Crime Law Soc Change (2006) 46:275–276
DOI 10.1007/s10611-007-9057-5

# Editor's postscript

**Peter Grabosky**

Published online: 13 March 2007


There are of course, many unresolved issues relating to cross-border cyber crime. A number of these were raised in an important article at the end of the last century [5]. They still apply today. In essence, they entail limited law enforcement capacity in the face of rapid technological change, the tensions arising from the conflict between national sovereignties and the imperatives of international cooperation, and the gap between digital haves and have-nots, otherwise known as "the digital divide."

Considerable progress has been made on a number of fronts to address the challenges of transnational cybercrime [2]. Perhaps the most significant achievement is the Council of Europe Cybercrime Convention (discussed in David Chaikin's article) whose efforts to harmonize substantive and procedural criminal law have served as a model for nations well beyond Europe. Elsewhere in the world, regional organizations have begun to turn their attention to cybercrime and its control. In 2006 The ASEAN Regional Forum published a statement on combating cyber crime, that called, *inter alia*, for countries to establish an appropriate legislative foundation [1].

Beginning in the late 1990s, the G8 subgroup on high tech crime established a 24/7 network of contacts, which now includes 45 members around the world.

So too has the private sector been active in enhancing the capacity to control cybercrime. The resources available to large corporations such as Microsoft, and to powerful industries such as the motion picture industry, dwarf those at the disposal of small developing nations, the very places that can serve as "electronic criminal havens." Microsoft, for example, assists law enforcement agencies with investigations, and offers rewards to informants who help identify the creators of malicious code. The company also co-produces an international training program for law enforcement agencies around the world that investigate computer-facilitated crimes against children [4].

In the nonprofit sector, the global proliferation of Computer Emergency Response Teams (CERTS) facilitates quick remedial response and takedown of offending sites by

P. Grabosky (✉)
Regulatory Institutions Network, Research School of Pacific and Asian Studies,
Australian National University, Canberra, ACT 0200, Australia
e-mail: peter.grabosky@anu.edu.au

cooperating industry professionals. Security bulletins published by CERTS permit rapid dissemination of security risks http://www.auscert.org.au/).

The recent history of cybercrime includes a spate of examples of successful multinational investigations of sophisticated transnational criminal conspiracies ([3] 76–79). Among numerous others, these have included:

- *Operation Cathedral*, a 1998 investigation involving authorities in 12 different countries targeting an international child pornography ring.
- *Operation Buccaneer*, which culminated in 2001 in simultaneous raids in six countries against participants in an internet copyright piracy conspiracy.
- *Operation Artus*, a investigation into a child pornography ring that led to the execution in 2002 of seven search warrants in the United States and 30 simultaneous searches in 10 additional countries.
- *Operation Site Down*, a 2005 investigation involving agents of 11 countries directed at organized piracy networks.

These, and other successes suggest that the interdiction of transnational cybercrime is not a "mission impossible." But it will continue to challenge authorities on both sides of the digital divide for the foreseeable future.

There seems no doubt that terrorists will continue to exploit digital technology, but how? The "Electronic Pearl Harbor" scenario remains plausible, but improbable, since, in the words of Professor Dorothy Denning, terrorists prefer the direct dramatic impact and gore produced by truck bombs, to the effects of logic bombs. Nevertheless, the immense empowerment provided by digital technology means that terrorist communications will be more efficient and effective than ever before, and their ability to communicate with mass audiences directly, without editorial intermediation, remains unprecedented. The challenges that governments face may be less electronically cataclysmic, but serious nonetheless, and the observations made by Stohl in this collection are no less apposite. How democratic nations respond without seriously infringing upon privacy and human rights will constitute a formidable challenge for the twenty-first Century.

One thing can be sure. Cyber criminals will seize upon every new technology, and every new application of these technologies, to commit crime. The increasing penetration of digital technology, the pervasiveness of electronic commerce, and the exponential takeup of technologies and applications in India and China will mean that criminal opportunities will abound. The challenge continues to lie in creating technologies, policies and practices of prevention and control that will allow legitimate users of digital technology to flourish while inhibiting illegitimate use.

## References

1. ASEAN Regional Forum (2006). *Statement on cooperation in fighting cyber attack and terrorist misuse of cyber space of the thirteenth ASEAN Regional Forum 2006*. http://globalwarming.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html (visited 16 January 2007)
2. Broadhurst, R. G. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management, 29*(3), 408–433.
3. Grabosky, P. (2007). *Electronic crime.* Upper Saddle River, NJ: Pearson Prentice Hall.
4. Microsoft (2005). *Microsoft security quarterly* http://download.microsoft.com/download/9/b/3/9b3b38df-0a36-43ad-adab-6a9d5c0b8882/Microsoft_Security_Quarterly.doc (visited 5 February 2007)
5. Sussmann, M. (1999). The critical challenges from international high-tech and computer related crime at the millennnium. *Duke Journal of Comparative and International Law, 9*, 451–489.