RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 235 – 14 December 2017

Smart Security: Balancing Effectiveness and Ethics

By Faizal A Rahman

Synopsis

Smart security – the application of smart technologies for security - offers better defences against evolving threats. Nonetheless, harnessing its full potential requires reimagining operational practices and contemplating the associated ethical issues.

Commentary

TECHNOLOGICAL ADVANCES are driving the law enforcement and private security sectors to adopt smart technologies for better defences against evolving terrorist and criminal threats. Two key considerations could determine how well the full potential of big data analytics and artificial intelligence (AI) which underpin smart technologies are harnessed.

First, social research suggests that technology adoption is not only about continuing current operational practices with greater efficiency. More importantly it is also about reimagining these practices so as to stay resilient in the face of evolving demands. Second, technology adoption is not only an operational decision and technological leap; it is also a multifaceted process that includes contemplating the associated ethical issues.

From Protection to Prevention

The private security sector – which supports law enforcement – adopts smart technologies (such as CCTV-based patrolling systems and drones) to protect public places and large-scale events. Human limitations in patrolling are overcome through automation to better detect potential threats. This first step towards technology adoption makes current operational practices more efficient through cost and productivity improvements.

The next step should reimagine these operational practices by seeking new opportunities to better support law enforcement's intelligence collection, to prevent potential threats from materialising. For example, law enforcement's efforts work well to preempt threats from known terrorists. However, lone wolves constitute a growing threat as they often do not arouse the suspicion of the authorities until their attacks unfold. Moreover, their unsophisticated tactics (such as knife attacks and vehicle ramming) can be discreet yet impactful as surveillance technologies may lack the capability to stop threats upon detection.

To this end, smart technologies deployed by the private security sector should over time develop more capacity to promptly channel information of possible terrorist pre-attack activities to the law enforcement sector for timely intelligence analyses. The law enforcement sector would need wider real-time access to private security systems, either on a voluntary or mandatory basis, to reduce blind-spots in surveillance and enhance information-sharing between both sectors. Currently, the commercial market is developing products that offer to integrate police and private security systems.

However, this next step could raise important ethical issues concerning augmented surveillance; this essentially uses AI for threat prediction (terrorist and criminal) and suspect profiling. The risk of AI perpetuating human biases – what is called "automated discrimination" – could be of concern to certain segments of the community.

Ethical Issues in Automated Policing

Automated discrimination is nascent and needs to be understood better. Its importance as an issue would grow as augmented surveillance becomes more common. It could evoke fears of wrongful targeting of law-abiding persons thus affecting public trust and confidence in the law enforcement sector and by extension, the state.

It is more than just a policy challenge; it intersects with the technical issues of unintended biases in algorithms and big data that could skew analyses generated by AI systems. Algorithms are computer procedures that tell computers precisely what steps to take to solve certain problems.

First, the problem of algorithmic bias – AI algorithms being a reflection of the programmers' biases – may possibly give rise to the risk of false alerts by AI surveillance systems thus resulting in wrongful profiling and arrest. For example, this concern was raised in media reports about the Guangzhou-based company Cloud-Walk. This firm had developed an AI system that could alert the police to take preemptive action against a person after computing his predilection for crime based on facial features, behaviour and movements. The ethical (and legal) issue of interdicting persons, based on predictions, for future crimes also comes to play.

Second, AI profiling systems utilise historical data to generate lists of suspects for the purposes of predicting or solving crimes. However, the data may only partially represent the current crime situation; but more importantly it may unknowingly contain human biases along the lines of race, neighbourhood, ex-criminals (although reformed) etc. For example, the reported use of an AI profiling system (Beware) by

Chicago Police had raised ethical concerns over racial discrimination towards people of colour.

Essentially, research suggests that AI systems – even with complex algorithms - are only as good as the data sets that the systems trained and worked with. The systems could thus generate more analyses (prediction and profiling) as well as lead to outcomes that reinforce existing human biases that may have been straining police-community relations in certain cities.

Finding the Equilibrium & "Black Box" Effect

In sum, the burgeoning use of smart technologies by the law enforcement and private security sectors is premised on the objective of augmenting surveillance (and intelligence) powers to better prevent threats. While this objective necessitates reimagining current operational practices, it could also give rise to ethical issues of automated discrimination.

The ethical issues are expected to grow in significance. This is because with machine-learning (ML), the algorithms underpinning smart technologies would become more powerful and play a more integral role in decision-making. Moreover, the challenges in addressing these issues would also evolve as ML could possibly lead to the "black box" effect – how algorithms "think" may be incomprehensible to the humans affected.

For smart security to work well there has to be an acceptable balance between augmented surveillance and ethics. First, the risk of false alerts could possibly be reduced if the process of adopting smart technologies incorporates efforts to determine how the underlying algorithms work; this could also support fairness in AI-driven decision-making.

Second, how data is collated and used must be reimagined to reduce the risk of unintended biases being introduced to AI systems. Finally, how AI-generated analyses are used (such as crime prevention through enforcement or social development) must be reimagined to reduce the risk of possible negative implications on the community.

Faizal A 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.