RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg

No. 300 – 13 December 2016

Smart CCTVs:
Third Eye of Secure Cities

By Muhammad Faizal Bin Abdul Rahman

Synopsis

Many cities around the world are exploring the use of Smart CCTVs as advances in Artificial Intelligence (AI) offer operational value for homeland security. However, cybersecurity and overreliance could impede the technology's potential.

Commentary

FOLLOWING RECENT terrorist incidents, Germany's Interior Minister announced in August 2016 that CCTV cameras at airports and train stations will be enhanced with facial recognition technology. Likewise, the New York Police Department has developed the Domain Awareness System that uses similar technology to track and monitor potential suspects.

Globalisation increases the exposure of cities to myriad transnational threats even as growing urbanisation is putting the strain on law enforcement by increasing the densities of population, property and critical infrastructure to be safeguarded in each precinct. These inherent challenges in protecting cities - population and economic centres that make attractive soft targets – necessitate the early warning and identification of threats. Smart CCTVs support this function as the third eye of cities by complementing the vigilance of police officers and the community.

Securing Smart Cities

CCTV surveillance of public spaces has been a routine security feature of urban environments since the 1990s but grew in ubiquity post 9/11. Premised on the concept of "defensible space", it is a physical expression of the community's ability to defend itself against perpetrators and over time grew in importance as the "fifth utility" alongside critical infrastructures: water, gas, electricity and telecommunications. Past incidents have demonstrated its utility in post-event investigations and disruption of further threats.

Advances in AI are improving the accuracy of video analytics - facial, behavioural and object recognition – therefore increasing the potential of Smart CCTVs to fully/semi-automate the processing and analysis of voluminous data collected from a vast network of cameras and in the long term decision-making. Smart CCTVs are capable of round the clock city-wide intelligent surveillance and not subjected to human limitations.

Countries are increasingly embracing Smart CCTVs as a quintessential feature of smart cities to meet evolving security needs given the changes to the character of cities due to growing urbanisation. For example, the Police Camera (Polcam) project which deploys CCTV cameras extensively in residential towns is a key feature of Singapore's Smart Nation initiatives and enhanced counter-terrorism strategy.

Private security firms have also begun adopting the technology to reengineer business processes by optimising security patrols with remote surveillance of their clients' properties.

Securing Smart CCTVs

While smart technologies are expected to bring benefits to modern cities, it also introduces vulnerabilities. Interconnectivity by nature enlarges the potential attack surface of cities and reveals novel attack vectors for threat actors to exploit. The hacking of the police-operated CCTV system during the 2015 Southeast Asian Games in Singapore demonstrated the plausibility and criminal intent to target law enforcement agencies.

In February 2016, Hezbollah's Al-Manar television station's claims that the militant group had purportedly hacked into CCTV cameras in Israel demonstrated a hostile intent to undermine CCTV systems as part of larger information warfare to undermine the Israelis' sense of security.

Therefore, the spectrum of cyberattacks on a city's Smart CCTVs could range from sheer criminality to compromising national security, given that cyberspace is the fifth dimension of warfare and cities are the lifeblood of nations.

Cybersecurity risk management should begin with assessments of the four aspects of plausible cyberattacks - as highlighted in a study on *Smart Insiders* by Oxford University, UK – namely: assets targeted, threat actors, outcomes of the attack, and attack vectors. Security policies and mechanisms should aim to protect the assemblage of assets - cameras, networks, databases and analytics tools - that constitute the Smart CCTV infrastructure. For example, Neighbourhood Watch could be alert for signs of suspicious activities (for e.g. drive-by hacking) in the proximity of police cameras and network infrastructure in addition to classical neighbourhood crimes.

Implementation - Other Factors

Security agencies' policies on the implementation of Smart CCTVs should factor in other critical factors; including interoperability with mission-critical systems such as criminal intelligence databases, and Command, Control and Communications systems; information-sharing between agencies; and addressing the unintended and unexpected implications such as public expectations of law enforcement standards with respect to police presence and response.

In a 2013 FBI Bulletin article on *Predictive Policing: Using Technology to Reduce Crime*, Santa Cruz Police Department emphasised that technology could supplement but never supplant the innate attributes of effective law enforcement such as good investigative instincts, Humint and community engagements. Undaunted adversaries might adapt their tradecraft to outsmart electronic surveillance. For example, the Bastille Day attack in Nice occurred despite the city being known as the "CCTV capital" of France.

At present, while the AI in Smart CCTVs can highlight potential security concerns, it cannot yet perform investigative tasks like assess the intent and capability of suspects. Overreliance on technology might also affect the officers' alertness to danger and regularity of face-to-face interactions with people on the streets. Thus, an intermediate knowledge of smart technology is now critical in the skillset of officers to make them both tech and street savvy.

Smart CCTVs will henceforth have a critical role in the coming years in securing cities as well as in homeland security. Its proliferation would expectedly raise privacy concerns, and its omnipresence could inadvertently create the illusion of "gated communities" and increase complacency in terms of personal security.

Subject to a city's socio-cultural context, legislation such as the Data Protection Act in United Kingdom would help to assuage privacy concerns by regulating the responsible use of CCTVs. A healthy community partnership, such as in Singapore, would help the public to acknowledge the necessity of Smart CCTVs for the collective good and that both community vigilance and Smart CCTVs are concomitant and essential aspects of enhanced crime prevention and security strategies.

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.