Palace, M, Frankel, R, Shortland, N, Jiang, W, May, B, Jones, A and Starkey, J

CCTV operators' perspectives on protecting soft target terrorist locations in England

CCTV operators' perspectives on protecting soft target terrorist locations in England

Abstract

Despite the significant importance of surveillance in counterterrorism, the CCTV operators' perspectives appear to be under-researched. To explore such perspectives, we conducted a number of semi-structured interviews with British security professionals tasked with CCTV monitoring of public spaces, and subjected their responses to the thematic analysis. Four themes emerged: *challenges to the use of CCTV systems*, *criticism of operator roles in counterterrorism*, *need for improvements*, and *the value of CCTV in counterterrorism*. While offering a critical view of current CCTV use in soft target (i.e., vulnerable) locations, these findings also highlight the value of CCTV in terms of deterrence, and support the Actor Actor-Network Theory (Terzi, 2019). As national security is increasingly looking to even more advanced technology for solutions (e.g., artificial intelligence), this exploratory research highlights the need for closer integration of human and technological actors, operator empowerment and continuous training that must be informed by actual CCTV operators who present themselves as marginalised.

Keywords: CCTV, counterterrorism, security, soft targets

CCTV operators' perspectives on protecting soft target terrorist locations in England

The cost and effectiveness of CCTV as a counterterrorism tool has been growing more controversial and questionable since 7/7 London bombings as even keeping two of the attackers under surveillance was not enough to stop them (Batty, 2006). It appears that targeted use of CCTV may also result in ethno-cultural tensions and backlash (Lewis, 2010), and that it plays a more significant role in the post-event analysis rather in actual prevention, which can be illustrated by the Westminster London Bridge attack (Dodd, 2017). Since the role of CCTV operators in such shortcomings has not been explored, the current paper will aim to shed light on their perspectives.

It is difficult not to find CCTV research on almost any public space (Ceccato & Paz, 2017; Cozens & Grieve, 2014; Liedka et al., 2019; Mucchielli, 2011; Nte, 2020). While there is similar research on counterterrorism (e.g., Coaffee, 2019; Eijkman & Weggemans, 2013; Iqbal & Arun, 2018; Robbins, 2021, the perspectives of counter-terror CCTV operators remain underexplored (Stedmon et al., 2012), which the current paper aims to (at least) partially address.

Such under-exploration seems unwarranted given the vulnerability of (easily attackable) soft-target locations (Hesterman, 2018; Jones et al., 2021; Schmid et al., 2021) that are defined as public-frequented, non-military, and easily attackable due to their limited security measures (Basu, 2021; Beňová et al., 2019; Schmid et al., 2021; Zeman, 2020).

Because of the open nature of soft target environments, CCTV is often relied upon as an effective security tool to both track down the perpetrator(s), understand what happened (Gallova et al., 2017; Roško et al., 2019), and detect potential future security threats (e.g., Robbins, 2022). As the UK is already one of the most CCTV-monitored countries in the world, which raises concerns about civil liberties being undermined by Orwellian invigilation (Starkey, 2022), it also shows some promising results. For instance, CCTV was used in the

identification (but not stopping) of terrorist Salman Abedi in the weeks leading up to and including the night of the Manchester Arena bombing (McCleery & Edwards, 2019).

Currently, the British ACT training does not encourage learners to ask questions or provide sufficient examples of suspicious behaviours and/or terrorist indicators, resulting in recruits that are unprepared for counter-terrorism tasks (Phelps (2021). Importantly, the operators should be better able to identify CCTV blind spots (Chapple, 2021).

An unintended consequence of surveillance is that terrorists often move their attacks to other, softer (more vulnerable) targets (Asal et al., 2009; Gill & Corner, 2016; Palasinski & Bowman-Grieve, 2017). Besides, there is a paucity of theories that would provide an adequate theoretical framework. Relatedly, Brown (2006), for example, illustrates the lack of techno-social networks, where human and non-human participants can come together to create an effective security unit. Elsewhere, the Actor-Network Theory (Terzi, 2019), which puts a premium on considering all aspects of CCTV, traces the complex interplay between human and non-human participants.

Despite changes in guidelines making Action Counter Terrorism (ACT) training mandatory (Security Industry Authority, 2021b), the guidelines on continuous CCTV training for operators remain unclear. It would therefore be of interest to explore the sufficiency of initial training in preparing the operator for counter-terrorism duties once recruited. Phelps (2020), for example, suggests that what is currently provided in counterterrorism training is inadequate, and that the training must be improved to include more general knowledge of terrorist behaviours and methods. However, his research was not specifically focused on UK counterterrorism, and thus cannot directly inform the British security context. Based on the above, the following research questions have been formed:

1. How are challenges to CCTV use constructed by CCTV operators?
2. How are criticisms of CCTV operator roles constructed?

3. How are improvements to CCTV use in soft (i.e., apparently vulnerable) target locations constructed?
4. How is the value of CCTV use constructed?

Method

Participants

From the initial pool of seventeen male operators tasked with CCTV monitoring of public spaces, thirteen were interviewed by an experienced male researcher. These all voiced concerns about being potentially identified and/or compromising their sensitive modus operandi. None of the thirteen agreed to be voice-recorded, and ten of the thirteen provided only very general answers that seemed evasive and lacked detail and elaboration. The remaining unrecorded three, however, did provided more detail, which then helped shape the direction of our final analysis). The remaining four of the seventeen operators were interviewed by a less experienced female researcher with a three-year training, and these all agreed to be voice-recorded and to share their full views without mentioning any reservations or potentially compromising their operational procedures, and thus it is the sample of four that is the focus of our analysis. This, in turn, raises the question of interviewer's gender as our operators were much more revealing and less reserved when the interviewer was a young female researcher. The question of what the responses would have been if the operators had been female is open.

While a larger sample would be always more preferable, what constitutes a sufficient sample in qualitative research is relative and depends on the extent to which the sample produces new insights (Vasileiou et al., 2018). The informational load of our recoded data produces hitherto unpublished and novel security insights with serious implications for public safety in England that may also inform other related research in the security field. Thus, we lend weight to the argument that the informational load may indeed compensate a relatively

small sample (Malterud et al., 2016). However, we stress that this is essentially an exploratory study.

To protect our male operators' anonymity and facilitate their free talk without anxiety about the potential repercussions from their managers, we agreed to share only some of their characteristics. Participant 1 (P1) was White British, trained as a Consultant Psychologist and specialised in developing and providing Behavioural Detection Training to security forces for 14 years. Participant 2 (P2) was British Indian, having worked with CCTV companies for over 15 years, and specialised in identifying system vulnerabilities. Participant 3 (P3) was White British with over 14 years working as a CCTV Operator and Security Consultant. Lastly, Participant 4 (P3) was White British with 26 years' experience involving counter-terrorism and security.

Semi-Structured Interviews

Following the first author's institution ethics clearance, the data were gathered through semi-structured interviews online, which were recorded and transcribed using the Otter software[1]. The interview primarily consisted of open-ended questions structured around our main research questions aimed at gleaning fresh insights into protecting public spaces in England (e.g., *How are suspicions followed?*); however, questions to elicit contextual information and participants characteristics *(e.g., What is your job role?)* consisted of closed-ended questions. The interviews ranged from 63 to 92 minutes (M=80.10 SD=12.25*).* The completion of each interview was immediately followed by emailing the CCTV operators a debrief sheet with a summary of the research and the researcher's contact information.

Data Analysis

[1] A transcription software that uses artificial intelligence to transcribe conversion in real-time (Corrente & Bougheult, 2022)

All transcriptions were thematically analysed, following Braun and Clarke's (2006) framework. This analytical method was chosen as it has previously been beneficial to identify recurrent patterns of meaning in related security research (e.g., Palasinski, 2009; Njoku, 2021; Wilson, 2014). The analytical process consisted of the following steps: (i) familiarisation of the participant responses; (ii) systematic analysis of the participants responses by coding (i.e., categorising into systematic groups) phrases and discussion points; (iii) an initial reduction of initial codes to create emergent sub-themes; (iv) a review of all sub-themes to generate high-level themes; (v) defining and reviewing all high-level of sub-themes; and (vi) developing an interpretive analytical commentary, so that the themes form a story.

To elaborate further, before each interview was analysed, the transcribed data was segmented into manageable numbered units determined by change of subject. The units were then probed for themes that were gradually reduced to a smaller number of increasingly more succinct and conceptually inclusive themes that were checked back and compared between and within interviews. They were also continually referred back to the original transcript. To identify reliability levels of the discerned 4 themes, two of the co-authors (raters) used the themes to number-code 40 items selected from the interviews. The 40 representative items comprised 20% of the total number of units (N=240) in all interviews. The two co-authors were in agreement on the coding of 73% of the items (i.e., they concurred that most of the items were given the same label), which was determined by item allocation to the same thematic category.

Results

The analysis revealed four overarching themes: (i) the challenges to the use of CCTV systems; (ii) *UK government and police neglect of CCTV as a counterterrorism tool; (iii)* constructed need for improvements to CCTV in soft target locations; and (iv) the value of

CCTV in counterterrorism. Each of the themes are discussed below, with exemplar quotes provided that best demonstrate each emergent theme.

Theme 1: The Challenges to the Use of CCTV Systems

Reliability raters were in 71% agreement this theme. Each operator was largely critical of CCTV systems in use at soft target locations, due to alleged poor procurement and installation practices. Furthermore, they expressed frustration at the alleged neglect of CCTV by the UK government and police, in their regulation and use of CCTV in security and counterterrorism. For example, vulnerabilities of current CCTV systems were put down to poor procurement by management, and installation by engineers:

"One of the things that, that fails time and time again, in many, many organisations, is that they don't understand the technology that they're bringing in. So they buy substandard equipment. They install it using substandard installers or integrators or whatever it's the cheapest ones that get in often" (P2, A2, p. 70).

Whilst this raises the issue of having technologically advanced CCTV at soft targets, it highlights the financial limitations and apparent lack of awareness on the part of the buyer or manager. It may be that those managing security procurement lack an awareness toward effective security posture. For example:

"it's understanding, what is it that we're protecting ourselves from? What is the cost and is it proportionate?" (P2, A2, p. 72).

The need for CCTV systems, brought into a soft target location to reflect relative threats and awareness of those threats, should perhaps, therefore, extend from management to the individual(s) installing the cameras. For instance, managing vulnerabilities is an integral part of installation and responsibility for adequate briefing is delegated to the management:

"I mean the whole thing about the design…the person who put the physical security cameras in at the beginning, they would be looking for those weak spots wouldn't they. So it's up to

them, when we were talking about management…they should have worked out…what you're covering and then work with a manufacturer that would provide them with a full design. So…it does depend a bit on the manager to some extent" (P3, A3, p. 103).

In addition, it was highlighted that those concerned with security systems were often ignored in their advice to government and police regarding the threats facing the surveillance systems. The prominent criticism was that CCTV was only used by authorities in the aftermath of an event:

"The thing that struck me that the police thought about…is the police are only interested primarily in, when it goes bang, in outlook…so their view of CCTV honed over the last 40 years of police use of CCTV in England, is to use CCTV after the event to support the investigation" (P4, A4, p. 112).

This demonstrates that security professionals are unimpressed at the basic level of CCTV value and lack of threat awareness. It was argued that this often occurred because *"the police, [are] not CT focused…[they] don't get it"* (P1, A4, p. 47). Perhaps, a lack of government legislation that instructs CCTV systems, software and operation may help explain this phenomenon:

"They produced two documents, one for manufacturers and one for integrators of systems, which are recommended best practice for people that use CCTV in buildings, and they include the cybersecurity of systems that I've mentioned, and what you should be doing. So that is sort of seen as best practice, it's not law…its becoming…a telecommunications law" (P3, A3, p. 89).

This suggests that the current publications are simply guidance, and not law. As such, the risk posed by a lack of regulation can have serious security implications:

"About five years ago we had the biggest CCTV botnet ever in the world, where…someone managed to hack in 200,000 cameras around the world, and then used it as a botnet, to

attack the internet infrastructure. And they managed to bring down the DNS servers…" (P2, A2, p. 79).

Theme 2: Criticism of CCTV Operator Roles in Counter-Terrorism

Reliability raters were in 74% agreement this theme. Poor training and recruitment, and poor operation of CCTV systems were identified as factors that can result in severe consequences for the safety of a location and hinder operators' performance. For example, the interviewees presented critical views of current CCTV operators' suitability to their roles, and of the information about counter-terrorism threats at their work locations:

"Manchester arena is a good example of…you know, if it's not a properly swept up team and…all functioning properly, then they potentially bugger off for a kebab" (P1, A1, p. 38).

This communicates the importance of dedication in the role of CCTV operator, and the dangers of allegedly neglecting one's responsibilities, as evidenced by the Manchester Echo Arena bombing. Expanding on this, communicating potential threats was presented as more than simply identification and incident management:

"That's incident response…that person should be reporting that and then there's a whole series of other processes that need to be exercised. The police come along grab the image on the CCTV interview. Try to recognise and build up a description. What car did they arrive in in the car park and this kind of thing never gets practice" (P4, A4, p. 119).

As such, it is suggested that CCTV operators should communicate actionable and detailed intelligence, and apply abstract, dynamic, and skilful security operations beyond just operating a camera:

"you need more than just the camera operator skills. You need skills from a variety of different expertise…the operators need to get good at using the technology as a tool, because that's all it is. It's nothing more than that" (P2, A2, p. 68-74).

One potential explanation for this, can be linked to ACT training, as illustrated by the following:

"the basic SIA training clearly isn't going to cover properly, things like terrorism" (P1, A1, p. 43).

"there were no feedback loops in the ACT training. From what I understand…the training is…one dimensional. There's no opportunity to ask questions" (P4, A4,cp. 118).

The lack of participation and learning occurring with those undertaking ACT, were presented as yielding insufficiencies in knowledge toward counterterrorism duties and principles commonly associated to terrorist indicators and reiteration of procedure following suspicion:

"Identifying suspicious behaviour. What is suspicious behaviour? Well, if this person is…taking a picture of your building, what are you going to do? So you're going to go up to them and say, excuse me, what's your strategy now? What's the company policies?" (P3, A3, p. 94).

Theme 3: Need for Improvements to CCTV in Soft Target Locations

Reliability raters were in 73 % agreement this theme. The operators addressed concerns toward the development of Converged Security Operation Centre's (CSOC). More specifically, participants highlighted a need to improve counterterrorism, at *"large built environments…shopping centres…sports stadiums"* (P3, A3, p. 86) among others. These centres were explained as a single location in which:

"You can gather a whole picture…so they have the CCTV system in access control, but you also have all the information from social media about what they're planning. And if you're quick enough, with all the data that's flying around, you have…alerts about it…a risk alert" (P3, A3, pp. 86-87).

This briefly presents the functioning of CSOC's as a place in which everything regarding the security of a location can be examined. It was also presented as a valuable counterterrorism tool to enable CCTV operators to track and gain information on the activity of suspects:

"If you really want to look at counterterrorism, it should be a bit like what you see in the movies where you've got massive screens, and you've got somebody following somebody else, through different screens through cameras, and somebody's checking out the Facebook account, somebody's checking out whatever" (P2, A2, p. 66).

The use of these CSOC's would improve security through bringing together the technology, and all security personnel of different expertise, who can work collaboratively to identify, neutralise and/or report threats. This was presented as an opportunity to learn and develop new skills:

"They're able to share that knowledge with the rest of the team and they're able to learn from the other team as to…what you need and what it is that they're looking for in terms of counterterrorism" (P2, A2, p. 67).

In turn, those more aware of counterterrorism risks and threats were constructed as highly-valued assets that could assist CCTV operators.

"If there was going to be an attack on Saturday at this time, it will be here, you know, security industry and the people that manage the security industry…don't have that concept well ingrained in them that you need to prepare for something to that extent" (P4, A4, p. 114).

Incorporating behavioural detection training for CCTV operators was also presented as a key skill that can assist in identifying suspects:

"increases the detection rate of actual positive detections by a factor of about 10" (P1,A1, p. 40). As such, ACT training should include: (i) when and where to look at the camera's, (i) be relative to the location, and (iii) involve behavioural detection training.

Theme 4: The Value of CCTV in Counter-Terrorism

Reliability raters were in 74% agreement this theme. Based on this theme, it turns out that CCTV has three primary benefits: (i) deterring attackers through the presence of cameras; (ii) the use of footage for evidence in investigations; and (iii) the use of software to assist in identifying terrorist activity. Importantly, despite such benefits the operators did not mention their potential downsides, such as raising the risk of community backlash through racial profiling.

As such CCTV as a counterterrorism tool provides insight and information to law enforcement regarding *what* took place before, during and after a terrorist attack. For example:

"CCTV, basically, at the end of the day is evidential. So, Boston bomber, you know" (P1, A1, p. 58).

The Boston marathon bombing demonstrates this value of CCTV in its role in identifying and charging the two attackers. Evidentiary use was also expressed as being equally as important as live surveillance:

"Going back in time and tracking them is just as big part of the operators' analytics…as it is looking at the current analytics. So, all of that is building up complete picture. It's not just one part of the story or one individual or one technology. It's several coming together to build the jigsaw" (P2, A2, p. 77).

As a measure of deterrent value, approaching those identified on CCTV and expressing to them that CCTV is an active security capability, can result in heightened

awareness of their activity being monitored, deterring them from future offending in that location:

"If it's the bad guy, the underlying message that you sent is there's someone in CCTV they spotted you that's why I've come over…So next time they turn up, that camera suddenly becomes a threat, not just a bit of furniture…because now you're thinking is that you know, are they watching it again, they were watching before so there's a little bit of kind of theatre there that you can start to use CCTV to create that deter" (P1, A1, p. 59).

CCTV as a tool, therefore, can be creatively used to deter terrorists and recognises the human as a supporting actor in carrying out this deterrence:

"it stands to prevent crime…That's the point of it. And to respond or to be used to follow up, trying to assist people in a positive way" (P3, A3, p. 93).

The advancement of CCTV software also allows for several counter-terrorism tasks to be carried out in the background, suggesting that there is less reliance on CCTV operators to continuously monitor soft targets for potential threats. For example, built-in artificial intelligence that monitors camera footage and provides a priority report to the operator can focus attention on urgent tasks, and prioritise security and counterterrorism measures:

"Basically, what it does is all the data that's on CCTV systems, all the images and all the other stuff that we've talked about, it will analyse it, and give you, prioritise the data for you. So that you can see what's important" (P3, A3, p. 105)

This is a common feature within more recently developed software, which offers operators a strategic and tactical advantage over potential adversaries. For example, Video Motion Detection (VMD) has the value of alerting operators to programmed behaviours of interest:

"VMD, its blank screen technology. You design it to detect what you're looking for. You tell the system design people that I want you to look for this here…then what you do is, say

somebody's moving left or right across the screen. Then you have video analytics that would only alert if somebody moves left to right across the screen.…" (P4, A4, p. 120).

Discussion

The purpose of the current research was to (at least to some degree) address a critical gap in knowledge about the perspectives of British security professionals tasked with CCTV monitoring of public spaces for terror threats. To this end, we ran a number of interviews and subjected them to thematic analysis, producing four main themes and original insights into practical implications for enhancing the security of public spaces.

Overall, the findings are in line with previous research and the Actor- Network Theory (Terzi, 2019) supporting and expanding upon the existing literature. Aligning with and building on the past research suggesting that the use of CCTV in counterterrorism lies primarily in deterrence opportunities (Dalton et al. (2017), the current research expands on the consideration that the overt presence of CCTV might potentially deter terrorism. It suggests that for this potential to be realised, however, the operators' perspectives and scepticism need to be taken into account much more seriously than they currently are. Their perspectives also imply a greater need for more focus on interoperability (i.e., their smoother communication with other security operatives) in their training. It appears that to optimise the role of CCTV in countering terrorism, the operators must be given more decision-making power and their concerns need to be integrated into the continuous professional training.

While it has been long apparent that technology-enabled behavioural detection capabilities are limited (Jupe & Keatley, 2020; Milbredt et al., 2022), our findings suggest that they might be enhanced by better software, investment, training and empowerment of operators. The highlighted need for extensive security training in general rather than in simply operating the CCTV technology is line with the Actor-Network Theory (Terzi, 2019), tying in with the idea that the technology and human operator can act jointly as a combined

system. Our findings also tie in with the argument that CCTV operators can increase their preparedness by participating in emergency response exercises.

Although our findings are ecological valid, one should be careful about extending them to other countries and contexts that entail different laws, operational procedures and other types of training. Although the relatively small sample does not represent a saturated understanding of CCTV as a counterterrorism tool (see, Hennink & Kaiser, 2022), this stage one research can now meaningfully inform the construction of other questions aimed at a larger group of CCTV operators (e.g., *how can the operators be more empowered? How can their perspectives inform the continuous training?*). In order to offer the public greater protection, it is imperative that more voices from the 'CCTV trenches' are explored and considered in countering terrorist and common criminal threats.

References

Asal, V. H., Rethemeyer, R. K., Anderson, I., Stein, A., Rizzo, J., & Rozea, M. (2009). The softest of targets: A study on terrorist target selection. *Journal of Applied Security Research*, *4*(3), 258-278. https://doi.org/10.1080/19361610902929990.

Basu, N. (2021). Learning lessons from countering terrorism: the UK experience 2017–2020. *Cambridge Journal of Evidence-Based Policing*, *5*(3), 134-145.

Batty, D. (2006). Two 7/7 bombers were under surveillance**.** *The Guardian,* 11th May. Available at: https://www.theguardian.com/uk/2006/may/11/july7.uksecurity

Beňová, P., Hošková-Mayerová, Š., & Navrátil, J. (2019). Terrorist attacks on selected soft targets. *Journal of Security & Sustainability Issues*, *8*(3).

Braun, & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223-244.

Ceccato, V., & Paz, Y. (2017). Crime in São Paulo's metro system: Sexual crimes against women. *Crime Prevention and Community Safety*, *19*(3), 211-226.

Chapple, M. (2021). Modelling adversary behaviour in crowded spaces. *The Crisis Response Journal, 16*(2), 71-76.

Coaffee, J. (2019). Terrorism, risk and the quest for Urban resilience. In *Handbook of Urban Geography* (pp. 225-240). Edward Elgar Publishing.

Corrente, M., & Bourgeault, I. (2022). Innovation in Transcribing Data: Meet Otter. ai.

Cozens, P., & Grieve, S. (2014). Situational crime prevention at nightclub entrances in Perth, Western Australia: Exploring micro-level crime precipitators. *Crime prevention and community safety*, *16*(1), 54-70.

Dalton, B., Martin, K., McAndrew, C., Nikolopoulou, M., & Triggs, T. (2017). Designing Visible Counter-Terrorism Interventions in Public Spaces. In *Hostile Intent and Counter-Terrorism* (pp. 261-276). CRC Press.

Dodd, V. (2017). London Bridge attack: CCTV shows fatal clash with police. *The Guardian,* 7th June. Available at: https://www.theguardian.com/uk-news/2017/jun/07/london-bridge-attack-cctv-shows-fatal-clash-between-police-and-terrorists.

Gallova, V., Palasinski, M., Shortland, N., Humman, M., & Grieve, L. B. (2018). Anxiety about digital security and terrorism, and support for counter-terror measures. *Safer Communities 17*(3),156-166.

Gill, P., & Corner, E. (2016). Lone-Actor Terrorist Target Choice. *Behavioral Sciences & the Law*, *34*(5), 693–705.

Hennink, M. M., & Kaiser, B. N. (2020). *Saturation in qualitative research*. Thousand Oaks, CA: Sage Publications Limited.

Hesterman, J. (2018). *Soft target hardening: protecting people from attack*. Routledge.

Iqbal, J. M., & Arun, S. (2018). Intelligent information system for suspicious human activity detection in day and night. *Int. J. Informatics Commun. Technol*, *7*(33), 117-123.

Jones, S. G., Doxsee, C., Hwang, G., & Thompson, J. (2021). *The military, police, and the rise of terrorism in the United States*. Center for Strategic & International Studies.

Jupe, L. M., & Keatley, D. A. (2020). Airport artificial intelligence can detect deception: or am i lying? *Security Journal*, *33*(4), 622-635.

Lewis, P. (2010). Birmingham stops camera surveillance in Muslim areas. *The Guardian*, 17th June. Available at: https://www.theguardian.com/uk/2010/jun/17/birmingham-stops-spy-cameras-project**.**

Liedka, R. V., Meehan, A. J., & Lauer, T. W. (2019). CCTV and campus crime: Challenging a technological “fix”. *Criminal justice policy review*, *30*(2), 316-338.

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: guided by information power. *Qualitative health research*, *26*(13), 1753-1760.

McCleery, M., & Edwards, A. (2019). A micro-sociological analysis of homegrown violent extremist attacks in the UK in 2017. *Dynamics of Asymmetric Conflict*, *12*(1), 4-19.

Milbredt, O., Popa, A., Doenitz, F. C., & Hellmann, M. (2022). Aviation security automation: The current level of security automation and its impact. *Journal of Airport Management*, *16*(2), 184-208.

Mucchielli, L. (2011). CCTV: The French controversy. *Crime Prevention and Community Safety*, *13*(4), 294-298.

Njoku, E. T. (2021). Queering terrorism. *Studies in Conflict & Terrorism*, 1-23.

National Counter Terrorism Security Office. (2020). *Guidance: CCTV*. https://www.gov.uk/government/publications/crowded-places-guidance/cctv.

Nte, N. D., Gande, G., & Uzorka, M. (2020). The Challenges and Prospects of ICTs in Crime Prevention and Management in Nigeria: A Review of CCTV Cameras in Abuja. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 75-100.

Palasinski, M. (2009). Testing Assumptions about Naivety in Insurance Fraud. *Psychology, Crime & Law, 15*(6), 547-553.

Palasinski, M., & Bowman-Grieve, L. (2017). Tackling Cyber-Terrorism: Balancing Surveillance with Counter Communication. *Security Journal, 30*(2), 556-568.

Phelps, M. (2021). The role of the private sector in counter-terrorism: a scoping review of the literature on emergency responses to terrorism. *Security Journal, 34*, 599–620.

Robbins, S. (2021). Facial Recognition for Counter-Terrorism: Neither a Ban Nor a Free-for-All. In *Counter-Terrorism, Ethics and Technology* (pp. 89-104). Springer, Cham.

Robbins, S. (2022). Machine Learning, Mass Surveillance, and National Security: Data, Efficacy, and Meaningful Human Control. In *The Palgrave Handbook of National Security* (pp. 371-388). Palgrave Macmillan, Cham.

Roško, M., Musladin, M., & Kazanský, R. (2019). Counter-Terrorism in the United Kingdom: Sustainable Measure or Violation of Human Rights. *Journal of Security & Sustainability Issues*, *9*(2), 603-616. http://doi.org/10.9770/jssi.2019.9.2(19)

Schmid, A. P., Forest, J. J., & Lowe, T. (2021). Counter-Terrorism Studies: A Glimpse at the Current State of Research (2020/2021). *Perspectives on Terrorism*, *15*(4), 155-183.

Security Industry Authority. (2021a, October 1). *Get Licensed*. GOV.UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1021162/sia-get-licensed.pdf.

Security Industry Authority. (2021b, November 25). *FOI release: SIA licence holders called upon to help combat terrorism*. GOV.UK. https://www.gov.uk/government/publications/sia licence-holders-called-upon-to-help-combat-terrorism/sia-licence-holders-called-upon-tohelp-combat-terrorism.

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, *37*(1), 167-175.

Stedmon, A. W., Lawson, G., Saikayasit, R., White, C., & Howard, C. (2012). Human factors in counter-terrorism. In *Advances in Social and Organizational Factors* (pp. 237-246). CRC press.

Starkey, J. (2022). The role of social categorization in predicting support for controversial digital and physical counter-terror measures. *Unpublished Doctoral Thesis.* Liverpool John Moores University.

Terzi, M. (2019). E-government and cyber terrorism: conceptual framework, theoretical discussions and possible solutions. *Tesam Akademi Dergisi*, *6*(1), 213-247.

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC medical research methodology*, *18*(1), 1-18.

Wilson II, S. F. (2014). *Terrorist Experts' Perceptions of how the Internet has Shaped International Terrorism* (Doctoral dissertation, Walden University). https://www.proquest.com/dissertationstheses/terrorist-experts-perceptions-how-internet-has/docview/1648432400/se-2?accountid=12118.

Zeman, T. (2020). Soft targets: Definition and identification 1. *Academic and Applied Research in Military and Public Management Science, 19*(1), 109-119.