Foreword

The world's online population now exceeds two billion people. Nearly five hundred million of them reside in China, but over half of China's population has yet to establish Internet connections. Most will do so in due course; there seems little doubt that the Internet's 'centre of gravity' is rapidly moving to China, where it is destined to remain.

For all its virtues as a medium of communication, education, entertainment, and other worthy ends, the Internet is vulnerable to criminal exploitation. This poses formidable problems for those countries whose well-being depends on information security. Their difficulty is compounded by the fact that the physical frontiers between sovereign states are not mirrored in cyberspace, and the international mobility of online criminal activity, in terms of both velocity and distance, has no terrestrial counterpart. If cross-border crime was ever a problem, it certainly is now.

The international community began to confront this challenge before the turn of the century, with efforts to enhance law enforcement cooperation and to harmonize laws of cybercrime. The Council of Europe Cybercrime Convention is the best example to date. The existing network of international cooperation, however, is hardly seamless. Only a handful of non-European states are signatories. Some countries lack the capacity to establish a legislative and regulatory framework to control cybercrime. Others have what they regard as more pressing priorities. Elsewhere, political realities may be a significant impediment to mutual assistance.

One of the most vivid examples of the latter is the situation existing between the People's Republic of China and Taiwan. The stresses that have existed between the two entities since 1949 have precluded most forms of intergovernmental cooperation. In recent years, a degree of relaxation in tensions has been accompanied by economic, educational, transport and tourism activity, but both sides have been wary of law enforcement assistance.

Both Taiwan and the PRC have experienced significant online criminal activity. Some of this is indigenous to each – a local issue. Some of it occurs across the Taiwan Strait, from one side to the other. And because of the jurisdictionally porous nature of cyberspace, some will be initiated on one side, against a target on that same side, after having been routed through facilities across the Strait. The provenance of a cybercrime is thus not always apparent. Even when it is, a collaborative solution has remained elusive. The relevance of cybercrime to overall security is also a critical matter for both Taiwan and China, compounding the challenge faced by both sides. The extent to which one or both parties is refining their information warfare capabilities is a matter of considerable secrecy, but it seems most unlikely that either has left the matter to chance. Since information security is more than just an issue of cybercrime, mutual assistance across the Strait would appear unattainable.

Dr Chang's path-breaking book highlights this problem and suggests ways of managing impediments to effective cross-Strait cooperation. Based on in-depth interviews with officials, academics, and knowledgeable contacts in the private sector from both sides of the Strait, the book contains penetrating insights and compelling quotes. His discussion of the potential for informal exchange in the absence of formal mutual assistance arrangements is both nuanced and insightful. Despite the inherent tensions in the cross-Strait relationship, informal contacts provide the basis for co-operation on certain matters (needless to say, these do not include matters of national security). The book demonstrates the importance of *guangxi* as the basis for a modicum of mutual assistance.

One of the classic challenges to cyber crime control, whether domestic or cross-jurisdictional, is the reluctance of some victims to disclose their misfortune. This choice may be entirely rational, as the disclosure of vulnerability may generate adverse publicity for the victim that may in the long run be more costly than their initial loss. However, such non disclosure may conflict with a wider public interest in identifying systemic patterns of vulnerability in order to design effective enforcement or technological countermeasures. Particularly noteworthy is Dr Chang's analysis of the ways to establish information incident sharing platforms between government and the private sector. His imaginative application of models of hospital infection control and aircraft near-miss incident reporting to the domain of cybercrime is indicative of his creative thinking.

Cybercrime, perhaps to a greater extent than conventional crime, exceeds the capacity of the state alone to control. This leads to Dr Chang's discussion of collective participation in the control of cybercrime, a process that he refers to as 'wiki cybercrime prevention'. Although mass participation in any endeavour poses challenges of accountability – one must recognize the risk of cyber-vigilantism – mass involvement in cybercrime control seems inevitable, and its evolution is certainly worth watching.

One notes that cross-Strait collaboration for cybercrime control is no longer limited to informal exchange. In 2011, Chinese and Taiwanese investigators worked together to interdict an internet-based fraud conspiracy involving Chinese and Taiwanese suspects physically located in Indonesia and other Southeast Asian nations. Whether this 'bridge' of collaboration across the Strait is a harbinger of future cooperation remains to be seen. But readers of Dr Chang's fine book will appreciate how it all started.

Peter Grabosky
Regulatory Institutions Network,
College of Asia and the Pacific,
Australian National University,
Canberra
September 2011