RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 111 – 8 May 2015

Cybersecurity: Advancing Global Law Enforcement Cooperation

By Caitríona Heinl & Stephen Honiss

Synopsis

When some dialogues in the wider cybersecurity debates are not progressing quickly enough, with sufficient political will, international collaborative efforts among law enforcement is one area that holds much promise.

Commentary

THREE MAJOR events in the international community's cyber calendar occurred during the week of 13 April to address the demand for more robust global cooperation to combat cybercrime. The inauguration of the INTERPOL Global Complex for Innovation (IGCI) in Singapore; the Global Conference on Cyber Space (GCCS 2015) in The Hague; and the third session of the UN Group of Governmental Experts (GGE) on Developments in the field of Information and Telecommunications in the context of International Security in New York; each had a deep focus on international cooperation.

The list of challenges facing communities and governments globally from cybercrime is daunting. Traditional models are no longer adequate for the transnational nature of cyber, which now require stronger international collaboration. Whilst people may be wary of carrying large amounts of cash to avoid being robbed, the reality is that they are far more likely to fall victim to some form of cybercrime. The successful modern-day thief is a far cry from gun-toting Bonnie and Clyde and are increasingly difficult to catch.

Intricacy of cybercrime

Cybercrime, "419" letter scams, hacking – these terms all relate to offences with two things in common. Firstly, they are committed using an electronic device and the Internet; and secondly, they are likely to have been committed by a criminal overseas from the victim with the stolen money transited through a series of accounts in different countries again. The law in most countries was not written with this situation in mind, making it difficult, if not impossible, for law enforcement to track down the criminals.

Then there are highly-sophisticated, aggressive, often surgically precise, cyber attacks against

industries that provide the lifeblood of economies, and against the agencies charged with defending those economies and countries.

In addition, there are few traditional crimes today that do not rely in some way on the use of the Internet. Such cyber-enabled offences are often cross-border crimes and they include, amongst many others, human trafficking, theft of intellectual property, blackmail and extortion, fraud, and drug trafficking. GCCS 2015 acknowledged that criminals are savvy in using countries where they know law enforcement is limited in legal recourse or technical capacity. GCCS 2015 follows three previous high-level dialogues that were first initiated in the United Kingdom in 2011, now known as the London Process. The last conference was held in Seoul in 2013 and it too continued to develop the theme of cybercrime.

Key developments

The inauguration of the IGCI was therefore a highly significant development for the global law enforcement community. It now provides a platform for collaboration both on operational matters and policy issues that have implications for the law enforcement community, as well as on the wider cybersecurity debate. It will also focus on emerging crime types and the impact of the Internet on traditional crimes.

This will be achieved by coordinating international law enforcement efforts on operations involving multiple jurisdictions and where needed; involving experts from industry, academia, research bodies, and the technical community, as well as other regional law enforcement bodies like Europol, ASEANAPOL, and AMERIPOL.

To further strengthen international cooperation, the 2014/2015 GGE is anticipated to build on the recommendations in the 2013 report. The report advised states to intensify cooperation against criminal or terrorist use of information and communication technologies (ICTs); to harmonise legal approaches as appropriate; and to strengthen practical collaboration between law enforcement and prosecutorial agencies. The Seoul Framework in 2013 later reiterated this recommendation in its guidelines.

The group also recommended enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile state actions in order to improve international security.

There is a growing recognition by law enforcement for the need to work more closely and in partnership with all stakeholders, such as the private sector, civil society, academia, research organisations, and the technical community. Hosting GCCS 2015, the Netherlands included government officials, international organisations, the private sector and civil society. This high-level conference specifically aimed to improve international cooperation with regard to the Internet and it focused on cybercrime as a part of the wider cybersecurity debate.

Important Issues at GCCS 2015

Strategies to fight cybercrime and resolving difficulties in determining jurisdiction were key questions posed during GCCS 2015. In particular, experts were present to analyse the role and responsibilities of stakeholders, such as law enforcement, in addressing challenges such as how to ensure people and organisations are protected; how to guard individual privacy; predictive policing; and how to ensure that the Internet remains both open and secure to support economic growth and innovation.

The Netherlands added the issue of the right to privacy to this year's agenda to promote further international debate. The key challenge it identified was to ensure that security is safeguarded while also making sure that the digital domain remains open and innovative. Another new item was civil-military relations and international military cooperation in cyberspace - in other words where the responsibility of law enforcement ends and that of the military begins for cyber incidents.

An increasingly critical subject open for discussion is that of the rising use of encryption built without back doors - what this would mean for the protection of individuals' and companies' data, and its impact on law enforcement investigating criminals who use this technology to avoid detection. Mutual

legal assistance procedures are also not fit for purpose when it comes to this space and GCCS 2015 aimed to assist in finding a new way forward.

Such recent focus on the role of global law enforcement in combating new developments in cybercrime further highlights the significance of these efforts to wider international cybersecurity efforts.

Caitríona Heinl is a Research Fellow at the Centre of Excellence for National Security (CENS) of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Stephen Honiss is a Detective Superintendent from the New Zealand Police, on secondment to the Cyber Innovation and Outreach Directorate of the INTERPOL Global Complex for Innovation (IGCI) in Singapore.

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg