Published in J. D. Ohlin, K. Govern & C. Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, 2015).

Cyberterrorism and Enemy Criminal Law

Stuart Macdonald

School of Law

Swansea University

Introduction

Since the events of 9/11 commentators have debated the appropriate legal framework for responding to the threat of terrorism. Some, like the Bush Administration, advocated a military response. Others argued that, whilst terrorism should be distinguished from warfare, the gravity of the contemporary terrorist threat justifies exceptional or emergency measures which operate outside of the normal legal framework and/or are temporally limited.[1] Still others urged the importance of a criminal justice based response in which the criminal law is deployed to prosecute suspected terrorists.[2] One of the principal arguments in favour of the latter approach is that it has greater moral authority and is more protective of human rights. The criminal law requires the state to prove its case in open court beyond reasonable doubt and gives the suspect the opportunity to respond to the case against him.

As the contributions to this volume show, those responding to the growing threat of cyberattacks also face this choice between different legal frameworks. This chapter contributes to this debate by providing a critical assessment of the UK's criminal justice based response to the threat of cyberterrorism. The chapter will show that, in fact, the different legal frameworks are not mutually exclusive. In recent years the UK has introduced a range of terrorism-related legislation. This has not only significantly extended the criminal law's reach, so that it encompasses both a wide range of preparatory activities and individuals who are only loosely connected to a feared attack. It has also indirectly diminished the procedural rights of suspected terrorists and provides for the imposition of severe sanctions which are rooted in a precautionary approach based on potential future harms. These are all marked departures from the normal standards of the criminal law and so, it will be argued, may be understood as the convergence of the criminal justice and exceptional measures approaches: in other words, as a form of enemy criminal law. The chapter argues that it is contradictory – and, ultimately, self-defeating – to insist on a criminal justice based framework without adhering to the features which give the criminal law its moral authority in the first place.

The inclusion of cyberattacks within the UK's definition of terrorism

Increasing attention is being paid to the threat of cyberattack. In November 2013 the heads of the FBI, Department of Homeland Security and National Counterterrorism Center told Congress that cyberattacks are likely to eclipse 9/11-style terrorist attacks as a domestic danger over the next

[1] Some well-known examples include: Bruce Ackerman, *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism* (Yale University Press 2006); Richard A Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (Oxford University Press 2006); Oren Gross and Fionnuala Ní Aoláin, *Law in Times of Crisis: Emergency Powers in Theory and Practice* (Cambridge University Press 2006).

[2] See for example David Bonner, *Executive Measures, Terrorism and National Security: Have the Rules of the Game Changed?* (Ashgate 2007); David Cole and Jules Lobel, *Less Safe Less Free: Why America is Losing the War on Terror* (The Free Press 2007); Conor Gearty, 'The Superpatriotic Fervour of the Moment' (2008) 28 OJLS 183; Gary Lefree and James Hendrickson, 'Build a Criminal Justice Policy for Terrorism' (2007) 6 Criminology & Pub Pol'y 781.

decade.[3] These attacks, they predicted, will come from individual actors as well as nation states.[4] Analysis of the Stuxnet malware – which damaged centrifuges at the Natanz uranium enrichment facility in Iran – has concluded that it could be used as a blueprint for cyber-physical attacks in the future. These would most likely focus on targets which are easier to attack, such as critical infrastructure installations, and importantly would not require nation-state resources.[5]

Warnings of the threat posed by cyberterrorism are not new. In 1997 Barry Collin of the US Institute for Security and Intelligence stated that the potential for multiple casualties and considerable publicity are likely to make cyberattacks desirable to terrorist groups. He gave the examples of contaminating food products through interference with manufacturing processes and the interception of air traffic control systems to engender fatal collisions.[6] Weimann has identified a total of five reasons why terrorists might choose to launch cyberattacks: comparatively lower financial costs; the prospect of anonymity; a wider selection of available targets; the ability to conduct attacks remotely; and, the potential for multiple casualties.[7] Related utility maximisation arguments suggest it is inevitable terrorists will employ cyber weaponry if benefits from doing so are likely,[8] and/or if an enemy employs computers and networks as security tools or maintains dominance in this area.[9] Indeed, in a recent survey of the global research community 58% of respondents stated that cyberterrorism poses a significant threat, with a further 12% saying that it may potentially become one.[10]

The UK Government considered the threat of cyberterrorism as part of its review of the definition of terrorism in the late 1990s. As part of this review, it published a consultation paper in 1998 which proposed a new statutory definition of terrorism.[11] This document rejected Lord Lloyd's earlier suggestion that the UK adopt the working definition of terrorism then in use by the FBI.[12] One of the Government's criticisms of the FBI's definition was that cyberattacks perpetrated by terrorists fell outside of its scope. The Government stated that such attacks might not only 'result in deaths and injuries', but also 'result in extensive disruption to the economic and other infrastructure of this country'.[13] To illustrate the last of these, the Government offered the example of contamination of a public utility system such as a water or sewage works.

The resultant definition can be found in section 1 of the Terrorism Act 2000. For an act to qualify to as terrorist, it must satisfy three criteria. First, one of five specified actions must have either been used or threatened. These are: serious violence against a person; serious damage to property; endangering another person's life; creating a serious risk to public health or safety; or, the focus of this chapter, actions which are 'designed seriously to interfere with or seriously to disrupt an

---

[3] Spencer Ackerman, 'Cyber-attacks eclipsing terrorism as gravest domestic threat – FBI' *The Guardian* (London, 14 November 2013) <http://www.theguardian.com/world/2013/nov/14/cyber-attacks-terrorism-domestic-threat-fbi> accessed 29 November 2013.

[4] 'Cyberattacks more serious domestic threat to U.S. than terrorism' (*Homeland Security News Wire*, 20 November 2013) <http://www.homelandsecuritynewswire.com/dr20131120-cyberattacks-more-serious-domestic-threat-to-u-s-than-terrorism-fbi> accessed 29 November 2013.

[5] Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (The Langner Group 2013).

[6] Barry Collin, 'The Future of Cyberterrorism' (1997) 13 *Crime and Justice International* 15.

[7] Gabriel Weimann, *Cyberterrorism: How Real is the Threat?* (Special Report 119, United States Institute of Peace 2004) <http://www.usip.org/sites/default/files/sr119.pdf> accessed 29 November 2013.

[8] Steven Simon and Daniel Benjamin, 'America and the New Terrorism' (2000) 42 Survival 59.

[9] Jerrold M Post, Kevin G Ruby and Eric D Shaw, 'From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism' (2000) 12 Terrorism and Political Violence 97.

[10] Lee Jarvis, Stuart Macdonald and Lella Nouri, 'The Cyberterrorism Threat: Findings from a Survey of Researchers' (2014) 37 Studies in Conflict & Terrorism 68.

[11] Home Office, *Legislation Against Terrorism: A Consultation Paper* (Cm 4178, 1998).

[12] Lord Lloyd of Berwick, *Inquiry into Legislation Against Terrorism* (Cm 3420, 1996).

[13] Home Office, *Legislation Against Terrorism* (n 11) para 3.16.

electronic system'.[14] Second, the action (or threat) must have been designed either to influence the government or an international governmental organization, or to intimidate the public or a section of the public.[15] Third, the action (or threat) must have been made for the purpose of advancing a political, religious, racial or ideological cause.[16] The application of the definition is not limited to the UK; it applies equally to actions outside the UK, to people and property outside the UK and to foreign governments.[17]

The UK's definition unquestionably has a broad scope.[18] In respect of cyberattacks, it is not limited to attacks on critical infrastructures. Attacks on anything deemed to be an electronic system could potentially qualify (such as a Distributed Denial of Service (DDoS) attack).[19] Moreover, the attack need not actually cause serious interference or disruption. It is enough that it was designed to. This far-reaching definition is expanded still further by the fact that it: applies to threats of cyberattacks as well as actual attacks; applies to cyberattacks which are designed merely to influence, not intimidate, a government; applies equally to all governments, however oppressive; and, contains no exemption for political protest or self-determination.[20]

For present purposes what is most important about the UK's definition is that it treats cyberterrorism as a subset of the broader category of terrorism, in spite of possible qualitative differences between cyberterrorism and traditional, physical forms of terrorism.[21] By so doing, it grants access to the full panoply of terrorism-related investigative powers, procedures, criminal offences and sentencing powers in any case involving a cyberterrorist attack that falls within the broadly couched statutory definition. The UK has thus sought to respond to the threat of cyberterrorism by using criminal laws and processes – as opposed to the law of war or emergency powers – just as it has done for traditional terrorism. The remainder of this chapter evaluates this criminal justice based response.

Enemy criminal law as a descriptive concept

The concepts of 'enemy criminal law' (*Feindstrafrecht*) and 'citizen criminal law' (*Bürgerstrafrecht*) were first advanced by the German professor of criminal law, Günther Jakobs.[22] Intended as ideal-types, the aim of these concepts was to draw attention to two contrasting tendencies within the criminal law (as opposed to two isolated spheres of criminal law).[23]

According to Jakobs, since trust alone is not a sufficient basis for individuals in society to engage with one another the role of law is to enable interaction. But law can only perform this function if

[14] Terrorism Act 2000, s 1(2).
[15] Terrorism Act 2000, s 1(1)(b). If the relevant action involved the use of firearms or explosives it is unnecessary to show that section 1 (1)(b) is also satisfied (s 1(3)).
[16] Terrorism Act 2000, s 1(1)(c).
[17] Terrorism Act 2000, s 1(4).
[18] The breadth of the definition was criticised by the Supreme Court in *R v Gul* [2013] UKSC 64, [2013] 3 WLR 1207 [28]-[29], [33]-[37], [61]-[64]. See also Keiran Hardy and George Williams, 'What is "Terrorism"?: Assessing Domestic Legal Definitions' (2011) 16 UCLA J Int'l L & For Aff 77, 111-20.
[19] Terrorism Act 2000, s 1(2)(e).
[20] Keiran Hardy and George Williams, 'What is Cyberterrorism? Computer and Internet Technology in Legal Definitions of Terrorism' in Tom Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism: Understanding, Assessment and Response* (Springer 2014).
[21] Lee Jarvis and Stuart Macdonald, 'What is Cyberterrorism? Findings from a Survey of Researchers' (2014) Terrorism & Political Violence <http://www.tandfonline.com/doi/pdf/10.1080/09546553.2013.847827> accessed 1 July 2014.
[22] Jakobs presented his theory at a major conference held in Berlin in 1999: G Jakobs, 'Selbstverständnis der Strafrechtswissenschaft vor den Herausforderungen der Gegenwart (Kommentar)' in A Eser, W Hassemer and B Burkhardt (eds), *Die Deutsche Strafrechtswissenschaft vor der Jahrtausendwende* (Beck 2000).
[23] Günther Jakobs, 'Bürgerstrafrecht und Feindstrafrecht' [2004] HRR-Strafrecht 88.

members of society believe that legal norms are generally recognized and respected. Citizens (a term which Jakobs uses synonymously with persons[24]) are therefore expected to cultivate loyalty to the law. This 'anchors the expectations of fellow members of the polity that the law will generally be followed, thereby enabling them to run their lives, if not in total security, at least without constant worry about being wronged'.[25] When a citizen commits a crime, the validity of the applicable law is called into question. Punishment is a counter-response which reinforces the loyalty to the law of both the offender (by forcefully reminding him of his duties as a citizen) and members of society in general (by reaffirming the law and making it clear that the conduct is unacceptable).

Citizen criminal law is therefore communicative. It assumes that the offender remains a loyal citizen and that the offending behaviour was a lapse which he now regards as a mistake, and so continues to address him as a 'person-in-law'.[26] By contrast, enemy criminal law is directed at individuals whose conduct manifests that they do not respect the validity of the legal system and no longer consider themselves bound by the law. Since these individuals do not provide others with this minimum level of cognitive reassurance, the legal system no longer regards them as citizens or persons but rather as a source of danger. Terrorists are the paradigmatic example of a non-citizen, because the terrorist lacks not only the requisite loyalty to law but also the interest in acting according to it.[27] Other possible examples include sexual predators, organized crime and drug dealers.

It follows that enemy criminal law is concerned not with communication or censure, but with management of risk. The enemy is one who demonstrates by his conduct that he can no longer minimally guarantee that he will conduct himself as a loyal citizen. Enemy criminal law therefore imposes sanctions not as retrospective punishment for past wrongdoing but prospectively in order to prevent future harms.

As well as the change in discourse (waging war against an enemy), Jakobs identifies three principal features of enemy criminal law. This section of the chapter outlines these features and argues that all three are apparent in the UK's raft of terrorism criminal offences.

Pre-inchoate liability

Few would deny that the criminal law has a preventive, as well as a punitive, function. As Ashworth and Zedner observe, 'If a certain form of harmful wrongdoing is judged serious enough to criminalize, it follows that the state should assume responsibility for taking steps to protect people from it'.[28] Indeed, as Duff remarks, 'a law that condemned and punished actually harm-causing conduct as wrong, but was utterly silent on attempts to cause such harms, and on reckless risk-taking with respect to such harms, would speak with a strange moral voice'.[29] Most legal systems accordingly have the general inchoate criminal offences of encouraging/inciting crime, conspiracy and attempt. These offences have a preventive role, penalizing conduct before any harm actually occurs. What marks out enemy criminal law, however, is that it criminalizes conduct at a far earlier, pre-inchoate, stage.

[24] In contrast to some other accounts which also employ the concept of citizenhood: see further Markus D Dubber, 'Citizenship and Penal Law' (2010) 13 New Crim LR 190.
[25] Daniel Ohana, 'Trust, Distrust and Reassurance: Diversion and Preventive Orders Through the Prism of *Feindstrafrecht*' (2010) 73 MLR 721, 724.
[26] ibid 724.
[27] Dubber, 'Citizenship and Penal Law' (n 24).
[28] Andrew Ashworth and Lucia Zedner, 'Prevention and Criminalization: Justifications and Limits' (2012) 15 New Crim LR 542, 543.
[29] RA Duff, *Criminal Attempts* (Clarendon Press 1996), 134.

In the UK, it has been deemed necessary to supplement the ordinary inchoate offences in terrorism cases. Although there have been some high profile convictions,[30] the offences of conspiracy and encouraging crime are notoriously hard to prove. Obtaining admissible evidence of an agreement or words of encouragement within secretive organizations is difficult, particularly given the UK's ban on the use of intercept as evidence in criminal trials.[31] Moreover, even if admissible evidence is obtained it may lack evidential value (many members of terrorist organizations observe good communications security and disguise the content of their communications) or there may be public interest reasons for not disclosing it (perhaps because it would expose other on-going investigations or reveal sensitive techniques or capabilities).[32] Meanwhile, the offence of criminal attempts has a limited reach. Narrower in scope than the US Model Penal Code's 'substantial step' test, the test in the UK is whether the defendant committed an act that was 'more than merely preparatory' to commission of the planned offence.[33] In other words, a defendant does not commit a criminal attempt until he actually 'embarks upon the crime proper'.[34] Given the level of risk and severity of the potential harm in terrorism cases, there are strong reasons to (in the words of the UK's Independent Reviewer of Terrorism Legislation) 'defend further up the field'.[35] This is the role of the pre-inchoate – or precursor – terrorism offences.

There are a large number of terrorism precursor offences in the UK, found predominantly in the 2000 and 2006 Terrorism Acts. These penalize a wide range of preparatory activities, including: fund-raising for terrorist purposes;[36] use or possession of money or other property for terrorist purposes;[37] possession of an article for terrorist purposes;[38] collecting information or possessing a document likely to be useful to a terrorist;[39] training for terrorism;[40] attendance at a place used for terrorist training;[41] and, the catch-all offence of preparation of terrorist acts.[42] In recent years this expanding use of the criminal sanction has received much attention from criminal law theorists.[43] As well as raising concerns about possible overreaching and the impact on human rights and rule of law values, this literature has offered possible principled justifications for these offences.[44] Wörner has suggested that the group-danger rationale that underpins the general offence of conspiracy could

[30] Including Abu Hamza's conviction for soliciting to commit murder and the convictions of seven men on conspiracy charges in the airline liquid bomb plot case.
[31] For discussion of the ban on intercept evidence, see Stuart Macdonald, 'Prosecuting Suspected Terrorists: Precursor Crimes, Intercept Evidence and the Priority of Security' in Lee Jarvis and Michael Lister (eds), *Critical Perspectives on Counter-terrorism* (Routledge 2014).
[32] Home Office, *Privy Council Review of Intercept as Evidence: Report to the Prime Minister and the Home Secretary* (Cm 7324, 2008).
[33] Criminal Attempts Act 1981, s 1(1).
[34] *R v Gullefer* [1990] 1 WLR 1063.
[35] David Anderson QC, 'Shielding the Compass: How to Fight Terrorism Without Defeating the Law' [2013] EHRLR 233, 237.
[36] Terrorism Act 2000, s 15.
[37] Terrorism Act 2000, s 16.
[38] Terrorism Act 2000, s 57.
[39] Terrorism Act 2000, s 58.
[40] Terrorism Act 2006, s 6.
[41] Terrorism Act 2006, s 8.
[42] Terrorism Act 2006, s 5.
[43] See for example AR Duff, L Farmer, SE Marshall, M Renzo and V Tadros (eds), *The Boundaries of the Criminal Law* (Oxford University Press 2010); AP Simester and A von Hirsch, *Crimes, Harms, and Wrongs: On the Principles of Criminalisation* (Hart Publishing 2011); Ashworth and Zedner, 'Prevention and Criminalization: Justifications and Limits' (n 28); GR Sullivan and I Dennis (eds), *Seeking Security: Pre-Empting the Commission of Criminal Harms* (Hart Publishing 2012).
[44] For an alternative perspective that preparatory acts should not, in general, be criminalized but regulated using a system of civil orders, see Daniel Ohana, 'Responding to Acts Preparatory to the Commission of a Crime: Criminalization or Prevention' (2006) 25 Criminal Justice Ethics 23.

also apply to many of the terrorism precursor offences. When a defendant provides weapons, training manuals or practical advice his behaviour ceases to be part of his '*internum*' and becomes part of the '*externum*'.[45] His behaviour may endanger others and, crucially, he is no longer able to control what happens next. An alternative, subjectivist, justification is provided by Simester and von Hirsch. They explain that the principal difficulty with imposing criminal liability on 'remote harms' (actions which do not themselves directly cause harm to others, such as collecting information, possessing items or raising funds) is that the feared eventual harm is contingent upon some other person or the defendant himself choosing to behave in a particular way in the future. They argue that to hold someone responsible now for the possible future acts of others is contrary to the fundamental right to be treated as autonomous individuals who are distinctively responsible for their own actions, whilst to hold someone responsible now for their own possible future actions is to undermine their autonomy and treat them as being incapable of deliberation and self-control.[46] Criminal liability for remote harms can therefore only be justified, they argue, if the defendant 'in some sense affirms or underwrites' the subsequent choice to cause harm.[47] They name this the principle of normative involvement: if a defendant endorses the potential future harmful actions of either himself or another, responsibility for the future harm may fairly be imputed to him.

These principled justifications provide a useful yardstick for evaluating the scope of the existing raft of terrorism precursor offences. What is readily apparent is that some of the offences overreach.[48] An example is the offence of collecting information or possessing a document likely to be useful to a terrorist. Not only does this offence not require any proof that the defendant had shared the information or document so that it was no longer under his exclusive control. It also requires no proof whatsoever of a terrorist connection or purpose. As a result, in *R v G*[49] the House of Lords upheld the conviction for this offence of a man who, whilst in custody for non-terrorism offences, collected information on explosives and bomb-making and left it in his cell for a guard to find. The defendant was a paranoid schizophrenic who, it was accepted, wanted to antagonize the prison staff because he believed that they had been whispering about him. In a case like this one, the effect of this offence is to 'make a terrorist out of nothing'.[50]

It is also important to point out that proof of normative involvement should be regarded as a necessary, but not a sufficient, condition for criminalization. There may be reasons not to enact an offence even if its terms do require proof that the defendant intended to commit, or had normative involvement in, future terrorist acts. An example is the offence of preparation of terrorist acts. A defendant commits this offence if he engages in 'any conduct' with an intention to commit or assist acts of terrorism.[51] Any form of conduct could potentially be penalized by this offence if carried out with the requisite intention. Simester offers the example of an individual who eats muesli for breakfast as part of a fitness programme in preparation for a terrorist act.[52] Where the conduct charged is something innocuous, the authorities will need to find some other evidence that the individual performed the act with the necessary intention. This could result in intrusive methods of policing. There is also the danger that the offence will be enforced in a discriminatory manner, with

[45] Liane Wörner, 'Expanding Criminal Laws by Predating Criminal Responsibility – Punishing Planning and Organizing Terrorist Attacks as a Means to Optimize Effectiveness of Fighting Against Terrorism' (2012) 13 German LJ 1037, 1052.
[46] Simester and von Hirsch (n 43) 80-81.
[47] Ibid 81.
[48] See further Carlile and Macdonald, 'The Criminalization of Terrorists' Online Preparatory Acts' in Tom Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism: Understanding, Assessment and Response* (Springer 2014).
[49] [2009] UKHL 13, [2010] 1 AC 43.
[50] Jacqueline Hodgson and Victor Tadros, 'How to Make a Terrorist Out of Nothing' (2009) 72 MLR 984.
[51] Terrorism Act 2006, s 5(1).
[52] AP Simester, 'Prophylactic Crimes' in GR Sullivan and I Dennis (eds), *Seeking Security: Pre-Empting the Commission of Criminal Harms* (Hart Publishing 2012).

certain groups feeling compelled to forgo some innocent behaviour for fear it may be misconstrued. Furthermore, there are numerous other precursor offences which already criminalize various specific forms of preparatory activity. The guidance notes which accompanied the legislation failed to identify any gaps that needed to be plugged.[53] So it is unclear whether this catch-all offence is in fact necessary.

The UK's terrorism precursor offences not only extend the temporal reach of the criminal law. They also encompass a wider range of individuals, penalizing those with an associative or facilitative role as well as potential perpetrators and accessories.[54] It reaches this wider range of individuals in four ways. First and foremost, there are a number of offences which target those with a supporting role, including: membership of a proscribed organization;[55] support for a proscribed organization;[56] encouragement of terrorism;[57] and, dissemination of terrorist publications.[58] Second, these offences not only target acts which facilitate terrorist attacks, but also acts which facilitate the assistance or encouragement of terrorist attacks. So, for example, it is not only an offence for D1 to provide training to D2 with an intention that D2 will use the skills to commit a terrorist act. It is also an offence for D1 to provide training to D2 with an intention that D2 will use the skills to assist someone else (D3) to commit a terrorist act.[59] Third, it is possible to commit many of the terrorism precursor offences in inchoate form. It is an offence, for example, to conspire to engage in conduct that is preparatory to an act of terrorism.[60] Fourth, in certain circumstances the law governing inchoate offences allows one layer of inchoate liability to be layered upon another (so-called double inchoate liability). When these four features are combined, the potential reach of the precursor offences becomes clear. Together, they mean that it is an offence for an individual (D1) to intentionally encourage someone else (D2) to intentionally encourage someone else (D3) to cause someone else (D4) to publish a statement which indirectly encourages someone else (D5) to instigate someone else (D6) to commit an act of terrorism.[61] Ordinarily, individuals who are several steps removed from the harm-causing conduct would be regarded as too remote to fall within the scope of the criminal law.

The imposition of severe sanctions

The second feature of enemy criminal law is the imposition of severe punishment. The rationale underlying these sanctioning powers is not the retributivist notion of communication and censure, but risk control. As a result, the sentences imposed for preparatory offences may be the same as those imposed for an attempt to cause the harm in question:

> [P]unishment is imposed uniformly, irrespective of the stage of apprehension prior to consummation of the offence, notwithstanding the principle that sanction severity should be commensurate with the blameworthiness of the actor as determined by the actual progress made toward the realisation of the criminal endeavour.[62]

[53] Available via <www.legislation.gov.uk >accessed 21 November 2013.
[54] Lucia Zedner, 'Terrorizing Criminal Law' [2012] CLPH <http://link.springer.com/article/10.1007/s11572-012-9166-9> accessed 21 November 2013.
[55] Terrorism Act 2000, s 11.
[56] Terrorism Act 2000, s 12.
[57] Terrorism Act 2006, s 1.
[58] Terrorism Act 2006, s 2.
[59] Terrorism Act 2006, s 6(1).
[60] Criminal Law Act 1977, s 1(1); Terrorism Act 2006, s 5(1).
[61] Serious Crime Act 2007, s 44; Terrorism Act 2006, s 1. Sections 44-46 of the Serious Crime Act 2007 create three separate offences. The form of double inchoate liability described in the text is only available in respect of the section 44 offence of intentional encouragement or assistance (see section 49 and Schedule 3).
[62] Ohana, 'Trust, Distrust and Reassurance' (n 25) 726.

The UK's terrorism precursor offences carry severe sentencing powers. Of the eleven terrorism precursor offences already mentioned in this chapter, two have a maximum sentence of seven years' imprisonment,[63] five a maximum of ten years,[64] two a maximum of fourteen,[65] one a maximum of fifteen[66] and the other a maximum of life imprisonment.[67] In recent years there have been a number of successful prosecutions for these offences.[68] In order to illustrate the potential severity of the sanctions, three of these cases will be outlined.

First, the case of *R v Worrell*.[69] In this case the police found a significant quantity of racist and right-wing material in the defendant's flat, including books, DVDs and Nazi memorabilia. The books included manuals on weapons and bomb-making. Officers also found some sodium chlorate, weed killer, matches, lighter fuel and fireworks. The defendant therefore had instructions on how to make an improvised explosive device and some of the materials necessary for their manufacture. At trial he was convicted of possession of articles for terrorist purposes[70] (an offence which, it should be noted, requires a reasonable suspicion that the defendant intended to use the items for terrorism-related activity[71]) and was sentenced to six years' imprisonment.[72] At his appeal against sentence the Court of Appeal acknowledged that the defendant was not part of a conspiracy or terrorist cell, that he had not actually manufactured an explosive device or attempted to do so and that there was no evidence that any attack was actually planned or imminent. The Court nonetheless upheld the sentence of six years, pointing out that these considerations had been taken into account by the sentencing judge and that in cases where a defendant's plan has progressed further the offence is punishable by up to fifteen years' imprisonment. A similar case to this one is *R v Tabbakh*.[73] In this case the police searched the defendant's flat and found three bottles, fertilizer and other chemicals, together with hand-written bomb-making instructions. Although the defendant had collected the correct ingredients, they were of a poor grade and would not in fact have exploded. He also had yet to make or obtain a detonator. At trial he was convicted of preparation of terrorist acts[74] and sentenced to seven years' imprisonment. The Court of Appeal dismissed his appeal against sentence, pointing out that although the bomb was not a viable one the maximum sentence for this offence is life imprisonment.

Second, *R v Karim*.[75] The defendant in this case had come to the UK from Bangladesh to study microelectronics. In 2006 he settled in the country with his wife and son, both of whom were British. In 2007 he began working at British Airways as a graduate IT specialist. In 2009 Karim's younger brother went to Yemen, contacted the notorious Jihadist Anwar al-Awlaki and put him in contact

[63] Terrorism Act, ss 1 and 2 (encouragement of terrorism and dissemination of terrorist publications).
[64] Terrorism Act 2000, ss 11, 12 and 58 (membership of a proscribed organization, support for a proscribed organization and collecting information or possessing a document likely to be useful to a terrorist); Terrorism Act 2006, ss 6 and 8 (training for terrorism and attendance at a place used for terrorist training).
[65] Terrorism Act 2000, ss 15 and 16 (fund-raising for terrorist purposes and use or possession of money or other property for terrorist purposes).
[66] Terrorism Act 2000, s 57 (possession of an article for terrorist purposes).
[67] Terrorism Act 2006, s 5 (preparation of terrorist acts).
[68] All successful prosecutions for terrorism-related offences are detailed on the website of the Counter-Terrorism Division of the Crown Prosecution Service. See <http://www.cps.gov.uk/publications/prosecution/ctd.html> accessed 27 November 2013.
[69] *R v Worrell* [2009] EWCA Crim 1431, [2010] 1 Cr App R (S) 27.
[70] Terrorism Act 2000, s 57.
[71] *R v Zafar* [2008] EWCA Crim 184, [2008] QB 810.
[72] He was also convicted on a separate count of racially aggravated intentional harassment, alarm or distress. For this offence he was sentenced to fifteen months' imprisonment to be served consecutively, giving a total sentence of seven years and three months.
[73] *R v Tabbakh* [2009] EWCA Crim 464, (2009) 173 JP 201.
[74] Terrorism Act 2006, s 5.
[75] *R v Karim* [2011] EWCA Crim 2577, [2012] 1 Cr App R (S) 85.

with Karim. Once al-Awlaki discovered that Karim worked for British Airways, he asked him about his knowledge of security and air travel. Karim responded by suggesting either a physical or electronic attack on British Airways computer servers. He also said that he might be able to get a package on-board a plane. When al-Awlaki discovered that Karim wanted to leave the UK and go and fight in Yemen, al-Awlaki told him that he would be of more use if he remained in the UK. At trial, Karim was convicted on four counts of preparation of terrorist acts.[76] The sentencing judge held that the sentence for these offences (twenty-four years) should be served consecutive to the sentence for an earlier period of activity in which Karim had sent money to help mujahideen in Pakistan/Afghanistan, produced a video in support of a terrorist organization and possessed a computer file containing instructions on making improvised explosive devices.[77] So in total Karim was sentenced to thirty years' imprisonment, with a further five year extension to be added to his licence period. At his appeal against sentence Karim's counsel argued that the sentence was excessive because Karim had not 'gone far down the road'.[78] He had not actually set about doing anything concrete, and he might never have done anything. The Court of Appeal rejected this argument and upheld Karim's sentence. Whilst accepting that Karim might never have gone on to commit the acts he intended to commit, the Court said that this case was 'quite different' from other cases which involve 'detailed planning by outsiders':

> The gravamen of the case against this appellant was that he was in a position, and was told from the e-mails in January 2010 to remain in position in the front line so he would be able to carry out from the inside acts of terrorism. It seems us to us that someone in that position is someone who has gone very, very far down the route, and the fact that he has not actually started to put together the paraphernalia for bombing, but has maintained a position where he can act at once, puts him in a category of someone who has overtly committed himself to the probability of committing really serious acts of terrorism. Comparison with the other cases is therefore unjustified, in the sense that it was not necessary to show overt acts, or preparing bombs or the like. It was sufficient that he was a 'sleeper'; he had maintained employment where he was in a position to act immediately.[79]

Third, *R v Gul*.[80] The defendant in this case was a Law student at a reputable University in London who, it is believed, radicalized himself over the Internet. When police searched his home they found videos on his laptop which he had uploaded to various websites including YouTube. The videos included martyrdom videos and ones which showed attacks on Coalition forces in Iraq and Afghanistan by insurgents. At trial he was convicted on five counts of disseminating a terrorist publication[81] and sentenced to five years' imprisonment. Gul's appeal against conviction focussed on whether the insurgents' actions in the videos fell within the UK's statutory definition of terrorism (with the Court holding that they do). Although he also sought leave to appeal against sentence, this was refused by the Court of Appeal.[82] The Court noted the defendant's young age, previous good character and the serious consequences for him for the rest of his life, but stressed the manner in which the videos glorified and encouraged attacks on UK forces overseas. A similar example is the conviction of Craig Slee on four counts of disseminating a terrorist publication.[83] Slee was sentenced to five years for posting videos on Facebook of al-Qaeda beheading captives. The sentencing judge explained that, whilst Slee had no links to any terrorist organizations and no plans to engage in any

[76] Terrorism Act 2006, s 5.
[77] *R v Karim* (n 75) [9].
[78] ibid [27].
[79] ibid [31].
[80] *R v Gul* [2013] UKSC 64, [2013] 3 WLR 1207.
[81] Terrorism Act 2006, s 2.
[82] *R v Gul* [2012] EWCA Crim 280, [2012] 1 WLR 3432.
[83] 'Craig Slee jailed for posting beheading videos on Facebook' (*BBC News*, 18 January 2013) <http://www.bbc.co.uk/news/uk-england-21090488> accessed 27 November 2013.

attack planning, the videos that Slee had distributed had been created in order to encourage people to rally to the terrorist cause.[84]

In their discussion of terrorism precursor offences, de Goede and Graaf suggest that terrorism trials may be understood as a performative space in which 'potential future terror is imagined, invoked, contested, and made real, in the proceedings and verdict, as well as through its wider media and societal echoes'.[85] As the preceding paragraphs illustrate, this potential future may be one of a multiplicity of possible futures, and need not be a probable future. On the one hand, a repentant Gul expressed regret at his actions,[86] the courts acknowledged that Slee had no terrorist connections or plans to commit an attack, that there was no evidence that Worrell was planning an attack, that Tabbakh's bomb was not viable and that Karim might never have gone on to commit the acts he intended. On the other hand, the courts simultaneously stressed that the videos Gul and Slee posted might have encouraged others to commit terrorist acts, that Worrell had been stopped before he had been able to go further along the road to perpetrating a terrorist act, that Tabbakh was doing his best to make a viable bomb and that Karim was a sleeper agent who might have been utilized by al-Awlaki in the future. The imagining of potential futures thus provides a space for the 'incorporation of precautionary counterterrorism into criminal law'.[87] This is just one example of the broader shift in criminal justice towards a pre-crime society,[88] a society which Zedner describes as one 'in which the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done'.[89] It is for this reason that Krasmann argues that enemy criminal law is in fact 'not about criminal law, it marks rather a new paradigm of security policy'.[90]

A reduction in defendants' procedural rights

The third feature of enemy criminal law is a reduction in the procedural rights of defendants. A stark example in the US is the trial of Guantanamo detainees by military commissions. By contrast, since 9/11 the UK Government has not generally sought to introduce modifications to the criminal trial itself. In Northern Ireland, 'Diplock Courts' were introduced in 1973 in response to a report submitted to Parliament which addressed the problem of dealing with Irish republicanism through means other than internment.[91] These courts consisted of a single judge, with the right to trial by jury suspended and a number of special rules as to pre-trial processes, evidence and punishment. But whilst Diplock Courts were common in the 1970s and 1980s in terrorism cases in Northern Ireland, they were abolished by the Justice and Security (Northern Ireland) Act 2007 and replaced with a new system of non-jury trial which only applies in exceptional circumstances.[92] Moreover,

---

[84] Information obtained from <www.thelawpages.com> accessed 27 November 2013.
[85] Marieke de Goede and Beatrice de Graaf, 'Sentencing Risk: Temporality and Precaution in Terrorism Trials' (2013) 7 International Political Sociology 313, 314.
[86] 'Islamic terrorist propaganda student Mohammed Gul jailed' (*BBC News*, 25 February 2011) <http://www.bbc.co.uk/news/uk-england-london-12576973> accessed 28 November 2013.
[87] Marieke de Goede and Beatrice de Graaf, 'Sentencing Risk: Temporality and Precaution in Terrorism Trials' (2013) 7 International Political Sociology 313, 327.
[88] Jude McCulloch and Sharon Pickering, 'Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror"' (2009) 49 Brit J Criminology 628.
[89] Lucia Zedner, 'Pre-Crime and Post-Criminology?' (2007) 11 Theoretical Criminology 261, 262.
[90] Susanne Krasmann, 'The Enemy on the Border: Critique of a Programme in Favour of a Preventive State' (2007) 9 Punishment & Society 301, 302.
[91] Secretary of State for Northern Ireland, *Report of the Commission to Consider Legal Procedures to Deal with Terrorist Activities in Northern Ireland* (Cm 5185, 1972). See further WL Twining, 'Emergency Powers and the Criminal Process' [1973] Crim LR 406.
[92] See for example Henry McDonald, 'Brian Shivers found guilty of Massereene murders' *The Guardian* (London, 20 January 2012) < http://www.theguardian.com/uk/2012/jan/20/brian-shivers-guilty-massereene-murders> accessed 1 July 2014.

Diplock Courts were not introduced in the rest of the UK. And whilst since 2003 courts across the UK have had a general power to order a non-jury trial in cases where there is a 'real and present danger' of jury tampering,[93] to date this power has only been used once. The defendants in this case were charged with the armed robbery of £1.75m from Heathrow Airport, not with terrorism offences.[94]

Whilst the criminal trial itself has not been modified, however, there are two respects in which the procedural rights of suspected terrorists have been indirectly diminished. The first is the wording of many of the terrorism precursor offences. As Tadros has explained, 'The fairness of a trial cannot be detached from the fairness of the offences which provide the basis of argument'.[95] Not only does the UK's statutory definition of terrorism have a very wide ambit.[96] The conduct identified by the definitions of many of the terrorism precursor offences is also specified in broad terms, such as collecting any information of a kind likely to be useful to a terrorist,[97] providing instruction in the use of any method for doing anything that is capable of being done for terrorist purposes,[98] possession of any property,[99] and even simply 'any conduct'.[100] Such broad definitions potentially render criminal law safeguards, particularly the beyond reasonable doubt standard of proof, 'toothless'.[101] Procedural safeguards have little bite when offence definitions are so broad that almost all citizens fall within them.

The breadth of many of the precursor offences has led Edwards to label them 'ouster offences'.[102] He explains that there is a discrepancy within these offences between the offence definition and the wrong that is being targeted. The offence of encouragement of terrorism,[103] for example, was targeted at extremists who promote a culture of hate, but is broad enough to also encompass North Korean exiles who criticize their native regime and those 'like Cherie Blair, who express their ability to understand the actions of Palestinian suicide-bombers'.[104] This is not analogous to offences that prohibit all possession of weapons – i.e., offences of necessitous over-inclusion – since those offences seek to guide all citizens away from possessing weapons even if their doing so would pose no risk. Terrorism precursor offences, on the other hand, do not seek to guide all citizens away from all of the conduct they encompass. Instead they operate as a 'facilitation device'.[105] Only some of those who fall within the offence definition will be selected for prosecution. It seems fair to assume that this choice will to a large extent be based on whether the individual is deemed to pose a threat to national security. But at trial the issue will be whether the requirements set out in the offence definition are satisfied. The national security considerations that led to the decision to prosecute will sit in the background. So 'Even though the pursuit of security is central to the justification for the law itself, it is not open to challenge by the defendant with respect to his particular case'.[106] The effect is to deprive the trial court of the opportunity to adjudicate on the actions that the offence is targeting. Whilst this might lighten the prosecutorial burden, it undermines the courts' ability to deliver procedural justice.

---

[93] Criminal Justice Act 2003, s 44.
[94] *R v Twomey, Blake, Hibberd and Cameron* [2011] EWCA Crim 8, [2011] 1 WLR 1681.
[95] Victor Tadros, 'Justice and Terrorism' (2007) 10 New Crim LR 658, 677.
[96] Terrorism Act 2000, s 1.
[97] Terrorism Act 2000, s 58(1)(a). The House of Lords subsequently narrowed the scope of this offence but stating that, whilst the information need not only be useful to a terrorist, it must be such that it calls for an explanation: *R v G* [2009] UKHL 13, [2010] 1 AC 43.
[98] Terrorism Act 2006, s 6(3)(b).
[99] Terrorism Act 2000, s 16(2)(a).
[100] Terrorism Act 2006, s 5(1).
[101] Tadros, 'Justice and Terrorism' (n 95), 675.
[102] James Edwards, 'Justice Denied: The Criminal Law and the Ouster of the Courts' (2010) 30 OJLS 725, 732.
[103] Terrorism Act 2006, s 1.
[104] Edwards, 'Justice Denied' (n 102), 730.
[105] Ibid 729.
[106] Tadros, 'Justice and Terrorism' (n 95), 688.

The second way in which defendants' procedural rights have been diminished is by the use of Terrorism Prevention and Investigation Measures (TPIMs). Introduced in 2011 as a replacement for the Control Order regime, TPIMs are designed for use against individuals who are believed to be involved in terrorism-related activity where there is no prospect of successful prosecution or deportation.[107] Although they are not as onerous as Control Orders,[108] they may still impose a range of obligations and restrictions.[109] These include: restrictions on travel and on places the individual may visit; restrictions on the individual's use of financial services and electronic communication devices; restrictions on whom the individual may associate and communicate with; a requirement to report to a police station at specified times; electronic monitoring of the individual's movements; and, a requirement that the individual reside at specified premises overnight.[110] Two conditions must be satisfied for TPIMs to be imposed: first, the Home Secretary must reasonably believe that the individual is, or has been, involved in terrorism-related activity; and, second, the Home Secretary must reasonably consider that TPIMs are necessary in order to protect the public from a risk of terrorism. This latter condition has an obvious resonance with Jakobs' account of enemy criminal law. Instead of focussing on punishing past actions of the individual, the test is forward-looking: are TPIMs necessary to protect the public from offending behaviour in the future. As Ohana explains, this implies that the authorities are expected to gauge the individual's capacity and commitment to abide by the law:

> Were the competent authority to find that the actor is suitably disposed to steer himself as a responsible law-abiding citizen, then the making of a preventive order would not be called for: the actor could be trusted to act appropriately, without there being a need to monitor his conduct by setting special restrictions which do not apply to other citizens.[111]

As one would expect given that TPIMs are intended for use in cases where prosecution is not a viable option,[112] the procedure for imposing TPIMs differs from the ordinary criminal process. First of all, TPIMs are imposed by the Home Secretary not the courts.[113] Although the Home Secretary must apply for the courts' permission before imposing TPIMs (save in urgent cases[114]), the courts' function at the permission hearing is simply to determine whether the Home Secretary's decision to issue TPIMs is 'obviously flawed'.[115] Moreover, the permission hearing may take place in the absence of the individual, without the individual having had an opportunity to make representations to the court and/or without the individual having been notified of the application.[116] Once the TPIMs notice has been served on the individual a review hearing must be held 'as soon as reasonably

---

[107] Home Office, *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (Cm 8123, 2011), ch 4.
[108] The two principal differences are that TPIMs ended the use of forced relocation and they have a maximum duration of two years (save in cases where fresh evidence comes to light). Control Orders lasted for one year, but there was no limited on how many times they could be renewed. The longest period for which someone was subject to a Control Order was 55 months (David Anderson QC, *Control Orders in 2011: Final Report of the Independent Reviewer on the Prevention of Terrorism Act 2005* (The Stationery Office 2012), para 3.47).
[109] Terrorism Prevention and Investigation Measures Act 2011, s 3.
[110] Terrorism Prevention and Investigation Measures Act 2011, sch 1.
[111] Ohana, 'Trust, Distrust and Reassurance' (n 25) 745.
[112] Prosecution may not be considered viable either because there is no realistic prospect of conviction or because prosecution would be contrary to the public interest (perhaps because the evidence against the suspect is of a sensitive nature): Crown Prosecution Service, *The Code for Crown Prosecutors* (7th ed., CPS Communication Division 2013).
[113] For an argument that TPIMs should be issued by the courts, see Stuart Macdonald, 'The Role of the Courts in Imposing Terrorism Prevention and Investigation Measures: Normative Duality and Legal Realism' [2013] CLPH <http://link.springer.com/article/10.1007%2Fs11572-013-9255-4> accessed 26 November 2013.
[114] Terrorism Prevention and Investigation Measures Act 2011, s 3(5).
[115] Terrorism Prevention and Investigation Measures Act 2011, s 6(3)(a).
[116] Terrorism Prevention and Investigation Measures Act 2011, s 6(4).

practicable'.[117] Here the court reviews the Home Secretary's decision that the conditions for issuing TPIMs were and continue to be met, applying the 'principles applicable on an application for judicial review'.[118] The court has the power to quash the TPIMs notice or specified measures within it and the power to direct the Home Secretary to revoke the TPIMs notice or modify specified measures within it.[119] In order to ensure that information is not disclosed contrary to the public interest, the court may exclude the individual and his legal representative from all or part of the proceedings[120] – although the House of Lords has ruled that Article 6 of the European Convention on Human Rights (the right to a fair trial) requires that an individual is always given 'sufficient information about the allegations against him to enable him to give effective instructions in relation to those allegations'.[121] During the closed sessions the interests of the individual are represented by a Special Advocate.[122] Before the closed materials are served the Special Advocate may communicate freely with the individual and his legal representative. Once the Special Advocate has been served, however, he may not communicate with either the individual or his lawyer[123] (save in certain limited situations which are rarely utilized in practice[124]). This restriction on communication between Special Advocates and those whose interests they represent has been strongly criticised, with one Special Advocate even suggesting that it renders their efforts 'pretty hopeless'.[125] Yet notwithstanding the fact that TPIMs are imposed on a reduced standard of proof and the individual may not have seen all of the evidence against him, breach of a TPIMs notice without reasonable excuse is a criminal offence punishable by up to five years' imprisonment.[126] This hybrid civil-criminal procedure (which has been employed in a number of different contexts in the UK[127]) has been likened to a Trojan horse[128] and described as 'an ingenious scheme for imposing harsh punishments yet by-passing the appropriate protections at the crucial stage of the proceedings'.[129]

TPIMs also have the potential to circumvent the criminal law in a second way: authorities might choose to rely on TPIMs in cases where it would have been possible to prosecute. Although the UK's counterterrorism strategy states that suspected terrorists should be prosecuted 'wherever possible',[130] the Terrorism Prevention and Investigation Measures Act 2011 does not require the courts to review the decision not to prosecute. Instead the Act imposes a requirement that before imposing TPIMs the Home Secretary must first consult with the police about the possibility of prosecution,[131] with an additional obligation to keep the individual's conduct under review with a

[117] Terrorism Prevention and Investigation Measures Act 2011, s 8(5).
[118] Terrorism Prevention and Investigation Measures Act 2011, s 9(2).
[119] Terrorism Prevention and Investigation Measures Act 2011, s 9(5).
[120] Civil Procedure Rules, r 80.18.
[121] *Secretary of State for the Home Department v AF & another* [2009] UKHL 28, [2010] 2 AC 269 [59] (Lord Phillips).
[122] Civil Procedure Rules, r 80.20.
[123] Civil Procedure Rules, r 80.21.
[124] One of the special advocates has explained: 'The position therefore remains that Special Advocates can communicate with the controlled person only with the permission of the court and that applications for permission must be made on notice to the Secretary of State. Such permission is very rarely sought. In practice, it would be very likely to be refused because any question that it would assist the Special Advocates to ask is likely to be one from which part of the closed case could be inferred' (Martin Chamberlain, 'Special Advocates and Procedural Fairness in Closed Proceedings' (2009) 28 *Civil Justice Quarterly* 314, 322).
[125] Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights (Eighth Report): Counter-Terrorism Bill* (HC 2007-08, 199) para 67.
[126] Terrorism Prevention and Investigation Measures Act 2011, s 23.
[127] Ian Dennis, 'Security, Risk and Preventive Orders' in GR Sullivan and Ian Dennis (eds), *Seeking Security: Pre-Empting the Commission of Criminal Harms* (Hart Publishing 2012).
[128] Editorial, 'In Favour of Community Safety' [1997] Crim LR 769, 770.
[129] Andrew Ashworth and Jeremy Horder, *Principles of Criminal Law* (7th ed., Oxford University Press 2013) 43.
[130] Home Office, *CONTEST* (n 107) para 1.16.
[131] Terrorism Prevention and Investigation Measures Act 2011, s 10(1).

view to prosecution for the duration of the TPIMs notice.[132] Having examined the cases of the ten men subject to TPIMs at the end of 2012, however, the Independent Reviewer of Terrorism Legislation found no 'undue reticence' to prosecute on the part of the police, Crown Prosecution Service or MI5.[133] Indeed, four of the ten men had previously been prosecuted for terrorism-related activity and in each case the jury had chosen not to convict. The Independent Reviewer commented:

> There is certainly an uncomfortable feel to the imposition of TPIMs on acquitted persons. The practice is however troubling not because it constitutes an abuse of the TPIM system, but because it reveals an unpalatable truth: that while it should always be the first and preferable option for dealing with suspected terrorists, the criminal justice system – whose open nature may prevent some relevant national security evidence from being used – is not always enough to keep the public safe.[134]

Interestingly, the Independent Reviewer went on to say that in his experience (corroborated by other studies) the imposition of TPIMs has not generated feelings of resentment amongst Muslim communities, even though all ten of the men that were subject to TPIMs at the end of 2012 were Muslims.[135] This appears to be because TPIMs have so far been used with restraint. He accordingly went on to warn that 'the situation could rapidly change if TPIM notices begin to be used on a significantly greater scale, or against less apparently dangerous targets, than has been the case to date'.[136]

Enemy criminal law as a prescriptive concept

The concepts of citizen criminal law and enemy criminal law have great value as explicatory and analytical tools. But Jakobs' account of enemy criminal law was also intended to be prescriptive.[137] He argued:

> Whoever does not provide sufficient cognitive reassurance of a law-abiding behaviour, not only cannot expect to be treated as a person by the State, but the State itself should not treat him as such, because if it does so, the State would be harming the right to security to which other persons are entitled. Hence it would be a terrible mistake to demonize what we are calling here 'enemy criminal law'.[138]

Whilst adding that too much enemy criminal law can damage the rule of law, Jakobs argued that if enemy criminal law is carefully disaggregated from citizen criminal law it can in fact preserve the integrity of the latter. This section of the chapter disputes this claim and advances four countervailing considerations which militate against the use of enemy criminal law. This is not to reject terrorism precursor offences, consequentialist sentencing or adapted, specially protective, criminal trials outright. There is a pressing need for criminal law theorists to evaluate whether, how and to what extent these may be justified.[139] Rather, the argument is that terrorism-related criminal

[132] Terrorism Prevention and Investigation Measures Act 2011, s 10(5)(a).
[133] David Anderson QC, *Terrorism Prevention and Investigation Measures in 2012: First Report of the Independent Reviewer on the Operation of the Terrorism Prevention and Investigation Measures Act 2011* (The Stationery Office 2013) 61.
[134] ibid 62.
[135] ibid ch 11.
[136] ibid para 11.17.
[137] On the distinction between ideal-types and ideals see Stuart Macdonald, 'Constructing a Framework for Criminal Justice Research: Learning from Packer's Mistakes' (2008) 11 New Crim LR 257.
[138] Quoted in Carlos Gómez-Jara Díez, 'Enemy Combatants versus Enemy Criminal Law' (2008) 11 New Crim LR 529, 536.
[139] For examples of some of the work done so far, see n 43.

laws and processes should not be regarded as existing in a separate realm where the ordinary rules and principles do not apply.

First, the empirical basis for the claim that enemy criminal law can secure the (cognitive) requirements for the legal system to exist is uncertain at best. Gómez-Jara Díez uses systems theory to explain that the criminal law not only presupposes the existence of conditions that the criminal law itself is incapable of securing, but that 'to the extent that the State uses enemy criminal law to secure citizen criminal law it risks the whole existence of the latter'.[140] In a similar vein, Melía states that there is no empirical basis for thinking that the existence of harsh terrorism offences will 'deter more or more efficiently than the use of a less draconian criminal law'.[141] Similar criticisms have been levelled at the popular balancing metaphor: there is no empirical basis for the over-simplistic assumption that sacrificing liberty will automatically result in enhanced security.[142]

Second is a danger that Jakobs himself adverted to, the possibility of enemy criminal law permeating into and contaminating citizen criminal law. Zedner, for example, has warned that whilst the introduction of exceptional measures is often controversial, 'once enacted they become accepted and, over time, percolate down into the everyday criminal law'.[143] This has been echoed by Melía:

> Thus, if such draconian measures creep into what has typically been considered legitimate and normal criminal laws, they may generate significant changes in which the logic of enemy criminal law slowly but surely contaminates our system of criminal law until it becomes the norm rather than the exception.[144]

An example in the UK is the expansion in the use of Special Advocates. Introduced by the Special Immigration Appeals Commission Act 1997, Special Advocates were originally only used in appeals in immigration and asylum cases where the Home Secretary's decision was based on national security concerns.[145] In the years since then Special Advocates have been deployed in numerous others contexts – including the Proscribed Organisations Appeal Commission,[146] the Pathogens Access Appeal Commission,[147] Employment Tribunals[148] and Parole Board hearings,[149] as well as TPIMs review hearings (as explained previously) – culminating in the Justice and Security Act 2013, which provides for the use of closed sessions in *any* civil proceedings before the High Court, Court of Appeal or Supreme Court where this is required in the interests of national security and the fair and effective administration of justice.[150]

Third, enemy criminal law adopts a relativistic approach to substantive and procedural rights which is at odds with the universality of human rights.[151] On this approach, human rights become conditional. They are not vested in the individual by virtue of their personhood, but have to be

[140] Díez, (n 138) 533.
[141] Manuel Cancio Melía, 'Terrorism and Criminal Law: The Dream of Prevention, the Nightmare of the Rule of Law' (2011) 14 New Crim LR 108, 114.
[142] Stuart Macdonald, 'Why We Should Abandon the Balance Metaphor: A New Approach to Counterterrorism Policy' (2008) 15 ILSA J Int'l & Comp L 95; Stuart Macdonald, 'The Unbalanced Imagery of Anti-Terrorism Policy' (2009) 18 Cornell J L & Pub Pol'y 519; Jeremy Waldron, 'Security and Liberty: The Image of Balance' (2003) 11 J Pol Phil 191; Lucia Zedner, 'Securing Liberty in the Face of Terror: Reflections from Criminal Justice' (2005) 32 J L & Soc 507.
[143] Lucia Zedner, 'Security, the State, and the Citizen: The Changing Architecture of Crime Control' (2010) 13 New Crim LR 379, 394.
[144] Melía, 'Terrorism and Criminal Law' (n 141) 112.
[145] John Ip, 'The Rise and Spread of the Special Advocate' [2008] PL 717.
[146] Terrorism Act 2000, sch 3.
[147] Anti-terrorism, Crime and Security Act 2001, sch 6.
[148] Employment Tribunals Act 1996, s 10.
[149] *R (Roberts) v Parole Board* [2005] UKHL 45, [2005] 2 AC 738.
[150] Justice and Security Act 2013, s 6.
[151] Mireille Delmas-Marty, 'Violence and Massacres – Towards a Criminal Law of Inhumanity?' (2009) 7 JICJ 5.

earned through loyalty to the law. Since the conditions for singling out citizens are so vaguely defined, this is capable of generating its own form of insecurity: anxiety that one's human rights might be suspended. The alternative is to insist that human rights are absolute:

> Arguably the criminal law is better protected by insisting upon the citizenship status of those against whom criminal proceedings are brought; by maintaining, through the presumption of innocence, that they are law-abiding members of society until proven guilty; and by adhering to the protections of the criminal process even in the gravest case.[152]

Closely connected to this is the final danger, that enemy criminal law will undermine the criminal law's moral authority. To apply a diminished level of human rights protection to a specific group of people when many members of that group come from particular ethnic minorities is to risk undermining the legitimacy of Government both domestically and overseas.[153] Moreover, as Fletcher argues, the discourse of loyalty and community is exclusionary. He states that enemy criminal law 'intensifies the perception of insiders and outsiders', thereby returning us 'to the most primitive way of handling criminals – expulsion, excommunication, and banishment'.[154] The UK's counterterrorism strategy emphasizes the importance of social inclusion in preventing radicalization.[155] As this suggests, enacting exclusionary laws which generate resentment and ill-feeling is likely to prove counter-productive.

Conclusion

In the concept of enemy criminal law the 'exceptional measures of the war on terror are legalized and incorporated into criminal law'.[156] Using the concept as an analytical aid, this chapter has highlighted: the extensive reach of the UK's raft of terrorism precursor offences; how potential futures and a precautionary desire to mitigate risk lead to the imposition of severe sentences on those convicted of these crimes; and, how the procedural rights of those accused of these offences have been indirectly diminished. As concern grows over the possibility of terrorists launching cyberattacks, and policymakers and legislators assess how best to respond to this threat, it is important to be mindful of the counter-productivity of enemy criminal law. Not only is there a danger that such laws will contaminate other parts of the criminal law and the legal system more generally, but the exclusionary discourse and relativistic conception of human rights are likely to generate resentment and ill-feeling amongst those communities most affected. Ultimately, it is self-defeating to create new offences, procedures and sentencing powers which undermine the criminal law's moral authority when this moral authority is the very reason for insisting that suspected terrorists should be prosecuted whenever possible in the first place.

[152] Zedner, 'Security, the State, and the Citizen' (n 143) 392.
[153] David Cole, *Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism* (New Press 2003).
[154] George P Fletcher, *The Grammar of Criminal Law*, vol 1 (Oxford University Press 2007), 172.
[155] Home Office, *CONTEST* (n 107) para 5.17.
[156] de Goede and de Graaf, 'Sentencing Risk' (n 85) 328.