RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 079 – 6 April 2015

Contemporary Cybercrime: Countering Through Cross-discipline Cooperation

By Caitríona Heinl and Stephen Honiss

Synopsis

The official inauguration of INTERPOL's Global Complex for Innovation (IGCI) in Singapore on 13 April 2015 is a significant step in the right direction to combine international efforts in the fight against contemporary cybercrimes. Still, this is no easy feat as numerous challenges face the international law enforcement community.

Commentary

CYBER IS a game changer since it now affects most law enforcement operations including those that traditionally had no technological aspect. INTERPOL's IGCI therefore held its first workshop in March involving law enforcement, industry, academia, and research bodies to more fully identify its research agenda for the near term.

In light of this workshop, there are at least three noteworthy challenges facing the international community. They are the need to proactively expect new trends and threats; the necessity for stronger international collaboration; and the requirement to more responsibly tackle privacy concerns over law enforcement's access to data.

Need to proactively anticipate trends and threats

Given that criminals are often quick to adopt new technologies and techniques, there is a need for law enforcement agencies to increase capacity to anticipate developments proactively so as to be more effective in combatting criminal activities. This area is very fast-paced; to be ahead of the curve, law enforcement authorities acknowledge that collaborative research efforts with non-law enforcement partners are necessary. Maintaining the edge in areas such as digital forensics, attribution, educating Internet users in cyber hygiene, cyber criminology, and forecasting looming threats are essential.

However, a key challenge adversely affecting this goal of increasing research output is often one of limited financial and labour resources. Compounding this issue is the need to identify key priority areas to focus these limited resources on given the wide range of cyber issues that warrant in-depth research and analysis.

To overcome labour constraints, this can be addressed by leveraging the expertise of industry and the research community. Private sector and research organisations possess different skill-sets and expertise that law enforcement authorities often do not. In light of the nature of cyber challenges, working more closely with such entities can help law enforcement agencies enhance their technical and policy capabilities to better measure cybercrime, anticipate future trends or threats, and improve information exchange.

Moreover, such collaboration could help law enforcement agencies decide which threats or issues should take priority. In addition, leveraging the capacity of other sectors in this collaborative manner might go some way to alleviate difficulties in identifying, training, and retaining the right personnel in this sector.

Some examples of collaboration include establishing research networks as well as knowledge exchanges through updates, newsletters or even joint research outputs. For instance, INTERPOL cyberfeeds are short analyses of cybercrime threats that are disseminated to raise awareness of current issues.

Joint workshops are another simple but effective way to better inform stakeholders of the actual challenges faced as well as a source for innovative solutions. This type of exchange is extremely beneficial since all parties develop a better grasp of each other's needs, expertise and constraints. For example, INTERPOL's recent workshop that involved law enforcement, industry, academia, and research bodies helped to better determine the research agenda.

Need for better international collaboration

Identifying and leveraging country strengths in this field might also create more tangible results. This is where an international organisation like INTERPOL, through the IGCI, will now be well placed to coordinate such efforts that benefit its member countries.

The harmonisation of legislation and definitions is a key challenge that is not easily resolved due to differing national legal systems, priorities and motivations, cultural differences on what is acceptable, and data sovereignty. There have therefore been some calls to reach a consensus at least (or perhaps even minimum standards).

In addition, some argue that a major challenge is not so much attribution, in other words accurately identifying those responsible. Rather, the flow of data across multiple borders and legal jurisdictions causes even further challenges for law enforcement. If information could be shared more freely in the community, this might then go some way to addressing the problem.

Again, this is another area where researchers might be able to further contribute. This could benefit law enforcement given that criminals are not bound by national boundaries whereas authorities must operate within national jurisdictions.

Privacy concerns over law enforcement access to data

Law enforcement authorities feel that they have been badly affected by the Snowden revelations in June 2013 due to negative public perception. Moreover, the relationship of trust between law enforcement and the private sector has been significantly hampered. The authorities must work hard to reestablish trust between the public and private sector as well as assure citizens on an ongoing basis that they only act in the interest of the public and citizens' legitimate concerns and rights are respected.

Other areas that now warrant deeper consideration from a policy as well as law enforcement perspective include what virtual currencies, encryption, and terrorist groups' use of the Internet mean for law enforcement's access to data. The media, too, can play an important role in informing these discussions.

Nevertheless, these issues are dealt with in different ways by many jurisdictions, and therefore a mapping exercise could help find commonalities as a starting point for future cooperation.

While experts agree that truly reliable metrics for cybercrime are difficult to find, efforts to fight crime are in the public interest. The real cost of financial losses, reputational harm, and recovery costs from breaches may not always be accurately determined; but this does not detract from the fact that the fight against contemporary cybercrimes is a matter of national and international importance.

While the mandate of IGCI in Singapore is global in scope, it should have a very practical and visible impact on this field across Southeast Asia and the wider Asia Pacific region. Industry, the policy research community, and law enforcement can play an important and more proactive role in supporting their respective efforts in several ways.

They are in a position to work together to translate policing needs into research problems or solutions that are mutually beneficial. While collaborative activities are already underway, there is still much scope for increasing such efforts to better prioritise issues on the policy agenda.

Caitríona H. Heinl is a Research Fellow at the Centre of Excellence for National Security (CENS), at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University in Singapore. Stephen Honiss is a New Zealand Police officer working on cyber issues at 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