Chapter 6
Understanding Digital Intelligence:
A British View

David Omand
King's College, UK

ABSTRACT

This chapter examines digital intelligence and international views on its future regulation and reform. The chapter summarizes the lead up to the Snowden revelations in terms of how digital intelligence grew in response to changing demands and was enabled by private sector innovation and mediated through legal, Parliamentary and executive regulation. A common set of ethical principles based on human rights considerations to govern modern intelligence activity (both domestic and external) is proposed in the chapter. A three-layer model of security activity on the Internet is used: securing the use of the Internet for everyday economic and social life and for political and military affairs; the activity of law enforcement attempting to manage criminal threats on the Internet; and the work of secret intelligence and security agencies exploiting the Internet to gain information on their targets, including in support of law enforcement.

DOI: 10.4018/978-1-4666-9661-7.ch006

INTRODUCTION

"It is not the strongest species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change." Charles Darwin was describing what happens when rapid changes take place to the specialized niche in which a species has become comfortable, challenging its very survival. Coincidentally, the last twenty years have seen three revolutionary changes in the environment of Western intelligence agencies.

Rapid change certainly describes the new intelligence requirements after the end of the Cold War, the dissolution of the Warsaw Pact and the integration of central Europe into the Western community of nations. Even more so, after the al-Qaeda attacks on Washington and New York on 9/11 2001, the urgency of the demands for intelligence to counter international terrorism and instability created huge pressure on intelligence communities around the world.

Over the same period, however, all intelligence agencies have simultaneously had to try to adapt their activity to the profound changes wrought by the digital revolution in their technological environment. The popularity of the Internet as a means of communication, the invention of the World Wide Web and the ability cheaply to store digital data transformed the opportunities for obtaining intelligence and the opportunities have not stopped growing since.

The third set of changes concerns the legal and political structures within which most security and intelligence agencies in the democracies now operate, with their existence avowed, their activities subject to law, and with web sites explaining their purpose and recruiting the next generation of staff.

By the end of the first decade of the 21st century, the most advanced intelligence communities at least had adapted to these changes. The signals intelligence agencies in particular had begun to settle comfortably into a highly productive new niche, actively exploiting unprecedented access to digital information to deliver to their military and law enforcement customers much highly valued intelligence on their targets, often in near-real time and with little if any serious public controversy over their powers and reach.

The Snowden revelations have, however, exposed to unprecedented and uncomfortable national and international gaze the very success of the United States agencies and those of its close intelligence allies, including the United Kingdom, in adapting to the digital world. The protection of personal information from unlawful exploitation, and the legality, proportionality and adequacy of regulation of digital intelligence access and intelligence sharing have become major international political issues. The adequacy of the previous changes in legal powers and governance arrangements are seriously challenged.

Many governments are reappraising their reliance on major US Internet companies (and also their reliance on Chinese information technology suppliers as the UK Parliamentary Intelligence and Security Committee (ISC, 2013) has reported) as some of the methods of digital intelligence become more generally known. The US Internet and technology companies themselves are busy reassuring their customers that their data will be made invulnerable to the bad guys – and by that they include the intelligence agencies of their own government. Behind their stance lies the commercial reality that although approximately 40% of world population has access to the Internet most are in the developed world and the expected future growth in business will be in China and elsewhere in Asia and South Asia, South America and Africa, where there is a suspicion of the dominance of the US information and technology companies and their links to government as well as a natural wish to see the development of indigenous capability. At the same time, most intelligence and security agencies around the world are no doubt trying to work out how to close an apparent capability gap with the United States. Meanwhile Western