament, the European partners should value the fact that this important layer of rule of law defence has not become entirely dysfunctional.

53. For an interesting discussion of the policy options for the EU, see Annegret Bendiek, 'An den Grenzen des Rechtsstaates: EU-USA Terrorismusbekämpfung', *SWP Studie S 3*, February 2011. Available online at: www.swp-berlin.org. Bendiek argues effectively for 'grey-zone management'.