Priorities for current policing policy and training: five challenges from cyber space

Dr Sally Leivesley, Newrisk Limited , www.Newrisk.com

There are five game changers in future policing most of which are external, highly complex and essential to understand if British policing is to retain its international leadership in command and control, intelligence, training and public confidence. These game changers apply also to police forces of other countries confronting a cyber space era of organised crime, terrorism and proxy nation state attacks against the security of the state, the lives of the public and the economic well-being of the population.

The rewards of rapid recognition of these and other game changers could be technological wisdom and balanced policing that will work with other agencies to outstrip organised crime, pre-empt devastating terror plots and assist in mounting barriers to sophisticated nation state attacks on infrastructure critical for public well-being. Commencing future planning now by police, in cooperation with other agencies and in consultation with other countries is an opportunity to empower, enable and deliver an increasingly pre-emptive crime fighting force that will protect the public and retain the public's trust.

The first game changer is an unseen challenge in cyber space. This is for police to bring novel measures for operating in cyber space that can constantly adapt to the emerging open society and business appetite for high speed, high volume trade and communications that denies slow-down from security measures and accepts losses as long as systems are able to keep serving the markets. The future is one where security as a concept disappears and sustainability of systems and services is the public's priority. This translates into airports being designed as shopping centres without visible security checking in the movement onto a plane and banking and trading that runs on systems not slowed by security and accepting losses as long as the delivery of services is maintained. The technology platforms and legislation to enable police to operate in this future environment needs design and testing now for implementation commencing in a year. Changes into sustainable cyber policing which should become the lead policing operation could evolve in less than three years and become come highly capable soon after. The speed of technology development and an increased risk of catastrophic effects from emerging threats facing this county and other countries are the basis for this timeframe.

A dirty cyber space is the second game changer and this relates to the primacy that will be required for security of policing systems and the capacity for police to integrate operations with other agencies nationally and globally. This includes the critical maintenance of government operations and public protection. The challenge will be to confront attacks from organised crime that will respond by attacks on police obstructions to international crime proceeds and from attacks by terrorists who will move from physical attacks on police targets to cyber-attacks on police capability. Cyber threats will also come from nation states working through deniable proxies to attack national security and confidence of the public and to deny police operations and command and control and intelligence if there is a conflict. (North Korea which has increased the risk of a nuclear conflict has already demonstrated this deniable cyber -attack strategy on critical South Korean infrastructure)

The third game changer is policing operations in a cyber-dominated environment which requires strength through integration of police with other agencies and real-time fusion of intelligence and operational data. The challenge is for police to pre-empt the cyber dominated future by integrating further with other agencies and contributing to a novel policy that could be a truly distributed

localised security system serviced by police alongside the security agencies including military intelligence and other emergency services. Central to this is the technology platforms for fused intelligence allowing the strengths of each agency and the police to be retained but run in real-time through fused data and intelligence, both OSINT (which would held industry) and secure.

Security would ideally be coordinated through city administrations which are far more flexible and localised critical national infrastructure hubs than central governments which would retain strategic direction. With localised delivery and highly distributed operations and communications, the public's recognition of differences between the police and agencies delivering local security and crisis response and recovery will become blurred. Preparation for this merged security identity and movement into a super strong localised and highly survivable operating system requires advanced thinking now in 2016, preparation of joint doctrine, recruitment streaming, training and also secondments to other countries to merge systems and trust well beyond national boundaries.

The fourth game changer is technical - police face a race in time, speed and capacity for integration and data and intelligence fusion. Big data, artificial intelligence, global standards for securing the Internet of Things and technical artificial intelligence mapping the increased fragility of cities dependence on cyber delivery of the needs of daily life, are all tools for policing action in coordination with the other agencies.

Policing operations will remain the closest interface of security with the public and policing delivery will need to be pre-emptive, aggressive and overwhelming of cyber and physical terrorists and nation states. All of these hostile agents are already demonstrating a build of attack interfaces through organised crime networks and crime supply systems. Public trust will need to be retained through policing operations to protect physical and cyber security of services for daily life and welfare. The current culture of trust and flow of communications between police and the public will assist with this challenge.

The fifth game changer is that Governments will become more technologically driven and will work through cyber space with other countries. The challenge for policing is blurring of policing identity in an increasingly dependence on technology driven operations, cross boundary work with other countries and delivery of policing through cyber space and through merged physical operations. Within this, policing will need to retain the identity and skills inherited from previous generations - this inter-generational continuity of policing identity is essential for trust to be maintained and for the police and public and industry to work together to pre-empt threats from crime, terrorism and hostile nation states in a successful way that that will reassure the public and retain public trust in an increasingly uncertain world.

Dr Sally Leivesley PhD Lond., MSPD, BA(Hons) Qld., FICPEM,FRSA,MACE,MIABTI,RSES
Managing Director of Newrisk Limited, trains and exercises companies and governments on protecting people and business from extreme incidents.
A Founder Member of The Exercise Group7 http://www.newrisk.com/theexercisegroup7.htm
Member of the Register of Security Engineers and Specialists (RSES)