I. Crime Scenes and the Terroir of Terror

The latter decades of the twentieth century and now the first decade of the twenty-first century have seen considerable changes in the ethical challenges we face. Many of those changes have been technologically driven. Technologies that enable people to be kept physiologically alive have posed new and difficult questions about the time, timing and circumstances of the end of life. Other technological developments have posed new questions at the beginning of life concerning the potential use of gene enhancement therapies, cloning and the emergence of personhood. Technological developments have also done much to overcome what the historian Geoffrey Blainey spoke of as "the tyranny of distance". Blainey wanted to argue that Australia's distance (from Europe in particular) had dramatically shaped its history, but his artfully chosen phrase also characterizes a wider phenomenon that has been largely eliminated. We can travel between countries in a matter of hours rather than days, weeks or even months. We can also communicate almost instantaneously with those in far places. The means for rapid travel and communication have, moreover, made possible the development of multinational corporations, cartels, and networks that are more powerful than the countries in which they are situated – posing distinct regulatory and ethical challenges to national and global governance structures.

With such developments have come the transnationalization and globalization of some of the less-attractive aspects of human society – crime and terrorism. The events of September 11, 2001 (9/11) did not occur in a vacuum, but they managed – for reasons that we need not pursue here – to refocus attention on the transnational and global character of much that is problematic in Western, liberal democratic societies. Although we might legitimately wonder whether there are really any "good guys" in our present global situation, the simple fact of the matter is that much of crime and terrorism is no longer local or multinational but transnational and international. Even though Westphalian borders remain in place, and indeed function as critical and oftentimes problematic elements in global politics, they no longer present impenetrable or controlled barriers to outsiders.[1] For many purposes, the passport that needs to be shown if A travels

1 Contemporary doctrines of national sovereignty tend to go back to the Peace of Westphalia, 1648. State sovereignty is one of the factors that makes the problem of developing global standards so difficult. See Michael Walzer, *Just and Unjust Wars* (1977). For a few recent contributions to the debate, see Omar Dahbour, "Advocating Sovereignty in an Age of Globalization", *Journal of Social Philosophy* 37, no. 1 (2006): 108–26; Joelle Tanguy, "Redefining Sovereignty and Intervention", *Ethics and International Affairs*, 17, no. 1 (2003): 141–48; Michael Dusche, "Human Rights, Autonomy and National Sovereignty", *Ethical Perspectives,* 7, no. 1 (2000): 24–36.

to X from Y to see B can be circumvented by the Skype call, email or other online transaction that A can make with B. The bomb or weapons that need to be physically transported across borders may not cause as much devastation as the computer virus or hacked website that is remotely controlled. Crime and terrorism have exploited the porosity of borders, along with the opacity that encryption and other technological advances have made available.

The advent of global terrorism has created an additional problem to that posed by porous boundaries. Global terrorism, like all terrorism, stands somewhere between crime and war. Countries that have been confronted by it have had to make difficult decisions about how to deal with it. Those involved in the first terrorist attack on the Twin Towers of the World Trade Center in 1993 were treated as though they had committed a number of serious crimes – including seditious conspiracy, explosive destruction of property and interstate transportation of explosives. Their intentions were to topple one of the towers against the other, with a view to bringing both down – arguably a more radical plan than that adopted by the terrorists on September 11, 2001, who appear to have seen the actual collapse of the towers as an unexpected bonus. However, what occurred on September 11 was treated as something much closer to an act of war, leading to the US invasion of Afghanistan. Given that there was some connection between those who plotted the first attack on the Twin Towers and those who were involved in the second, what made for the difference? Was it that the second attack included other targets besides the Twin Towers? Was it the death toll? Admittedly, the events of 1993 already raised questions about the sufficiency of law enforcement strategies for dealing with terrorism.[2] Nevertheless, terrorism seems to occupy a broad space between crime and war, intersecting with each and thus blurring once-clear conceptual boundaries. We tend to think of crimes as serving the personal interests of those who perpetrate them; war, on the other hand, is politically motivated as one state seeks to take control of the affairs of another. But Timothy McVeigh's (and Terry Nichols's) terroristic destruction of the Alfred P. Murrah Building in Oklahoma City, though politically motivated, was treated as a crime, as was the first World Trade Center bombing. Terrorism does not clearly constitute war either, even though it is usually politically motivated. If we generally think of war as armed conflict between states, terrorism does not clearly constitute an act of war. There is no standing army to fight or head of state with whom to negotiate.

2 See Dale Watson, "Foreign Terrorists in America: Five Years After the World Trade Center" (Senate Judiciary Committee), February 24, 1998, available at: http://fas.org/irp/congress/1998_hr/s980224w.htm. See also Seumas Miller, *Terrorism and Counter-terrorism: Ethics and Liberal Democracy* (Oxford: Blackwell, 2010), ch. 5.

This is not the place to engage in an extended discussion of what constitutes terrorism.[3] Perhaps it is enough for our purposes to say that terrorism seeks to further some political or politico-religious end, using, as the name implies, indiscriminate violence to intimidate a people. Unlike war, which may also involve terror – though not generally as a strategy – terrorism does not usually constitute armed conflict between jurisdictionally bound political communities.[4]

What we designate as crimes are generally jurisdictionally defined. That is, the designation of "doing φ" as a crime applies only in country P, though country Q may in some cases also designate "doing φ_1", an act similar to φ, as a crime. That will commonly be the case with respect to crimes that are said to be *mala in se*, but less frequently so with respect to *mala prohibita* crimes. The firearm whose possession is illegal in jurisdiction P may be permitted in Q. Technological advances, however, may enable A, who wishes to do what is criminalized in P, to accomplish it by transacting it in Q. Secret offshore bank accounts can hide the proceeds of criminal activity or avoid tax requirements (or both). Of course, a jurisdiction may choose to make illegal acts that would move doing φ offshore, but it is much more difficult if the evidence of an offense in P is hidden in Q. This is only one of many possible options and a particularly simple one. A may not be in P when the offense takes place. If A is in Q and by means of a computer transaction defrauds C in P, A may be beyond the reach of investigatory authorities unless there is some agreement between the authorities in P and Q. Such agreements are frequently absent, but even when such an agreement exists it may take time and effort to implement it if there are local sensitivities to be negotiated[5] and, if there are significant differences in the legal understandings of P and Q, it may be impossible for C to get redress. Although Westphalian boundaries are sometimes flouted or quietly subverted,[6] they continue to pose

3 Some of the diversity of definitions and complexities involved are discussed in Alex P. Schmid, A.J. Jongman, and Irving Horowitz, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature* (Amsterdam: Transaction Books, 1998); Bruce Hoffman, "Defining Terrorism", in *Terrorism and Counterterrorism: Understanding the New Security Environment*, ed. Russell D. Howard, Reid L. Sawyer, Natasha E. Bajema, third ed. (NY: McGraw-Hill, 2009), 4–33; Miller, *Terrorism and Counter-terrorism*, ch. 2.

4 However, we leave to one side what is often referred to as state terrorism (as was evident in Stalin's Soviet Union) as well as terrorism used in the course of war (say, British carpet bombing of German cities during World War II) and state support for terrorism (say, Syrian support for Hezbollah).

5 A recent case concerned the extradition of a permanent resident of Australia (of 37 years) to the US for cracking copy-protected software and then distributing it free of charge over the internet. Although the scale of the offense was not great, because there was an extradition treaty between the US and Australia it still raised eyebrows. Some felt that extraditing "simply" to protect US commercial interests gave the US excessive influence in Australia. See Kenneth Nguyen, "Australia Hands over Man to US Courts", *The Age* (Melbourne), May 7, 2007; P.W. Young, "Extradition to the US", *Australian Law Journal* 81 (April, 2007): 225. On June 22, 2007, he was sentenced to 51 months imprisonment in the US, though because of the time served in Australia during extradition proceedings he served less than 15 months. See http://www.sys-con.com/read/393715.htm. He returned to Australia in March, 2008.

6 There is evidence of both subversion and flouting in the so-called extraordinary renditions of suspected terrorists that were carried out by US authorities. See Association of the Bar of the City of New York & Center for Human Rights and Global Justice, *Torture by Proxy: International and Domestic Law Applicable to*

major obstacles to the effective control and prosecution of much criminality. When transactions become more complex than the simple ones noted, as indeed they often do, then the problems of investigation, prosecution and, perhaps, recovery can become even more difficult. If A, in P, steals B's identifiers from Q (either by hacking or phishing or some other ruse), opens an account under B's name in R, transfers B's assets to R and then arranges for them to be cashed out by an accomplice in R, the task of investigation and prosecution may become almost impossibly intricate. Moreover, actual criminality, especially at the high end, may be much more complex than this. The point is simply that technology has made possible forms of criminality that challenge the traditional means for their control, creating ethical quandaries as those committed to their control find that time-tested tools are no longer sufficient.

ATM card fraud is an example of the type of fraud that is becoming increasingly international in nature. ATM card numbers and even complete track 2 information[7], as well as card security codes, are available for purchase on websites that have been located in former eastern bloc countries, Russia, China, and other nations that often do not cooperate with US and European law enforcement authorities.[8] Access to this contraband is available to cyber thieves throughout the world who frequently work in highly organized groups and make use of the information to withdraw funds at ATMs located in various nations before financial institutions can detect the fraud and invalidate the cards. Access to contraband sites often requires a password or a cryptographic key available only to cyber thieves who establish a trust relationship with the criminal organization that sponsors the site.[9] Sensitive personal financial information, including social security and bank account numbers, captured in major data breaches at American retailers, banks and card processors have frequently turned up on these foreign sites.[10] Although the current discourse consistently weighs privacy against national security needs, the widespread availability of personally identifiable financial information puts individuals at risk for fraud.

"Extraordinary Renditions", New York: ABCNY & NYU School of Law, 2004; available at *The Record* (of the Bar Association of the City of New York) 60 (2005): 13–193; David Weissbrodt and Amy Bergquist, "Extraordinary Rendition: A Human Rights Analysis", *Harvard Human Rights Journal,* 19 (Spring, 2006): 123–60; idem, "Extraordinary Rendition and the Torture Convention", *Virginia Journal of International Law*, 46 (Summer, 2006): 585–650; idem, "Extraordinary Rendition and the Humanitarian Law of War and Occupation", *Virginia Journal of International Law*, 47 (Winter, 2007): 295–356; Michael V. Sage, "The Exploitation of Legal Loopholes in the Name of National Security", *California W. International Law Journal* 37 (Fall, 2006): 121–42.

7 Track 2 information is the information contained on the card's magnetic strip and can be used to fabricate a duplicate card.

8 K. Perreti, "Data Breaches: What the Underground World of Carding Reveals", *Santa Clara Computer and High Tech Law Journal* 25, no. 2 (2009): 375–413.

9 Statement of Rita Glavin, Acting Assistant Attorney General, Criminal Division, US Department of Justice, before the House of Representatives Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, March 31, 2009.

10 Douglas Salane, "Are Large Scale Data Beaches Inevitable?", Cyber Infrastructure Protection Conference '09, City College and SSI US Army War College, the City University of New York, June 2009. Available at: http://www.jjay.cuny.edu/centers/cybercrime_studies/D_SalaneLargeScaleDataBreaches.pdf.

Terrorism has also moved across territorial boundaries. Although localized terrorism still occurs (in places such as Egypt and Spain, and until recently in Northern Ireland and Sri Lanka), the attacks of 9/11 were a sharp reminder that terrorist activity does not need to be grounded in local discontent but may reflect disaffection from afar. The attacks of 9/11, moreover, were not the work of another "state" but of a much more amorphous group with no clear political identity. Whatever we may think of the responses to those events, they posed a challenge that had not been clearly thought through – attackers from afar and an operational center or centers that could not be identified with a government or country (even though an insurgent Taliban gave cover in Afghanistan). Furthermore, it was clear that the coordination required for the attack was possible only because it had become technologically feasible to move money and messages electronically. For the US authorities, it presaged things to come.

Reactive responses

Political authorities have responded to these transnational, international, and global challenges in a number of ways. One obvious response has been to try to increase border security (fences, patrols, etc.), but important as border interceptions have been, it has been argued that these have not been sufficient. Westphalian constraints have for the most part required that intergovernmental agreements are sought. Agreements between and among sovereign states have ranged from extradition treaties to exchanges of salient information. They have operated at a number of levels, sometimes through international organizations such as Interpol or through high-level memoranda of understanding.

As well as monitoring the incoming, outgoing and through-passing movement of human beings, there have also been efforts to monitor incoming, outgoing and through-passing transactions such as phone calls, internet communications and financial wire dealings. Indeed, these activities are increasingly conducted by specialized agencies set up for this very purpose. For example, AUSTRAC in Australia monitors international financial transactions of AU$5,000 or above.[11] These monitoring activities have sometimes proved problematic. In the US, for example, certain legal constraints have traditionally been applicable to many of these transactions. Most significantly for the contemporary era – at least until quite recently – the Foreign Intelligence Security Act of 1978 (FISA) was set up to ensure that any monitoring of cross-border communications satisfied a range of conditions. FISA was introduced to place stringent – though not insuperable – conditions on governmental monitoring of communications, generally communications between the US and foreign countries. It provided for

11 See Appendix.

a special court to handle requests for monitoring. These conditions, however, were relaxed in cascading fashion by both the USA PATRIOT Act of 2001 and the FISA Amendments Act of 2008. In addition, as we see later, widespread commercial collection and mining of digitalized data has also been accessed by government agents.

Although Westphalian constraints have for the most part required that intergovernmental agreements are sought, more has been thought necessary. Agreements that allow for exchanges of information or other actions that enable the interception and prosecution of criminal or terroristic enterprises have not always been thought adequate. If the security of borders cannot be achieved at the borders they can perhaps be achieved by unilateral actions taken beyond the borders. Sovereign states have instituted their own means of monitoring communications and transactions in their efforts to curb transnational, international and global criminal and terrorist activity.

To counter both crime and terrorism, technology is being turned to. In itself, this is not intrinsically inappropriate. But warring on crime and counter-terrorism strategies may overreach and the values of those in whose defense they are employed may be in danger of being undermined. No less problematic is that we may find that the coordination of effort that is required is jeopardized by jurisdictional differences.

The purpose of this study is to address such counter-crime and counter-terrorism concerns and offer some best practice recommendations.