RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 139 – 24 July 2017

Law Enforcement: Security Challenges Ahead

By Muhammad Faizal Bin Abdul Rahman

Synopsis

The second Interpol World Congress in Singapore in early July 2017 highlighted a spectrum of relevant issues that intersect the cross-border, physical and cyber domains. It also defined the evolving security landscape.

Commentary

THE FUTURE of policing is set to be a perpetual race where threat actors, particularly criminals and terrorists, ride the wave of three megatrends – globalisation, urbanisation and new technologies – to strengthen their nexus and outsmart the law. The role of law enforcement agencies is increasingly intertwined with national security as they face these threats by countering cybercrime, leveraging technology to protect global cities, and employing identity-management systems to secure borders.

Two overarching hurdles could be discerned from the Interpol Congress which the agencies need to surmount to stay ahead of the threats: the first is to strengthen the culture of innovation in their organisations; the second is to enhance partnerships with the private sector.

Challenge #1: Innovation – More than just Technology

Technology itself is not the panacea but an essential part of law enforcement strategies. A stronger culture of innovation in law enforcement agencies is crucial to developing solutions for the various challenges that may limit its utility.

Organisational challenges are numerous, but four key issues stand out: *People*

issues such as staff training and mindset; *process issues* such as operational procedures to safeguard privacy and responsible use of data; *technical issues* such as data protection and ensuring that Artificial Intelligence (AI) tools are free from human biases; lastly *interdependency issues* such as the effects of new technologies on relationships with stakeholders and the wider community.

For example, the use of police drones is an airspace management issue to civil aviation agencies but may be a privacy issue to certain segments of the public.

Adversarial challenges stem chiefly from the threat actors' swiftness in adopting technology and innovative tactics. Unlike law enforcement agencies, they do not hesitate to acquire technology through unlawful means and use them unethically. For example, Europol's Serious and Organised Crime Threat Assessment 2017 highlighted that threat actors could easily acquire tools and services for cyberattacks from cybercriminals through the Dark Web.

Strengthening the Innovation Culture

To confront these challenges, agencies need to discern and diminish existing barriers to innovation such as red tape. This is so that they can be more agile in enhancing operational procedures and experimenting with technological solutions for better information-sharing and forming a comprehensive approach to security.

Additionally, a stronger culture of innovation should be underpinned by a framework for managing plausible risks associated with the wider use of technology. Key among these risks are the operational gaps that may unfold when agencies have to grapple with a) data overload during crises, amid pressures from regular policing duties and resource constraints; b) insider (cyber) threats from unwitting employees; and c) possible harm caused to the public if AI tools such as police robots malfunction.

Challenge #2: Partnerships – Increasingly Important

Several implications of digitisation and globalisation have elevated the importance of partnerships between law enforcement agencies at the domestic and global levels and the private sector. Two areas are especially critical: in information-sharing and capacity building.

Firstly, the efficacy of biometric data to detect transnational criminals and terrorists depends on good information-sharing at the global level. Moreover, actionable intelligence could be extracted from big data such as advanced passenger information and social media, and knowledge of unreported incidents that reside within the private sector, besides law enforcement databases.

Secondly, the research and development efforts of the private sector could help accelerate law enforcement projects to develop innovative tools and tactics for threat detection and response. For example, Interpol had partnered with the industry to launch a facial recognition system in November 2016. Looking ahead, advances in biometric technology could better link people's digital and physical identities, thus supplementing existing measures to combat cybercrime and deter illicit online activities.

Thirdly, various threat actors are beginning to resemble each other more; this could frustrate intelligence efforts if information-sharing between law enforcement agencies and private sector is sub-optimal. For example, the use of cybercrime tactics across the spectrum of threat actors (criminals, terrorists, state-sponsored) suggests that they are forging ahead with illicit partnerships to innovate by learning from each other.

Fourthly, while the private sector may be driven by profit, it is also in their interest to cooperate with law enforcement for the protection of their clients and customers, people and assets given the nature of contemporary threats.

Enhancing Partnerships

The most critical step to enhancing partnerships is to discern and diminish existing barriers. Key among these barriers is the level of trust and confidence in information-sharing, which may in turn shape the state of cooperation in joint capacity building.

To enhance trust and confidence, law enforcement agencies should review legislative frameworks and policies to ensure robustness in data protection and facilitate information-sharing, streamline information-sharing procedures, and increase the level of transparency in the use of information in order to reciprocate the partners' cooperation. These actions should however be buttressed with sustainable efforts in building meaningful relationships with the partners.

At the global level, law enforcement agencies could better leverage established mechanisms and forums such as Interpol's to connect across borders and with the private sector for information-sharing and joint capacity building. These in turn could boost the agencies' role in assisting – bilaterally and multilaterally - cities which may lack state-of-the-art technical capabilities and expertise in crime-fighting and information-sharing.

This can help overcome any weak links in the global law enforcement community. In sum, stronger public-private partnerships could drive higher levels of innovation in law enforcement to face the security challenges ahead.

Muhammad Faizal bin Abdul Rahman is a Research Fellow with the Homeland Defence Programme at the Centre of Excellence for National Security (CENS), a unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.