SMART CCTVS FOR SECURE CITIES: POTENTIALS AND CHALLENGES

Policy Report
July 2017

Muhammad Faizal Bin Abdul Rahman

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

POLICY REPORT

SMART CCTVS FOR SECURE CITIES: POTENTIALS AND CHALLENGES

Muhammad Faizal Bin Abdul Rahman

July 2017

TABLE OF CONTENTS

Executive Summary

The operating environment for law enforcement particularly in cities[1] has grown more complex over the last decade. Security threats emanate from both traditional and non-traditional sources, emerging technologies give rise to new forms of crimes, and public demand for more agile responses make policing extremely challenging.

Leveraging new technologies is one key way in which law enforcement has responded to these challenges. In particular, the integration of smart technologies with regular closed-circuit televisions (CCTVs), otherwise known as Smart CCTVs, is envisaged to help law enforcement improve situational awareness as well as obtain additional sources of data for analysis or investigation. Yet, not much has been written about this emerging technology. As such, this exploratory study aims to: (i) examine how Smart CCTVs can be used to enhance law enforcement capabilities; (ii) identify issues and challenges associated with that use; and (iii) examine approaches to mitigate such challenges.

Upon examination, this study has found that Smart CCTVs can enhance law enforcement capabilities in four ways. They can: (i) act as a force multiplier; (ii) support police patrols; (iii); overcome human limitations; and (iv) support crisis and emergency management. As Smart CCTVs are powered by Artificial Intelligence (AI) and Machine Learning (ML), it is argued that they should not be regarded simply as tools for law enforcement, but rather as "partners".

With that, the challenges associated with the use of Smart CCTV for law enforcement include: (i) cybersecurity issues; (ii) adaptive and resolute adversaries; (iii) operational surprises; and (iv) an overreliance on the technology.

As such, approaches to mitigate these challenges include: (i) a multi-pronged cybersecurity strategy that focuses on resilience rather than deterrence; (ii) empowering law enforcement officers with new skill sets; (iii) experimenting with plausible security scenarios to optimally integrate the use of Smart CCTVs into patrol operations, investigations and intelligence; (iv)

[1] In this report, cities refer to both: (a) large and major urban centres (e.g. Stockholm, New York, London and Beijing) in countries; and (b) sovereign city-states (e.g. Singapore and Monaco)

ensuring that the adoption of technology is done in tandem with community partnership; and (v) deepening partnership with the private sector in terms of both regular[2] CCTV and Smart CCTV surveillance.

[2] This refers to existing CCTVs which are either (i) analogue or (ii) full digital systems that allow remote storage and viewing using Internet Protocol (IP), but have not incorporated or are in the early stages of incorporating AI capabilities.

1. Introduction

The nature of crime and security threats, such as transnational crime and urban terrorism, will evolve as the confluence of growing urbanisation and emerging technologies start to change the physical and socioeconomic character of cities.[3] Current threats may take new forms even as emergent threats emanate from both traditional and non-traditional sources. Coupled with greater public scrutiny and demand for more agile responses, the operating environment is envisioned to be extremely challenging for law enforcement.

Many cities across the world have already begun leveraging surveillance technology, most notably CCTVs, to enhance situational awareness for the early detection of potential threats, as well as to collect data for post-incident investigation and analysis. CCTVs have been instrumental in solving high-profile terrorist and criminal cases in Singapore[4] and abroad such as the Boston Marathon bombings in 2013,[5] London riots in 2011,[6] London bombings in 2005,[7] and the murder of toddler James Bulger in Britain in 1993.[8] Moreover, CCTVs complement police patrols and community watch programmes by functioning as a visible "eye in the sky" that acts as a deterrent.[9]

[3] Franz Vanderschueren, UN-HABITAT/Global Network on Safer Cities, "The Evolution and Challenges of Security within Cities", August 2013, UN Chronicle, Vol. L, No. 2 2013, https://unchronicle.un.org/article/evolution-and-challenges-security-within-cities

[4] Tan Tam Mei, "Committing a crime? Smile, you're on police camera", 31 October 2015, The New Paper, http://www.tnp.sg/news/singapore/commiting-crime-smile-youre-police-camera

[5] Anthony Bergin, "Boston tells us not to be blind to CCTV's uses", 29 April 2013, The Sydney Morning Herald, http://www.smh.com.au/comment/boston-tells-us-not-to-be-blind-to-cctvs-uses-20130428-2imkl.html

[6] Olivia Williams, "England Riots Changed Public Attitudes towards CCTV, Survey Claims", 25 October 2011, The Huffington Post, http://www.huffingtonpost.co.uk/2011/10/25/england-riots-support-for_n_1030428.html

[7] Will Knight, "CCTV footage shows London suicide bombers", 13 July 2005, New Scientist, https://www.newscientist.com/article/dn7669-cctv-footage-shows-london-suicide-bombers/

[8] Jane Cornwell, "The boys who killed James Bulger", 21 July 2016, The Sydney Morning Herald, http://www.smh.com.au/lifestyle/life-and-relationships/real-life/the-boys-who-killed-james-bulger-20130208-2e2nd.html

[9] Ibid

Singapore was an early adopter of using CCTVs to enhance policing.[10] In 2003, the Singapore Police Force introduced the Public Camera Zone (PCZ) project to provide surveillance of strategic commercial precincts.[11] The Hawk Eye Remote Observatory System introduced in 2013 comprises high-rise CCTV cameras that are capable of capturing faces and vehicle number plates,[12] and complements the existing street-level PCZ initiative.[13] The unified CCTV monitoring system integrates data from external CCTV cameras in the public transport network and the Integrated Resorts to support frontline policing.[14] The most extensive ongoing project is the Police Cameras (PolCam) initiative which has seen the installation of over 62,000 cameras at some 10,000 public housing blocks thus far.[15]

In light of the contemporary threats and operational challenges mentioned at the start, a more efficient approach towards surveillance and video data analysis has become necessary. This is because the increasingly voluminous footage captured from CCTV cameras cannot be efficiently processed and analysed due to manpower constraints.[16] Advances in the field of AI and ML[17] have resulted in the creation of Smart CCTVs that are envisaged to address these constraints.

[10] Edric Sng, "How can we keep Singapore safe and secure? Ministries unveil long-term plans", 18 Jan 2016, Channel News Asia, http://www.channelnewsasia.com/news/business/how-can-we-keep-singapore/2435302.html

[11] Lim Yan Liang, "More 'eyes' on the ground for police", 3 May 2014, The Straits Times, http://www.straitstimes.com/singapore/courts-crime/more-eyes-on-the-ground-for-police

[12] Muhammad Alif Bin Sapuan, "Ready for the Future", Police Life Special Edition (Police Week 2013), p. 29

[13] Lim Yan Liang and Lim Min Zhang, "Hawk-eye cameras to keep close watch on the city, able to zoom in on faces & cars", 4 May 2013, The Straits Times, http://www.straitstimes.com/singapore/hawk-eye-cameras-to-keep-close-watch-on-the-city-able-to-zoom-in-on-faces-cars

[14] Singapore Budget 2011, Ministry of Home Affairs, 18 Mar 2011, http://www.singaporebudget.gov.sg/budget_2011/expenditure_overview/mha.html

[15] Dean Koh, "EXCLUSIVE – Enhancing public safety through ICT technologies at the Singapore Police Force (SPF)", 12 June 2017, OpenGov, http://www.opengovasia.com/articles/7691-exclusive-enhancing-public-safety-through-ict-technologies-at-the-singapore-police-force-spf

[16] Tang See Kit, "Long hours, thankless job: Singapore's security sector struggles to secure talent", 10 January 2017, Channel News Asia, http://www.channelnewsasia.com/news/singapore/long-hours-thankless-job-singapore-s-security-sector-struggles/3422890.html

[17] Machine Learning is a type of Artificial Intelligence (A.I) that provides computers with the ability to learn without being explicitly programmed. The term was first defined in 1959 by the late Arthur Samuel who was a computer scientist known as a pioneer of A.I research

Smart CCTVs are systems comprising of various digital cameras that are web-connected (IP-enabled)[18] or connected over a wireless mesh network.[19] The in-built AI technology automates real-time monitoring and improves analytics of recorded footage. The system is linked to other types of databases, which help facilitate the identification of individuals and objects. Among the key features of Smart CCTVs are: (i) facial recognition (physical biometrics); (ii) detection of anomalous behaviour and gait (behavioural biometrics);[20] (iii) detection of unattended objects; (iv) vehicle license plate recognition; (v) crowd and directional flow detection; and (vi) tracking of persons and objects.[21]

Smart CCTVs will have a profound impact on law enforcement. The laborious tasks of video monitoring and analytics can be performed more efficiently and intelligently by machines. This leaves officers more time to perform other complementary functions like community engagement and attend to new offences (e.g. tech-based crime). In this respect, this report argues that law enforcement agencies should not regard Smart CCTVs simply as tools to enhance operations, but rather as “partners” whose adoption requires a strategic approach.

Despite Smart CCTVs’ value, not much has been written about the strategic approach in adopting this emerging technology from the perspective of law enforcement agencies. This exploratory study was undertaken as a result, and aims to: (i) examine how Smart CCTVs can be used to enhance law enforcement capabilities; (ii) identify issues and challenges associated with that use; and (iii) examine approaches to mitigate such challenges.

This study is qualitative and draws on the reviews of publicly available journals and industry reports, analysis of news articles, and insights that could be gleaned when invited experts consult with public agencies.

[18] Leon Spencer, “Smartphone surveillance on the rise for SMBs”, 10 June 2016, ZDNet, http://www.zdnet.com/article/smartphone-surveillance-on-the-rise-for-smbs/

[19] Bernard Scaglione, “How Cities Use Mesh Networks for Surveillance”, 4 September 2012, Security Magazine, http://www.securitymagazine.com/articles/83468-how-cities-use-mesh-networks-for-surveillance

[20] Chaurasia, Yogarajah, Condell, Prasad, McIlhatton and Monaghan, “Countering terrorism, protecting critical national infrastructure and infrastructure assets through the use of novel behavioural biometrics”, 14 January 2016, Behavioural Sciences of Terrorism and Political Aggression, pp. 198 – 199

[21] Schlehahn, Hansen and Lamina, “Report on Surveillance Technology and Privacy Enhancing Design”, Executive Summary, June 2013, SurPRISE consortium, European Union, p. iv

The report is divided into three sections that correspond to its aims. Section two identifies four primary ways in which Smart CCTVs can enhance law enforcement capabilities. Section three discusses some of the issues and challenges associated with the use of Smart CCTVs for law enforcement. Section four follows up by recommending several approaches that may help optimise the utility of Smart CCTVs, as well as addresses the issues and challenges.

2. Enhancing Law Enforcement Capabilities

This section identifies four primary ways in which Smart CCTVs can enhance law enforcement capabilities. Smart CCTVs can: (i) act as a force multiplier; (ii) support police patrols; (iii) overcome human limitations; and (iv) support crisis and emergency management.

2.1 Act as a force multiplier

The AI technology driving Smart CCTVs enhances the camera's ability to better scrutinise the landscape for anomalies, which makes it extremely useful for threat detection.[22] Of significance is the facial recognition feature that can identify persons of interest with greater speed and accuracy.[23] Regarded as a form of 'silent technology', facial recognition is less intrusive as compared to other forms (i.e. fingerprints and iris recognition) of biometric recognition.[24] The technology is versatile, and can be integrated into existing CCTV systems, immigration clearance systems and law enforcement photo databases.[25]

As a "partner" to its human CCTV operators, Smart CCTVs can reduce the occurrence of human oversight pertaining to real-time video surveillance. As the AI technology learns and self-improves, it can potentially avoid errors commonly associated with human limitations. These include fatigue, declining attention span, inability to scrutinise multiple items simultaneously, and reduced vision due to environmental factors such as low lighting.[26] When fully automated,[27] Smart CCTVs can not only detect anomalies but more critically decide whether intervention by law enforcement officers is necessary, as well as decide on the mode of intervention required.

[22] John P. Mello Jr, "Qualcomm Unveils Muscle Camera for Surveillance Systems", 28 October 2015, Tech News World, http://www.technewsworld.com/story/82671.html

[23] "It's all about the face: Face Recognition", 2013, NEC Public Safety Whitepaper, p. 3, http://safecities.economist.com/wp-content/uploads/sites/5/2015/01/NEC-FR_white-paper.pdf

[24] Introna & Wood, "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems", 2004, Surveillance & Society, CCTV Special, Vol. 2, No. 2/3 (2004), p. 183

[25] "Next Generation Identification (NGI)", Federal Bureau of Investigations, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

[26] Dr. Mahesh Saptharishi, "The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology" , 25 August 2014, Wired.Com, http://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/

[27] It should be noted here that the move to full automation must consider the potential operational, legal and ethical implications that would inevitably emerge. See Koch, Matzner and Krumm, "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", European Journal of Law and Technology, Vol. 4, No. 2, 2013, pp. 1 – 2

2.2 Support police patrols

Smart CCTVs strongly complements human patrols. The intelligence that Smart CCTVs distils from real-time video data can support patrol officers' situational awareness as well as help them determine how best to respond to the threat.[28] Furthermore, with intelligence alerts from Smart CCTVs, officers can better discern whether to investigate anomalies or individuals. They would also be more prepared to face potential dangers from this intelligence. The efficacy, efficiency and safety of officers on the frontlines would be improved significantly with Smart CCTV intelligence.[29]

2.3 Overcome human limitations

Police patrols redeployed for other purposes during major crises can have adverse consequences on public order and crime.[30] For example, the London Metropolitan Police Service (Scotland Yard) noticed a significant increase in the number of street crimes in 2002. An internal study revealed that this was due to a major redeployment of police officers to Central London to assist counter-terrorism efforts following the 9/11 attacks in the U.S. which took place the year before.[31] Leveraging Smart CCTVs to complement, and in some circumstances replace police patrols is, particularly in this scenario, a viable solution.

In short, Smart CCTVs can be used to help manage some of the operational challenges related to police patrols such as manpower shortages and the redeployment of police officers during emergencies.

[28] Prof. Elizabeth E Joh, "The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing", 26 October 2015, Harvard Law & Policy Review, Vol. 10, pp. 15 – 16

[29] Jeffrey E. Rose and Donald C. Lacher, "Managing Public Safety Technology: Deploying Systems in Police, Courts, Corrections, and Fire Organisations", 2017, p. 161

[30] The challenges arise due in part to: (a) the deployment of police officers is threat-dependent, and as such, they cannot be deployed at every location; (b) other locations such as residential areas may become more vulnerable as patrols are redeployed to 'higher risk' areas (e.g., commercial districts and tourist enclaves); and (c) police officers may be called upon to perform non-traditional policing functions (e.g., support counter-terrorism efforts). See Leslie W. Kennedy and Edmund F. McGarrell, Crime and Terrorism Risk: Studies in Criminology and Criminal Justice, (London, UK: Routledge, 2011), p. 78.

[31] Phillip Nettleton and David Taylor, "Yard blames terror duties for massive rise in crime" 17 April 2002, Evening Standard, http://www.standard.co.uk/news/yard-blames-terror-duties-for-massive-rise-in-crime-6310944.html

2.4 Support crisis and emergency management (man-made threats & natural hazards)

Smart CCTVs can support crisis and emergency management by enhancing two mission-critical capabilities: (i) the early warning system of public agencies; and (ii) the situational awareness of emergency responders on the frontlines. The enhancement of these capabilities would make cities more resilient according to the United Nations (UN) Habitat Programme's list of essentials for urban resilience.[32] The coastal city of Nice in France, for example, was designated in 2012 by the UN as a model resilient city for using its wide network of CCTV cameras for flood monitoring and crime prevention.[33]

Similarly, the expanded CCTV coverage at train stations[34] in Singapore enhances the ability of rail operators and the Land Transport Authority to intelligently monitor commuter traffic as well as incidents. This enables the authorities to better manage crowds and the overall situation especially during emergencies.[35]

In the aftermath of security incidents such as terrorist attacks, Smart CCTVs can potentially facilitate the return to a state of normalcy by expediting post-incident management and investigations, complementing enhanced patrols to prevent further attacks, and in some cases identify perpetrators. This was demonstrated in the 2005 London bombings, 2013 Boston Marathon bombings, and the 2011 London Riots (Operation Withern) where CCTVs were central in the identification and apprehension of the perpetrators.

Given its ubiquity and significance in the resilience of cities, CCTVs, and soon Smart CCTVs, will be regarded as the fifth utility alongside other critical nodes of public infrastructure (i.e. water, gas, electricity and telecommunications).[36]

[32] "How can cities become more resilient", UN-Habitat, http://unhabitat.org/urban-themes/resilience/?noredirect=en_US

[33] "The Resilient City, the other Aspect of the Smart City", 30 May 2016, Brussels Smart City, http://smartcity.brussels/news-139-the-resilient-city-the-other-aspect-of-the-smart-city

[34] "Award of CCTV Works Contracts for Stations of the North-South-East-West and North-East Lines", 28 August 2008, Land Transport Authority, https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=1992

[35] Sophie Hong, "MRT cameras not just for security", 30 November 2011, My Paper, http://news.asiaone.com/News/AsiaOne+News/Singapore/Story/A1Story20111130-313462.html

[36] Stuart Croft, "The Everyday Resilience of the City: How Cities Respond to Terrorism and Disaster", pp. 72 – 79, 106 – 109

3. Issues and Challenges

This section discusses some of the issues and challenges associated with the use of Smart CCTVs for law enforcement. The focus is on strategic issues that can impede the potential utility of Smart CCTVs, rather than technical performance and ethical challenges such as privacy and automated discrimination, which warrant separate studies.

On privacy in particular, the issue has long been debated upon since the 1970s.[37] However, given its pivotal role in law enforcement, denouncing the use Smart CCTVs would be erroneous as its benefits far outweigh the concerns. As modern life becomes more digitised, people may become more amenable to sharing and collection of data (by state and corporations) as a normal aspect of life.[38] Legislation such as the Data Protection Act in the United Kingdom and the Personal Data Protection Act in Singapore which regulate the responsible use of CCTVs, and a healthy community partnership such as in Singapore, could help assuage some, if not all, privacy concerns. These concerns are summarised in Appendix E.

3.1 Cybersecurity issues

While smart technologies such as Smart CCTVs are expected to bring benefits, they also introduce vulnerabilities. Interconnectivity, by nature, enlarges the potential cyberattack surface of cities and agencies. Adversaries can exploit novel attack vectors that come with these vulnerabilities to commit hostile acts such as cyber espionage or scour for other weaknesses within the security architecture of cities.[39] Popular websites like Twitter, Spotify and Reddit have experienced such attacks in October 2016 when their operations were disabled in a massive distributed denial of service (DDoS) attack launched through web-enabled CCTV cameras that had been commandeered by hackers.

[37] Wright. D, "Sorting out smart surveillance", 2010, Computer Law and Security Review, p. 11

[38] "Digital Life in 2025: The Future of Privacy", December 2014, Pew Research Centre, pp. 11 – 20, http://www.pewinternet.org/files/2014/12/PI_FutureofPrivacy_1218 141.pdf

[39] Bryce Boland, "Networks on Fire: Defending Critical Government Networks", Cybersecurity – Some Critical Insights and Perspectives, 1 November 2014, pp. 14 – 15

Cities which have embarked on the smart city bandwagon can become more vulnerable as any cyberattack on their smart infrastructure could also disable their Smart CCTVs.[40] In order to weaken states, adversaries can also specifically target Smart CCTVs given its crucial role as a line of defence against threats, and its strategic status as the fifth utility of public infrastructure.[41] For example, the hacking of the police-operated CCTV system during the 2015 Southeast Asian Games in Singapore suggests that CCTVs are vulnerable to attacks, and can be targeted by individuals with malicious intentions.[42]

On a related point, the hacking of a CCTV system underscores the need to mitigate insider threats. Ordinarily, the risk of hacking into police-operated CCTVs is low as the agency would, presumably, have robust measures (e.g. network segmentation and firewalls) in place to protect the assets.[43] Expectedly, these protections would be ineffective if the attacker is from the organisation itself or has access to the system (e.g. a contractor).

Apart from criminal motives, there could be instances where tampering with CCTV systems is designed to undermine public confidence. This could be part of a larger information warfare campaign carried out to undermine the targeted city or country without resorting to kinetic attacks.[44] For example, Hezbollah, a militant organisation, claimed in February 2016 that it had successfully hacked into CCTV systems in Israel, particularly those around government buildings and popular public venues. Although unverified, the claim was designed to cause panic and doubt within the Israeli society.[45]

[40] Tereza Pultarova, “Smart city cyberattack extremely likely, IT professionals fear”, 22 September 2016, Engineering and Technology, https://eandt.theiet.org/content/articles/2016/09/smart-city-cyber-attack-extremely-likely-it-professionals-fear/

[41] Derek Major, “Hackers target local law enforcement systems”, GCN – Technology, Tools and Tactics for Public Sector IT, 1 February 2016, https://gcn.com/blogs/pulse/2016/02/police-systems-vulnerabilities.aspx?m=1

[42] Vanessa Paige Chelvan, “Engineering director gets 8 months jail for SEA Games CCTV hack”, 16 August 2016, Channel News Asia, http://www.channelnewsasia.com/news/singapore/engineering-director-gets/3047220.html?cid=FBcna

[43] Dr. Eric Cole, “Insider Threats in Law Enforcement”, August 2014, SANS Whitepaper, SANS Institute, p. 2

[44] Professor David Stupples, “What is information warfare”, 3 December 2015, World Economic Forum, https://www.weforum.org/agenda/2015/12/what-is-information-warfare/

[45] “Hezbollah: We hacked into Israeli security cameras”, 20 February 2016, Times of Israel, http://www.timesofisrael.com/hezbollah-we-hacked-into-israeli-security-cameras/

3.2 Adaptive adversaries

As Smart CCTVs reshape the operating landscape, adversaries — criminals and terrorists — can be expected to alter their behaviour and adapt.[46] They could, for instance, leverage the same technologies to perpetrate attacks and commit crimes. For example, they could use Unmanned Aerial Vehicles (UAVs) or drones[47] instead of human operatives to conduct pre-attack reconnaissance of potential targets to minimise the risk of detection by street-level Smart CCTVs.[48] Adversaries could also discover and exploit patterns in police responses, as well as cultivate individuals working for law enforcement agencies.[49] Criminal groups in India for instance, reportedly used their own CCTV cameras to conduct counter-surveillance on police officers. They also used the intelligence gathered to evade police detection.[50]

Existing studies suggest that it is possible to evade detection by Smart CCTVs[51] through manipulating the environment[52] or by clever disguise.[53] For example, Ahmad Khan Rahimi who was responsible for the 2016 New York bombings was reported to have used construction work near the target sites to avoid being seen by CCTV cameras.[54] In terms of disguises, anti-surveillance textiles designed to camouflage its wearer by confusing facial recognition algorithms in Smart CCTVs are already being developed by privacy advocates.[55]

[46] Dr. Grant Wardlaw, “The Future and Crime: Challenges For Law Enforcement”, March 1999, Australian Institute of Criminology, http://aic.gov.au/media_library/conferences/outlook99/wardlaw.pdf, p. 10

[47] Danielle Muoio, “ISIS may be using DJI consumer drones for surveillance”, 13 January 2016, Tech Insider, http://www.techinsider.io/oxford-research-group-warns-of-terrorist-drone-use-by-isis-2016-1

[48] Christopher Flaherty, “The Role of CCTV in Terrorist TTPs: Camera System Avoidance and Targeting”, 9 November 2015, Small Wars Journal, p. 7

[49] Treverton, Wollman ,Wilke and Lai, “Moving Toward the Future of Policing”, 2011, RAND Corporation, National Security Research Division, pp. 3, 104 – 105

[50] PTI, “Role Reversal: Police Baffled As Criminals Use CCTV To Monitor Them”, The Indian Express, http://indianexpress.com/article/india/india-news-india/role-reversal-police-baffled-as-criminals-use-cctv-to-monitor-them-2790172/

[51] Cade Metz, “How To Fool AI Into Seeing Something That Isn’t There”, 29 July 2016, WIRED, https://www.wired.com/2016/07/fool-ai-seeing-something-isnt/

[52] Daniel Bates, “EXCLUSIVE: Manhattan bombing suspects could have used CONSTRUCTION WORK to hide from CCTV cameras”, 18 September 2016, Daily Mail, http://www.dailymail.co.uk/news/article-3795572/Manhattan-bombing-suspects-used-CONSTRUCTION-WORK-hide-CCTV-cameras.html

[53] Paul Rubens, “Can disguises fool surveillance technology”, 18 November 2014, BBC, http://www.bbc.com/future/story/20121207-do-disguises-fool-surveillance

[54] Daniel Bates, “Exclusive: Manhattan bombing suspects could have used construction work to hide from CCTV cameras”, 18 September 2016, http://www.dailymail.co.uk/news/article-3795572/Manhattan-bombing-suspects-used-CONSTRUCTION-WORK-hide-CCTV-cameras.html

[55] http://www.dailymail.co.uk/sciencetech/article-4088076/The-anti-surveillance-clothing-hides-people-security-cameras-using-ghostly-patterns.html

Adversaries may also use diversionary tactics like staging incidents near Smart CCTVs to distract law enforcement officers while the actual crime is being perpetrated elsewhere.[56] Such tactics could also be used to test police responses so as to discover vulnerabilities that can be exploited.[57]

3.3 Resolute terrorists are not deterred by Smart CCTVs

As a visible security measure, Smart CCTVs can be a strong deterrent against ordinary criminals and anti-social behaviours assuming that they are rational actors who would act only if they perceive that the fruits of crime (e.g. financial gains) outweigh the risks of offending (e.g. arrest, fines and imprisonment).[58] However, the decision-making process of terrorists may be more complex given the interplay of motivations (politico-religious issues, psychological issues, etc.).

Smart CCTVs may not be effective in deterring crimes like mass homicides or suicide attacks. The Bastille Day attack in France suggests that the attacker was not deterred by the city's numerous CCTVs. The attack also suggests the inherent limitation of CCTVs, that is, they can "record crimes [attacks] but can't prevent them".[59] As French criminologist Alain Bauer remarked: "cameras don't get out from the poles to arrest terrorists with their little hands".[60]

A location that is heavily protected and monitored by Smart CCTVs (e.g. a government building) may be regarded as a high-value target to an ambitious adversary.[61] A successful attack on such a target: (i) exposes flaws and weaknesses in the system; (ii) has significant propagandistic value; and (iii) generates other challenges (e.g. undermining social cohesion and confidence

[56] Ashley Craig, "Wal-Mart Fire a Cover for Robbery, police say", 2 March 2016, Charleston Gazette Mail, http://www.wvgazettemail.com/news/20160302/wal-mart-fire-a-cover-for-robbery-police-say

[57] Douglas Page, "Police Behaving Predictably: The Other Enemy", February 2009, Officer.Com, http://www.officer.com/article/10233886/police-behaving-predictably-the-other-enemy

[58] Ben Brown, "CCTV in Town Centres: Three Case Studies", 1955, Police Research Group, Crime Detection and Prevention Series Paper No. 68, London: Home Office Department, p. 5. The "rational choice" theory (Clarke and Cornish, 1985) argues that offenders are involved with making decisions and choices exhibit a measure of rationality. Offenders would be deterred by cameras only if they interfered in some way with the likelihood of offenders benefitting from this behaviour within that particular context.

[59] Daniel Estrin, "Despite Heightened Security, France Struggles To Cope With Terrorism", 19 July 2016, National Public Radio (NPD), http://www.npr.org/2016/07/19/486646217/despite-heightened-security-france-struggles-to-cope-with-terrorism

[60] Ibid

[61] "Terrorist Targets", MI5 Security Service, United Kingdom, https://www.mi5.gov.uk/terrorist-targets

in the government).[62] The 9/11 attacks that targeted the U.S.' symbols of military power (Pentagon) and economic power (World Trade Centre) is a good example.

3.4 Operational surprises

Although using Smart CCTVs may bring immediate operational gains, the unanticipated knock-on issues can surprise law enforcement agencies. The adverse public reactions and responses to increased police surveillance through the use of Smart CCTVs is a case in point.[63] The Lucy Parsons Labs, a Chicago-based group of online activists, have developed a web tool called OpenOversight to protest police surveillance of individuals connected to the "Black Lives Matter" campaign.[64] The tool enables users to collect and publicise private information (photographs, names, addresses, etc.) of police officers on social media platforms. The availability of the tool has alarmed Chicago police as operations and the lives of police officers and their families have been put at risk. Hence, such operational surprises can complicate future operations.

3.5 Overreliance on Smart CCTVs and impact on policing and community vigilance

The growing ubiquity of Smart CCTVs can potentially influence human behaviour and attitudes in unintended and unexpected ways. The focus here is on police officers and the general public.

While smart technology allows law enforcement officers to leverage machines (Smart CCTVs) to perform laborious surveillance tasks more efficiently and intelligently, overreliance on the technology may have negative implications on: (i) how officers do their jobs; and (ii) how they engage and interact with the community.[65]

[62] Prof. Andrew Silke, "The Psychology of Counter-Terrorism", 2011, pp. 164 – 169

[63] "Moving Toward the Future of Policing", 2011, RAND Corporation, National Security Research Division, pp. 107 – 108

[64] George Joseph, "Chicago Activists Turn the Tables on Police Surveillance", 25 October 2016, City Lab, http://www.citylab.com/crime/2016/10/crowdsourcing-police-accountability/504650/

[65] Yvonne Lim and Nadia Samdin, "People, not tech, key to foiling terror attacks: Former head of US Homeland Security", 13 April 2016, Channel News Asia, http://www.channelnewsasia.com/news/singapore/people-not-tech-key-to/2691284.html

Being overly reliant on Smart CCTVs can negatively impact policing functions in the following ways: (i) officers may feel less inclined to hone their investigative instincts and problem-solving skills since the cameras are already performing these tasks;[66] (ii) officers do not learn important tradecraft skills that can only be picked up through on-job-training and on-the-ground experience;[67] and (iii) traditional policing skills may not be taught to officers.[68] Such overreliance can also adversely affect police engagement with the community, which is an important part of policing even in contemporary times.[69] As Smart CCTVs can perform patrol functions, the requirement for regular police patrols is reduced or in some cases eliminated. As officers are no longer required to conduct face-to-face interaction or engagement with the community, they may be perceived as strangers and untrustworthy as a consequence.[70]

Public expectations about Smart CCTV capabilities are also problematic. A 2001 study by the Australian Institute of Criminology on surveillance cameras and their effectiveness in crime prevention revealed that many individuals perceive CCTVs to be a panacea for crime reduction and prevention.[71] The increased use of Smart CCTVs may give the public a false sense of security, which is a serious consequence given the recent terror attacks on public spaces with CCTVs.[72] The call for greater community vigilance and reporting of suspicious activities and individuals to police may be ignored if more people perceive that Smart CCTVs are keeping them safe.

[66] Conversation with Mr Tim Godwin, CENS DVP, January, 2017.

[67] Ibid

[68] "The U.S. Naval Academy just resumed training officers to navigate by sextants. Historically the only way to determine a ship's location at sea, this technique is being taught again both as a backup in case cyber attackers interfere with GPS signals and to give navigators a better feel of what their computers are doing". See Jonathan Coopersmith, "Is technology making us dumber or smarter? Yes", 17 June 2016, The Conversation, https://theconversation.com/is-technology-making-us-dumber-or-smarter-yes-58124

[69] Tim Godwin, 'CENS Seminar on Smart CCTV and National Security Threats: Surveillance, Privacy and Public Trust', 17 January, 2017.

[70] Ibid

[71] Adrienne Isnard, "Can Surveillance Cameras be Successful in Preventing Crime and Controlling Anti-Social Behaviours", 2001, Australian Institute of Criminology, p. 2

[72] Stutzer and Zehnder, "Is camera surveillance an effective measure of counterterrorism", 29 February 2012, Defence and Peace Politics, pp. 8, 10 – 11

4. Optimising Smart CCTVs

This section recommends several approaches that may help optimise the utility of Smart CCTVs, as well as addresses the issues and challenges identified in the previous section.

4.1 Securing Smart CCTVs

Defence against cyberthreats often requires a comprehensive strategy that focuses on resilience rather than deterrence.[73] Employing this same approach to protecting Smart CCTVs from cyberattacks requires protection of various components that form the Smart CCTV infrastructure. These include cameras, networks, databases and video content analysis tools.

According to a study on Smart Insiders by the University of Oxford, the cyberthreat landscape has grown more onerous especially with the proliferation of the Internet-of-Things. Smart devices can potentially facilitate insider attacks and circumvent traditional security measures that are more effective against external attacks. Therefore, when developing a comprehensive risk assessment of plausible cyberattacks that can affect Smart CCTVs, analysis of the potential threat actors, attack vectors, outcomes of attacks, and the assets (i.e. CCTV infrastructure, data, personnel and agency's reputation) targeted, should be included.[74]

4.1.1 Redundancies and red teaming

Redundancies can be built in, where necessary, to mitigate the debilitating effects of system failures. This will also ensure the continuity of critical frontline functions that are supported by Smart CCTVs.[75] Determining where redundancies should be built can be done through red teaming exercises.[76]

[73] Daniel Dobrygowski, "Cyber resilience: everything you (really) need to know", 8 July 2016, World Economic Forum, https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/

[74] Cyber Security Centre, Department of Computer Science, University of Oxford, UK, "Smart Insiders: Exploring the Threat from Insiders using the Internet-of-Things", September 2015, International Workshop on Secure Internet of Things 2015 (SIoT 2015), European Symposium on Research in Computer Security (ESORICS 2015), p. 7

[75] Ted G. Lewis, "Critical Infrastructure Protection in Homeland Security", 2006, pp. 239 – 241

[76] Kaspersky Lab demonstrated that Red teaming is central to cybersecurity as "the 'good guys' need to test security before 'the bad guys' can use it for malicious intent". See Vasili Hioureas and Thomas Kinsey, "Does CCTV put the public at risk of cyberattack", Secure Smart Cities, p. 8, http://securingsmartcities.org/wp-content/uploads/2015/05/CCTV_research_final.pdf

Such exercises simulate attacks and worse-case scenarios, which reveal inherent weaknesses and areas that require strengthening.[77]

4.1.2 Interdependencies

The interdependencies between Smart CCTVs and other essential services and infrastructure can be mapped out in order to develop measures that can alleviate vulnerabilities that are not obvious. For example, a prolonged disruption of the city's energy grid can adversely affect the ability of Smart CCTVs to function.[78]

In addition, the interdependencies between cities can be mapped as digital interconnectivity has diminished the physical boundaries between them. The Economist Intelligence Unit emphasised in a 2015 *Safe Cities* report that good cybersecurity in one city may not insulate it from compromised security in another.[79] Hence, addressing cross-border cyberthreats on Smart CCTVs calls for international cooperation between cities and states, which may be pursued through existing bilateral and regional security platforms that can include cooperation in science and technology matters.[80]

4.1.3 Intelligence

Intelligence is crucial to determining the response needed to mitigate the impact of: (i) Smart CCTV failure during frontline operations; (ii) monitoring manoeuvres of adversaries in the infiltrated system; (iii) pre-empting subsequent cyberattacks; and (iv) assessing if the cyberattack is a diversionary move that may be part of a larger hostile stratagem. The stratagem may comprise of: (i) attacking Smart CCTVs to open alternative pathways to infiltrate other sensitive Information and Communications Technology (ICT) systems in law enforcement agencies;[81] and (ii) attacking other ICT systems to open a pathway to infiltrate Smart CCTVs.

[77] John Dewar, "Cyberterrorism Attacks on Police Departments", 3 March 2010, The Police Chief, Vol. LXXVII, International Association of Chiefs of Police, p. 4, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=print_display&article_id=2037&issue_id=32010

[78] Sandeep Dutta and Shalabh Srivastava, "Intelligent Cities: How smart grids will be the key building block", 2016, Accenture Business Journal for India, p. 4

[79] "The Safe Cities Index 2015: Assessing Urban Security in the Digital Age", January 2015, the Economist Intelligence Unit. p. 15, http://safecities.economist.com/report/safe-cities-index-white-paper/

[80] For example, see "Agreement between the Government of The United States of America and the Government of Singapore on Cooperation in Science and Technology for Homeland/Domestic Security Matters", https://www.dhs.gov/xlibrary/assets/agreement_us_singapore_sciencetech_cooperation_2007-03-27.pdf

[81] John Leyden, "Ironic: CCTV systems slide open a backdoor into your biz network", 14 March 2016, The Register, http://www.theregister.co.uk/2016/03/14/cctv_insecurity_rife/

In developing intelligence on possible cyberthreats to Smart CCTVs, agencies need both skilled cybersecurity professionals and AI-enabled analytical tools.[82] Agencies would also need to ensure proper coordination (intra-agency and inter-agency) when monitoring the manoeuvres of adversaries in infiltrated systems. A lack of coordination may give adversaries the space to retaliate or withdraw if they realise that they are being monitored.

An insider management threat plan to prevent and investigate breaches from within is crucial in minimising insider attacks and internal breaches. Agencies may need to focus on both employees and contractors by raising their security and cyber hygiene awareness through training programmes, but also review internal monitoring processes.[83]

In pre-empting the attacks, agencies may need to collaborate with academia and the private industry to study the possible insider threats that may be facilitated by smart devices. The study may include developing indicators that can aid in detecting anomalies that may signal possible attacks.[84]

4.2 Empowering law enforcement officers

While Smart CCTVs may not be able to stop terrorist attacks that are already in motion, advances in ML can potentially enable Smart CCTVs to better detect complex and obscure patterns that are indicators of imminent attacks. As terrorists and other adversaries are adaptive by nature, attempts to outsmart Smart CCTVs should be expected. Hence, it is vital for human officers like CCTV operators and patrol officers to adopt new skill sets.

In this regard, it will be necessary for officers to have an intermediate knowledge of smart technology to make them both tech and street savvy. This would enable them to use both technology and the community for intelligence-gathering and other policing work. For example, intelligence derived from Smart CCTVs can be instrumental in identifying areas that would benefit from more police patrols. Also, such intelligence could identify human assets – people who are living or working near crime hotspots – who could be approached for information or assistance.

[82] Mark Pomerleau, "Cyber-threat hunt teams would benefit from machine assistance", 4 November 2016, C4ISRNET, http://www.c4isrnet.com/articles/how-to-observe-threats-on-your-network

[83] Lippert and Walby, "Municipal Corporate Security and the Intensification of Surveillance", 2012, Surveillance and Society, Vol. 9, No. 3, p. 318

[84] Dr. Eric Cole, "Insider Threats in Law Enforcement", August 2014, SANS Whitepaper, SANS Institute, p. 2

Furthermore, knowledge of smart technology may help officers to better appreciate the capabilities and limitations of Smart CCTVs, therefore preventing an overreliance of technology. To ensure the currency and usefulness of the knowledge, agencies may need to monitor how the use of Smart CCTVs influences the behaviour and attitudes of their officers over time.

It will be beneficial to first determine how best to use Smart CCTVs in daily operations to enhance law enforcement. This can be done by assessing the circumstances and types of crime and threats that can be best monitored, investigated or mitigated with the use of Smart CCTVs. The overarching objective of these exercises is to optimally integrate the use of Smart CCTVs into patrol operations, investigations and intelligence.

Operational risks and trade-offs that may arise from the increased use of Smart CCTVs can also be discerned from these exercises. Lessons learned can feed into the review and improvement of work processes, operational and information-sharing (within and between agencies) protocols. They can also enhance interoperability with other mission-critical systems such as criminal intelligence databases, and Command, Control and Communications (C3) systems. Related to interoperability with other databases, the efficacy of Smart CCTVs can potentially be enhanced if officers are able to enrich its data with images or footage collected from other sources. These sources include social media, crowdsourcing platforms,[85] and initiatives that tap on civilian-owned CCTVs that face public spaces.[86]

4.3 Community partnership and good will

As mentioned above, law enforcement agencies are empowered by the trust and goodwill of the communities they serve. This is particularly important in an era where public mistrust of law enforcement is high in certain societies.[87] Hence, using Smart CCTVs may provoke adverse reactions if the public perceive such moves to be against their interests.

[85] Crowdsourcing platforms launched by the Ministry of Home Affairs and Police Force in Singapore are the SG-Secure and Police@SG (i-Witness) smartphone apps.

[86] Laura Elizabeth Philomin, “Police gets extra eyes through 760 participating in-car cameras”, 18 May 2015, TODAY, http://www.todayonline.com/singapore/police-launch-vehicles-watch-programme-using-vehicle-cameras, An example in Singapore is the “Vehicle on Watch” project in which participating vehicle owners can share the video footages from their in-vehicle cameras with the Police as a form of wider neighbourhood watch.

[87] https://www.washingtonpost.com/investigations/survey-reveals-disconnect-between-police-and-public-attitudes/2017/01/10/65b24f3a-d550-11e6-a783-cd3fa950f2fd_story.html?utm_term=.c4e096bd5875

Therefore, it would be prudent for agencies to monitor public sentiments, and in so doing, manage expectations. More importantly, agencies must ensure that any misuse or abuse of this technology do not occur or is minimal at the very least. If transgressions do occur, culprits must be held accountable and disciplined to build trust. An example is the internal audit system that Singapore has in place to help detect malpractice and laws to mete out stern action against law enforcement officers who misuse access to ICT systems for personal gains or to advance malicious intents.[88]

Agencies need to continue investing heavily in building relationships with the community even as more resources are channelled to the adoption of smart technology. The message that both community vigilance and Smart CCTVs are concomitant and essential aspects of crime prevention and security strategies must be regularly emphasised. For example, the PolCam project in Singapore mentioned in the introduction is not implemented as a standalone or Smart Nation initiative only but as part of a comprehensive Community Policing System launched in 2012.[89]

Cultivating strong relationships with the community is key to sustaining public confidence in the agencies especially during emergencies. It fosters a deeper understanding of the community's concerns and environment, and also supports the collection of local intelligence from community sources.[90] Good local intelligence and public confidence may stand agencies in better stead when having to deal with operational surprises brought upon by technology.[91]

[88] Singapore takes a strong stance against computer misuse, See for example http://www.straitstimes.com/singapore/courts-crime/police-officer-fined-10000-for-illegal-search-on-computer-system

[89] http://www.straitstimes.com/singapore/polcams-and-carcams-play-key-role-in-fighting-crimes-police

[90] "Engagement and Communication", 23 October 2013, Authorised Professional Practice, College of Policing, UK, https://www.app.college.police.uk/app-content/engagement-and-communication/engaging-with-communities/#benefits-of-effective-engagement

[91] Brian A. Jackson, "Strengthening Trust between Police and Public in an Era of Increasing Transparency", October 2015, RAND Corporation, pp. 1 – 2 and 6, Information technology has affected the practice of policing in many ways, but, for the public, it has created the potential for new awareness of how police - from the department to the individual officer level - are doing their jobs. The relationships between (police) departments and the public will be tested more frequently — by every controversial video posted by a citizen or published analysis of newly available data questioning the effects of policing strategies — so police departments will have to be prepared.

4.4 Public-private partnership

Smart CCTVs have enhanced the surveillance capabilities of private sector security companies.[92] For example, Smart CCTVs are increasingly being used to monitor shopping malls, thus enabling better deployment of security manpower and detection of anomalies.[93] This presents more opportunities for public-private partnership in terms of co-developing technologies and information-sharing, and could extend beyond traditional areas of cooperation (e.g. operations, training and regulatory matters, and setting technical standards for CCTV systems).

4.4.1 Co-developing technologies

As technology is constantly evolving, the partnership must be underpinned by a well-defined and adaptable strategy that can provide a platform for law enforcement agencies and the private security sector to collaboratively research and co-develop technologies. Co-developing technologies would be highly advantageous as products or services will benefit from the joint expertise of the public and private sectors.[94]

4.4.2 Information-sharing

Another area of possible partnership is the sharing of CCTV footage for intelligence gathering and investigations.[95] As soft targets such as nightspots, educational institutes, tourist attractions and commercial premises are vulnerable to terrorist attacks, there is a need for law enforcement to access real-time footage from privately-owned CCTVs installed in these locations.[96] Although the footage from privately-owned CCTVs may vary in terms of quality and volume, it can still be useful for pre-incident monitoring and post incident analysis. With more private security companies adopting Smart CCTVs, it is useful for law enforcement agencies to harness private CCTV

[92] In this report, the private security sector refers to in-house security units and private security firms that are tasked to develop physical security solutions or/and manage the security of buildings and large-scale events.

[93] Koh Xing Hui, "Tech at malls to cut security manpower needs", 28 September 2016, The Straits Times, http://www.straitstimes.com/singapore/security-tech-at-malls-to-cut-manpower-needs-by-20-per-cent

[94] "Zim, China in smart security partnership", 21 January 2017, The Herald, http://www.herald.co.zw/zim-china-in-smart-security-partnership/

[95] Treverton, Wollman ,Wilke and Lai, "Moving Toward the Future of Policing", 2011, RAND Corporation, National Security Research Division, pp. 81 – 83

[96] Garret Ellison, "Police getting real-time access to private security cameras in downtown Grand Rapids", 29 June 2014, Michigan Live, http://www.mlive.com/news/grand-rapids/index.ssf/2014/06/police_getting_real-time_acces.html

footage in real time. For example, the CCTV systems of the Integrated Resorts in Singapore are linked to the police's Unified Close Circuit (CCTV) Monitoring System.[97]

Forming partnerships with the private sector to gain access to such footage may entail several challenges: (i) finding a willing partner including incentives for entering into partnership; (ii) ensuring minimal disruption to the partners' business operations when accessing their CCTVs; (iii) managing insider threats that may emanate from the partner's associates, employees, etc.; (iv) addressing legal or privacy issues that may arise from attempting to access CCTVs that monitor non-public spaces; and (v) addressing quality issues related to cameras and video footage.[98]

4.4.3 Pre-empting new threats and identifying new opportunities

More collaborative private-public partnerships can also help both sectors keep pace with technological advances to pre-empt possible challenges or threats (i.e. cyberattacks, safety of data, policy, legal and ethical issues) as well as identify new mutually beneficial opportunities.[99]

While public-private partnerships will certainly be challenging, there are examples of successful collaborative efforts. The State CCTV strategy of Western Australia is one such initiative. It "articulates a framework which facilitates" the sharing of data between private CCTV owners, the state government and law enforcement".[100] It does this through four elements: (i) a State-CCTV register that functions as a comprehensive database of CCTVs in the state; (ii) a set of criteria and policies that help the public and private sector adopt best practices in CCTV surveillance; (iii) encouraging and enabling "high-value" owners of privately-owned CCTVs to give the police direct, non-disruptive and real-time access to footage; and (iv) exploring

[97] Singapore Budget 2011, Ministry of Home Affairs, 18 Mar 2011, http://www.singaporebudget.gov.sg/budget_2011/expenditure_overview/mha.html, By linking strategic CCTV systems that are available in the public and private sectors to a central monitoring centre, SPF will have access to a larger network of CCTV systems from which images can be selected to meet its virtual policing needs.

[98] John S. Dempsey, "Introduction to Private Security", Second Edition, 2010, p. 363. The Private Sector Liaison Committee (PSLC) maintained by the International Association of Chiefs of Police (IACP) in the U.S develops projects that are designed to benefit both the law enforcement and private sector. These projects include developing guidelines for legal and ethical use of CCTV surveillance.

[99] Smaller companies may lack the resources to procure high-end CCTV systems.

[100] https://www.police.wa.gov.au/Our-Community/Western-Australian-State-CCTV-Strategy

mobile video sharing solutions to harness data collected from smart devices — including smartphones and tablets — used by the public.[101]

In sum, public-partnership is essential to achieving ubiquitous smart surveillance for homeland security by complementing law enforcement's Smart CCTVs with images and footage from the private security sector and the wider community.

[101] "WA Plans Integrated State-Wide CCTV By 2017", 9 February 2016, Security Electronics and Networks, http://www.securityelectronicsandnetworks.com/articles/2016/02/09/wa-plans-integrated-state-wide-cctv-2017

5. Conclusion

Smart CCTVs can potentially engender better situational awareness as well as more timely and actionable intelligence. This will enable law enforcement agencies to better address evolving crime and security threats that emanate from a more complex operating environment.

Essentially, advances in AI and ML would enable Smart CCTVs to be more than just a tool but a “partner” that supports human officers in patrol operations, investigations and intelligence. The improved situational awareness that Smart CCTVs can provide also enhances the resilience of cities by supporting early warning and emergency management capacities, and facilitates the return to normalcy in the aftermath of security incidents.

The potential utility of Smart CCTVs can be impeded by several challenges: (i) cybersecurity issues; (ii) adaptive and resolute adversaries; (iii) operational surprises; and (iv) an overreliance on the technology.

Approaches to address these challenges include: (i) a multi-pronged cybersecurity strategy that focuses on resilience rather than deterrence; (ii) empowering law enforcement officers with new skill sets; (iii) experimenting with plausible security scenarios to optimally integrate the use of Smart CCTVs into patrol operations, investigations and intelligence; (iv) ensuring that the adoption of technology is done in tandem with community partnership; and (v) deepening of partnership with the private security sector in the domains of both regular CCTV and Smart CCTV surveillance.

In sum, Smart CCTV technology is constantly evolving even as agencies seek to increasingly leverage it to transform their operations. There is therefore a need for continued research into its further development such as in the areas of public-private partnership, possible insider threats to Smart CCTV-enabled law enforcement functions, and how adversaries may adapt to evade Smart CCTVs.

Appendix A

Three Modes of Smart CCTV

Adapted from the article "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", European Journal of Law and Technology, Vol. 4, No.2, 2013

Modes of Use	Features
Full Automation	• Computer filters the information and makes the decision. • Computer recognises suspicious behaviour and decides whether intervention is necessary, as well as the type of intervention. • Entails more potential ethical and legal issues.
Partial Automation - Unblinkered	• Computer and human operator filter the information but human operator decides. • Suitable for security situations where false negatives and false positives can lead to serious problems. • Human operators can intervene if the computer does not deliver results.
Partial Automation - Blinkered	• Computer filters the information and human operator decides. • Only suspicious persons or behaviour are recorded and reported to the human operator. Human operator can only view unusual or noteworthy events. • Less potential privacy issues. • Suitable if false negatives will not lead to serious problems.

Appendix B

Evolution of CCTV Video Surveillance Technology

Adapted from "CCTV Futures Report – For Australian Customs and Border Protection", 2009, National ICT Australia (NICTA).

CCTV Generations	**Main Features**
1st Generation	• Analogue components • Slow video search • VHS cassette tapes for storage • Lower quality video images • Lack of interoperability between CCTV systems.
2nd and 3rd Generation	• Combination of analogue and digital components, particularly storage. • Faster video search and better quality video images. • Internet Protocol (IP) system allows for remote storage. • Also allows for secure and convenient multi-user remote viewing and access.
4th Generation (Today & Future)	• Fully digital systems • CCTV cameras connect directly to network. • Systems can incorporate video analytics to alert operators to suspicious activities and behaviours, and persons on watch-lists.

Appendix C

Smart CCTV Applications for Real-Time Situational Awareness

Adapted from "A National Approach to CCTV – National Code of Practice for CCTV Systems for Mass Passenger Transport for Counter-Terrorism, March 2012", Transport and Infrastructure Council, Council of Australian Governments.

Application	Features & Issues
Facial Recognition	• Requires high resolution and extensive database capability. • Current face-in-a-crowd technology has low reliability. • Requires significant Research & Development (R&D) and testing in real environment.
Gait Analysis	• Differences in walking style used to biometrically identify individuals.
Loitering	• Detects the extended presence of an individual in one place. • Affected by proximity to the camera, lighting and crowd conditions. • Requires site-specific evaluation.
"Man Down"	• Detects when someone has fallen over. • Affected by proximity to the camera, lighting and crowd conditions. • Requires site-specific evaluation.
Directional Flow	• Detects contra-directional traffic flow. • Affected by proximity to the camera, lighting and crowd conditions. • Requires site-specific evaluation.
Vehicle Number Plate Recognition	• Reads vehicle number plates and highlights targets of interest. • Requires specific camera position and target illumination. • Established and proven technology.

Application	Features & Issues
Unattended Item Recognition	• Current technology requires extensive configuration for individual environments, and can have high false-alarm rate. • Requires further R&D to reduce false-alarm rate and improve analysis of video motion and events.

Appendix D

Smart CCTV Applications for Post-Event Forensic Analysis

Adapted from "A National Approach to CCTV – National Code of Practice for CCTV Systems for Mass Passenger Transport for Counter-Terrorism, March 2012", Transport and Infrastructure Council, Council of Australian Governments.

Application	Features & Issues
Automated Person Identification	• Currently requires significant human effort to search. • Requires significant R&D to efficiently and accurately search archived footage with low false-alarm rate.
Automated Event Search	• Needs to be tailored to specific application or event. • Possible high false-alarm rate. • Can be applied to face, pattern or movement matching. • Requires significant R&D for full reliability.
Automatic Event Reconstruction	• Collection, analysis and meaningful combination of CCTV (and other) imagery from disparate systems (e.g. shops, supermarkets, chemists, liquor stores) to form a 'combined' view of an event from imagery originally recorded for other purposes. • Disclosure and privacy regulations need to be considered. • Requires significant R&D for full reliability (problems include different formats, quality etc.).
Video Parameter Enhancement	• Manipulation of various image components and temporal or spatial processing to enhance an existing photograph or video segment. • Requires significant R&D for full reliability (limited by quality of original information—requires high frame rate).

Appendix E

Summary of Smart CCTV-related Privacy Concerns

Key Points	Ameliorating Factors
1. Privacy concerns with respect to surveillance technology are not new as it has been discussed since the 1970s.[102] The discussions often scrutinise whether the reliability and accuracy (rate of false positives and negatives) of CCTVs could justify the perceived loss of privacy.[103]	• Privacy concerns should not be allowed to demonise the adoption of Smart CCTVs given its pivotal role in law enforcement, to ensure safety and security. • Advances in Smart CCTV technology such as the use of AI would enhance the accuracy of CCTVs. With AI, the process of surveillance would be "smart" rather than "mass". • Privacy would be better preserved as the footage is processed by AI instead of human operators. Human operators would be alerted only if: (i) anomalous behaviour or objects are detected; and (ii) persons with criminal records are detected through facial recognition. Hence, only the privacy of persons with criminal records or those behaving suspiciously would be affected.[104]

[102] Wright. D, "Sorting out smart surveillance", 2010, Computer Law and Security Review, p. 11

[103] Stuart Kaplan, "Is Ubiquitous Video Surveillance Of Public Spaces Good Public Policy", 16 September 2013, American Civil Liberties Union of Oregon (ACLU), http://www.aclu-or.org/is-video-surveillance-public-spaces-good-public-policy

[104] Koch H, Matzner T and Krumm, "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", 2013, European Journal of Law and Technology, Vol. 4, No. 2, pp 1 – 3

Key Points	Ameliorating Factors
2. Privacy norms may differ across societies especially in modern cities where elements of electronic surveillance (e.g. social media, mobile apps, biometrics and wearables) are embedded in homes, workplaces, public services (e.g. transport), and retail settings to enhance efficiency and convenience.	• As modern life becomes more digitised, it is not possible to live without revealing personal information to the state and corporations, as highlighted by Pew Research Centre in the “Future of Privacy” report. Hence, people may become more amenable to sharing and collection of data as a normal aspect of life, and adjust their privacy norms.[105] • People may be more amenable to CCTVs if there are safeguards to ensure responsible use of CCTVs and to prevent abuse.[106] For example, legislation such as the Data Protection Act in the United Kingdom and the Personal Data Protection Act in Singapore help to regulate the responsible use of CCTVs.[107] In the U.S., privacy guidelines regulate the responsible use of the New York Police Department’s Domain Awareness System.[108] • A healthy community partnership such as in Singapore can help people understand that both community vigilance and Smart CCTVs are concomitant and essential aspects of enhanced law enforcement strategies.[109] This point can also be drawn from a study commissioned in 2011 by the Danish Security and Intelligence Service which noted that attitudes towards visible security measures (e.g. CCTVs) are generally positive if there is a healthy level of communal trust and trust in the government.[110]

[105] “Digital Life in 2025: The Future of Privacy”, December 2014, Pew Research Centre, pp. 11 – 20, http://www.pewinternet.org/files/2014/12/PI_FutureofPrivacy_1218 141.pdf

[106] Yvonne Lim and Nadia Samdin, “People, not tech, key to foiling terror attacks: Former head of US Homeland Security”, 13 April 2016, Channel News Asia, http://www.channelnewsasia.com/news/world/people-not-tech-key-to/2691284.html

[107] “Guide to Data Protection”, UK Information Commissioner’s Office (ICO), https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

[108] http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

[109] Toh Ee Ming, “Public security more important than privacy”, 19 March 2016, Today Online, http://www.todayonline.com/singapore/public-security-more-important-privacy

[110] Nielson, Laisen and Wandorf, “Visible Counterterrorism Measures in Urban Spaces – Fear Inducing or Not?” 19 August 2014, Terrorism and Political Violence, 28:692–712, 2016

Key Points	Ameliorating Factors
3. Privacy concerns may arise from the linking of police Smart CCTVs with privately-owned CCTVs as such initiatives would extend the surveillance gaze of law enforcement agencies beyond public spaces and into privately-owned (or semi-public) spaces.[111]	• Policies can address these concerns by: (i) limiting access only to privately-owned CCTV cameras that are placed outdoors and along public thoroughfares where people expect minimal or zero privacy; (ii) eschewing audio surveillance; and (iii) maintaining a tight access control of the CCTV monitoring centre. These policies, for example, underpin the initiative in Grand Rapids, Michigan, U.S. which enables law enforcement agencies to access privately-owned CCTVs in real-time.[112] • Policies that regulate the responsible use of CCTVs in public spaces should be reviewed for its possible impact on the rights and responsibilities of both owners and operators of private CCTVs who collaborate with law enforcement. For example, Western Australia's State CCTV strategy stipulates that existing legislation which regulates the use of surveillance devices will be reviewed given the involvement of the privately-owned CCTVs. Reviews should include public consultations in order to maintain trust by meaningfully engaging all stakeholders for their views. • Cybersecurity efforts should involve owners and operators of private CCTVs as their CCTVs may present another attack (e.g. data theft) vector that can threaten police Smart CCTVs. Measures to incentivise these owners/operators to adopt better cybersecurity standards for their CCTVs may include: (i) incorporating cybersecurity of CCTV solutions into private security agencies' grading systems; (ii) factoring in baseline cybersecurity standards for CCTVs in the design stage as one of

[111] "Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations", 2009, Office of the Privacy Commissioner, New Zealand, p. 4, http://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf

[112] Garret Ellison, "Police getting real-time access to private security cameras in downtown Grand Rapids", 29 June 2014, Michigan Live, http://www.mlive.com/news/grand-rapids/index.ssf/2014/06/police_getting_real-time_acces.html

Key Points	Ameliorating Factors
	the construction standards for strategically important building projects; and (iii) cost-sharing arrangements. On cost-sharing, law enforcement agencies can harness public support by depicting such arrangements as stretching the taxpayers' dollars while delivering essential public services.[113]

[113] Pamela Qiu, "Can Public-Private Partnerships Deliver Better Public Services?" 13 March 2013, Ethos Perspectives, Issue 4, 2010, https://www.cscollege.gov.sg/Knowledge/Pages/Can-Public-Private-Partnerships-Deliver-Better-Public-Services.aspx

About the Author

Muhammad Faizal Bin Abdul Rahman is a Research Fellow with the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). He holds a Bachelor of Business Administration (with Merit) from the National University of Singapore. Prior to joining RSIS, Faizal served with the Singapore Ministry of Home Affairs where he was a Deputy Director and had facilitated international engagements with foreign security counterparts. He also had postings in the Singapore Police Force where he supervised and performed intelligence analysis, achieving several commendation awards including the Minister for Home Affairs National Day Award (2009) for operational and analysis efficiency; and in the National Security Research Centre (NSRC) at the National Security Coordination Secretariat (NSCS), where he led a team to research emergent trends in domestic security and monitor terrorism-related developments. Faizal also has certifications in Counter-Terrorism, Crime Prevention and Business Continuity Planning.

About the Centre of Excellence for National Security

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides fulltime analysts, CENS further boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg

NOTES

NOTES

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg