Safety Science 189 (2025) 106888

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Anticipating public acceptance of anti-terrorism technologies in urban spaces: Insights from Czech Republic, Greece, and Spain

Arturo Cuesta [*], Javier González-Villa, Gemma Ortiz, Daniel Alvear

University of Cantabria, Los Castros s/n 39005, Santander, Spain

ARTICLE INFO

Keywords:
Public acceptance
Security technologies
Terrorism
Urban spaces

ABSTRACT

This study surveyed citizens (n = 1.501) from the Czech Republic, Greece, and Spain to analyse public acceptance of new technologies for preventing terror attacks in urban areas. Our results reveal that threat perception and privacy concerns impact on pre-existing attitudes toward surveillance technologies. We found that 25 % of participants trusted the proposed technologies while 50 % saw them as effective but invasive. Results also reveal sociodemographic factors that significantly shape acceptance including age, gender, education, political views, and geographical location. Furthermore, the proposed model, which links acceptance to knowledge, perceived effectiveness, intrusiveness, and trust in institutions, was found reliable and valid.

1. Introduction

Protecting the public from terrorism has become a top priority in Western countries (Pavone et al., 2016). While technology alone cannot ensure security, it plays a central role in this effort (Schmitt et al., 2004). Consequently, governments, companies, and researchers have been actively working to develop and implement new surveillance security technologies (Beck, 2002) leading to an important change in counter-terrorism strategies, moving from merely reacting to threats to proactive prevention (Verhelst et al., 2020; Jonas & Harper, 2006). However, this approach involves monitoring and labelling citizens thus raising concerns and fears of authoritarian overreach, which may result in public resistance (Pavone et al., 2015). Surveillance technologies, in particular, blur the line between security and civil liberties which are often framed as mutually exclusive and uncontextualized abstract categories. This issue has gained importance with the increasing use of artificial intelligence in various aspects of life. As these technologies become more prevalent, understanding public acceptance is essential for evaluating their feasibility and impact in a comprehensive manner. Citizen consultation for assessing new security technologies is becoming essential in the context of research and innovation, especially in Europe (Wynne, 2006; Felt and Wynne, 2007). It also may help policymakers to better understand issues, desires, and needs regarding security technologies leading to more informed decision-making and transparent governance (Demuijnck & Fasterling, 2016).

In line with this approach, this study investigated public perceptions of near-future security technologies designed to prevent terrorist attacks in urban public spaces. The study was conducted as part of the Societal Impact Assessment (SIA) (Hempel et al., 2013) within the S4AllCities project (https://www.s4allcities.eu/project) and surveyed citizens from the countries involved in the project—Czech Republic, Greece, and Spain. We first analysed public attitudes toward terrorist threats, surveillance, and data protection. Then, we analysed public acceptance of a system designed during the project to prevent, detect, and monitor terrorist threats in public spaces. The system includes two key technologies: smart video analytics and mobile phone location tracking.

2. Literature review

A large and growing body of literature has investigated public perceptions of terrorism, exploring opinions (Sinclair & LoCicero, 2006), fears (West & Orr, 2005), and concerns about this issue (Haner et al., 2019). Researchers have also examined public attitudes toward anti-terrorist measures (Rykkja et al., 2014), the impact of terrorist attacks on policy preferences (Economou & Kollias, 2019), post-terror attack reactions (Jakobsson & Blom, 2014), and views on counterterrorism authorities (Christensen & Aars, 2019).

Building on this, another strand of research has focused on public acceptance of new security technologies, which is shaped by several factors (Degli Esposti et al., 2017). Institutional trustworthiness has been positively associated with the acceptance of security technologies (Ball et al., 2018; Pavone & Degli Esposti, 2012) while lower trust

[*] Corresponding author.
E-mail address: cuestaar@unican.es (A. Cuesta).

https://doi.org/10.1016/j.ssci.2025.106888
Received 10 December 2024; Received in revised form 22 March 2025; Accepted 28 April 2025
Available online 7 May 2025

correlates with a reduced inclination to compromise privacy for security (Davis & Silver, 2004). Privacy concerns also can play a significant role. A study found that air travellers prefer uniform screening over risk-based screening due to privacy issues (Veisten et al., 2011). Similarly, another study showed that concerns about privacy can lead to distrust in technologies like RFID tags and smart cards, highlighting the importance of strong privacy policies (Strickland & Hunt, 2005). Another study found that people perceive Deep Packet Inspection (DPI) as intrusive and therefore less accepted, unless they believe it is effective at stopping terrorism (Degli Esposti et al., 2017). The trade-off between privacy and security is another area of research. People were found to sacrifice certain rights under relevant security threats (Dragu, 2011; Davis & Silver, 2004), yet a lack of understanding and trust on authorities can undermine this willingness (Strickland & Hunt, 2005). Conversely, a study suggests that public acceptance of surveillance technologies changes following terrorist attacks, leading to an increase in transparency demands and a decrease of privacy concerns (Wester & Giesecke, 2019). Some researchers argue that the perceived trade-off between security and privacy is an oversimplification (Solove, 2007; Solove, 2011; Friedewald et al., 2015), with many citizens desiring both protection and privacy simultaneously (Van den Broek et al., 2017).

Researchers have also shown how demographic factors can shape attitudes toward security technologies. For instance, a study suggested that higher-income and more educated individuals generally show less acceptance of AI-driven surveillance (Park & Jones-Jang, 2023) whereas another study found that young females tend to trust more video surveillance while older and educated individuals are more concerned about crimes in public spaces (Ardabili et al., 2024). Regional differences were found significant as well, with Western and Nordic countries showing lower acceptance of surveillance technologies compared to post-Communist countries, where phone tapping and video surveillance are more accepted than internet monitoring and personal data collection (Školník & Haman, 2024). Finally, another important issue for the public acceptance of emergent technologies is related to the potential effects of framing in opinion formation. A study suggested that the way surveillance technologies are presented can affect their acceptability, but this effect is mediated by pre-existing beliefs and attitudes of individuals (De Pauw & Vermeersch, 2017).

While previous studies have examined public perceptions and acceptance of surveillance technologies, challenges remain in developing models that account for the interplay between subjective perceptions and sociodemographic variables. This study contributes to the existing literature by quantitatively analysing how these factors interact in shaping public acceptance of new technologies designed to prevent terrorism in urban spaces. To address this, we pose the following research questions:

> *Q1: How do terrorism threat perception and general privacy concerns impact the acceptance of surveillance-oriented security technologies?*
> *Q2: How do perceived effectiveness and intrusiveness of these technologies affect public acceptance?*
> *Q3: What is the influence of sociodemographic factors on the acceptance of these technologies?*
> *Q4: How do knowledge, trust, intrusiveness, and effectiveness collectively influence public acceptance, and what are their interrelationships?*

3. Method

3.1. Design

The survey items were based on the SurPRISE project (Pavone et al., 2015) and adapted for this study. The questionnaire consisted of three main sections. The first section examined general attitudes toward the terrorist threat, privacy concerns, and acceptance of surveillance-oriented security technologies, without framing to capture pre-existing attitudes (Table 1). After this section, participants were presented

Table 1
Constructs and items included in this study.

Constructs		**Item. — Statement**
General Attitudes	*T.*- Threat perception	*T0.- I'm concerned about the threat of a terrorist attack* *T4.- Because of terrorism, I am alert when I am in crowded places* *T5.- I am worried about being caught up in a terrorist attack*
	P.- Privacy concerns	*P1.- I am concerned that too much information is collected about me* *P3.- I am concerned that my personal information may be shared without my permission* *P4.- I am concerned that my personal information may be used against me*
	A.- Technology acceptance	*A0.- Overall, I believe surveillance-orientated security technologies should be routinely implemented to improve national security* *A1.- The use of surveillance-orientated security technologies improves national security* *A3.- If surveillance-orientated security technology is available authorities might as well make use of it*
Attitudes towards the system and its technologies	*K.*- Knowledge	*K0.- I understand why these technologies are used* *K1.- I understand what the system is* *K2. — I understand what mobile phone location tracking is* *K3.- I understand what smart video is*
	E.- Effectiveness	*E1.- I believe that these technologies can improve urban security* *E2.- In my opinion these technologies are effective security tools* *E3.- I would feel more secure when these technologies are in operation* *E4.- These technologies are appropriate to address terrorist threats*
	Tr.- Trust	*Tr1.- Security agencies which use this kind of technologies are trustworthy* *Tr2.- Security agencies which use this kind of technologies are competent at what they do* *Tr3.- Security agencies which use this kind of technologies are concerned about welfare of citizens as well as the national security* *Tr4.- Security agencies which use this kind of technologies do not abuse their power* *Trt5.- Laws and regulations ensure that this kind of technologies are not misused*
	I.-Intrusiveness	*I1.- I believe that the system is intrusive* *I2.- The idea of surveillance technologies in the system (smart video and mobile location tracking) makes me feel uncomfortable* *I3.- I feel that surveillance technologies of the system (smart video and mobile location tracking) are forced upon me without my permission* *I4.- The surveillance technologies of the system worry me because it could violate my fundamental rights* *I5.- The system worries me because it could violate everyone's fundamental rights*
	Ac.- Acceptance	*Ac0.- Overall, I support the adoption of these technologies to improve terrorist security*

(continued on next page)

Table 1 (*continued*)

Constructs		Item. – Statement
		Ac1.- Overall, I support the adoption of this system as a security measure in my city/town *Ac2.- Overall, I support the adoption of mobile phone location tracking as a security measure in my city/town* *Ac3.- Overall, I support the adoption of smart video as a security measure in my city/town*
	SP-B.- Security-privacy balance*	*Chose the statement you agree most* *SP-B1.-The system is…* *SP-B2.-The Smart video is…* *SP-B3.-The Phone location tracking is…* *…Useful and not very intrusive/ Useful but highly intrusive/Useless and highly intrusive/ Neither useful nor intrusive/Don't know/don't want to answer*

with a scenario: Imagine that a System to monitor and early detect terrorist attacks is implemented in your city/town, described briefly with text and images (Fig. 1). Participants received descriptions of two key technologies in the system: (1) Smart video, referring to video analytics (digital cameras linked to recognize individuals, analyze behavior, and detect objects), and (2) Mobile phone location tracking (analyzing location data to collect information about the user's location and movements). These technologies were selected for their potential trade-off between privacy/liberty and increased security (Strickland and Hunt, 2005). The second section focused on the following factors that may affect public perception and acceptance of the described system and technologies (Table 1):

- Knowledge (K).- The clarity of how a technology operates and the purposes for which it is operated, may affect acceptability (Jasanoff, 2004). This factor indicates to what extent participants have understood how the presented technology works and why it is used.
- Effectiveness (E).- Those technologies perceived as more effective are likely to have a higher degree of acceptability among citizens (Sanquist et al., 2008). This factor indicates whether the presented technology is perceived as effective in fighting terrorism.
- Trust (Tr).- Previous research showed that trust in public authorities is an influencing factor of technology acceptance (Knights et al., 2001; Lodge, 2007, Pavone & Degli Esposti, 2012; Bali, 2009; Ball et al., 2018).This factor reflects confidence in the trustworthiness, competence, ethical behaviour, and regulatory oversight of agents that use the technology.
- Intrusiveness (I).- This factor is expected to negatively influence acceptability (Sanquist et al., 2008). It is defined as the extent to which technology is perceived to intrude into an individual's personal sphere (e.g. leading a person to feel uncomfortable and/or to think about civil liberty infringement).
- Acceptance (Ac).- This factor measures the extent to which the presented technologies are considered as desirable, satisfactory and/or tolerable security measures by the public.
- Security-privacy balance (SP-B).- This represents the trade-off approach citizens may use to assess the introduction of new security technologies. This usually happens when technology is both privacy infringing and security enhancing (Strickland and Hunt, 2005).

The third section of the questionnaire gathered sociodemographic factors (Table 2), including age, gender, education, and income, which offer insights into the broader context that shapes respondents' views on security technologies and, consequently, their acceptance of these technologies (Park & Jones-Jang, 2023; Ardabili et al., 2024). The section also included questions about country/city and place of residence to account for geographical variations in perspectives influenced by local political, cultural, and security contexts (Školník & Haman, 2024). Political orientation and ethnic minority status were considered as factors that affect attitudes toward surveillance, particularly regarding trust and fairness in security measures (Ball et al., 2018; Pavone & Degli Esposti, 2012). Finally, behavioral factors, such as frequency of public space usage and personal experiences with terrorism, were included to assess how exposure to different environments and events may shape individuals' opinions on surveillance technologies.

3.2. *Development*

The English version of the questionnaire was translated into Czech, Greek and Spanish by native speakers. They were requested to pay special attention to achieve semantic, idiomatic, experiential, and conceptual equivalence to the original version. The translation was made by two independent translators per language to detect and resolve subtle differences/discrepancies. Also, the resulting versions were back-translated to ensure the accuracy of the translation. Check-box answers were provided in the questionnaire to reduce the time to answer. Most items were rated by a 5-point Likert scale, i.e. simply-worded statements to which respondents indicated their agreement or disagreement ranging from "strongly disagree" to "strongly agree". The exception were items for Security-privacy balance (SP-B) measured through a nominal scale of four options: useful and highly intrusive; useful and not very intrusive; useless and highly intrusive; useless and not very intrusive, based on (Pavone and Degli Esposti, 2012). Sociodemographic information was gathered at the final section of the questionnaire. A pilot study was conducted involving 41 students from the Czech Republic two weeks after they participated in a drill of a terrorist attack at the Pilsen football stadium, as part of the technology demonstrations of the S4AllCIties project. This pilot survey enabled us to assess whether the designed questionnaire met the objectives of the study.

Imagine that a **System** to monitor and early detect terrorist attacks is implemented in your city/town. The system uses advance technology for smart detection of weapons, explosives, suspicious behaviours and cyber-attacks and provides crucial information to protect citizens.

The system uses:

- **Mobile phone location tracking**: By analysing location data from a mobile phone, information can be collected about the location and movements of the phone user over a period of time.
- **Smart** video: Features digital cameras, which are linked together in a system that have the potential to recognise individuals, analyse their behaviour and detect objects.

3.3. *Survey administration*

The electronic questionnaires were tested for usability and functionality before fielding the final version. The target population included residents of urban areas in Greece (Trikala, Athens), the Czech Republic (Prague, Pilsen), and Spain (Bilbao, Vitoria). A survey company sent email invitations to participants in these locations ensuring quality control during data collection. The questionnaire consisted of 40 items plus sociodemographic questions and took approx. 20–25 min to complete. Responses were automatically captured and sent to researchers in an Excel spreadsheet for analysis.

3.4. *Data analysis*

Analyses were conducted using JASP statistical program v0.15 and R version 2022.07.2. Multiple logistic regression was conducted to assess the significant independent sociodemographic predictors of technology acceptance with 95 % confidence intervals (95 % CI).

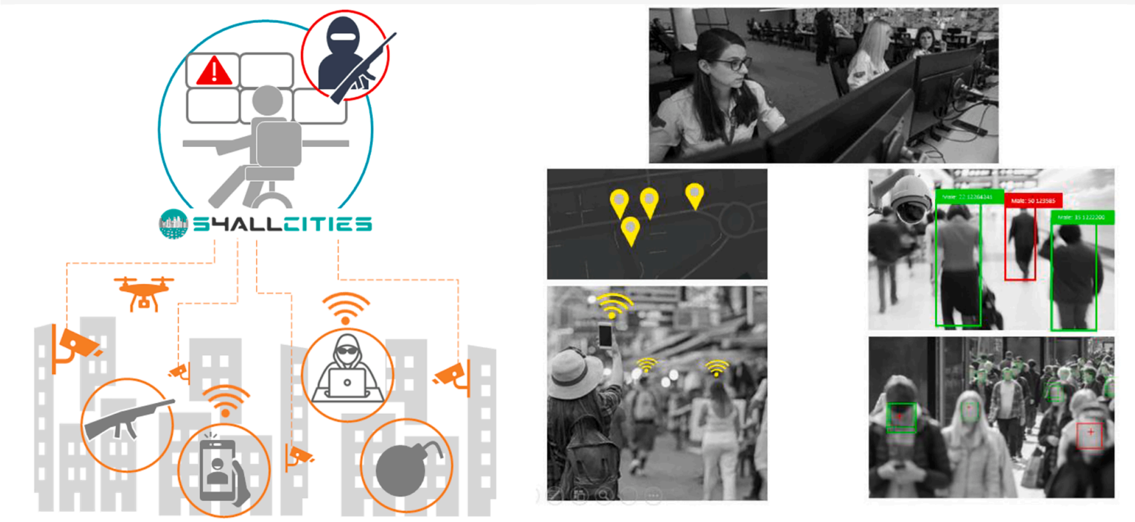


Fig. 1. Text and graphical description of the security system and the technologies in the questionnaire

Table 2
Baseline characteristics of the surveyed participants.

Variable/category	n (%)	Variable/category	n (%)
Age (years)		Country/City	
18–24	115 (7.7)	Spain/Bilbao	338 (22.5)
25–34	239 (15.9)	Spain/Vitoria	162 (10.8)
35–44	413 (27.5)	Czech Republic/Pilsen	245 (16.3)
45–54	410 (27.3)	Czech Republic/Prague	256 (17.1)
55–65	225 (15.0)	Greece/Trikala	22 (1.5)
> 65	99 (6.6)	Greece/Athens	478 (31.8)
Gender		Income (€/month)	
Male	740 (49.3)	<1.500	504 (33.6)
Female	749 (49.9)	1.500–2.500	527 (35.1)
Non-binary	7 (0.5)	2.600–3.000	218 (14.5)
Other	5 (0.3)	>3.000	252 (16.8)
Education level		Place of residence	
Primary	47 (3.1)	In the city center	423 (28.2)
Secondary	657 (43.8)	Close to city center (< 2 Km)	553 (36.8)
University	797 (53.1)	Far from city center (≥ 2 Km)	525 (35.0)
Political orientation		Frequency in public spaces	
Centre	406 (27.0)	< 2 times a week	232 (15.5)
Right	270 (18.0)	2–3 times a week	457 (30.4)
Left	353 (23.5)	4–5 times a week	391 (26.0)
None	472 (31.4)	6–7 times a week	421 (28.0)
Belong to a minority ethnic group		Involved in a terrorist attack before	
Yes	89 (5.9)	Yes	132 (8.8)
No	1412 (94.1)	No	1369 (91.2)
Current situation		Children under 16 years at home	
Student	65 (4.3)	Yes	525 (35.0)
Unemployed	91 (6.1)	No	976 (65.0)
Employee	981 (65.4)		
Self-employee	166 (11.1)		
Stay at home parent/ career	54 (3.6)		
Retired	144 (9.6)		

Survey responses were transformed for analysis by grouping some sociodemographic variables into broader categories and recoding them into categorical or binary formats to simplify the logistic regression model. For example, the “Political orientation” variable was recoded into a binary variable: “Ideology” (Centre, Right, and Left) and “No Ideology” (None). This transformation helps focus on the distinction between individuals with and without a clear political ideology, simplifying the analysis of how ideological affiliation influences attitudes toward surveillance and security measures. Confirmatory Factor Analysis (CFA) and Structural Equation Modelling (SEM) were conducted to check the relationship and consistence between the observed variables and their underlaying latent constructs. Reliability was measured as well using Cronbach’s alpha. All statistical analyses were done using two-tailed tests. For all analyses performed in our study, p-values ≤ 0.05 were considered statistically significant.

3.5. Ethics

The questionnaire was anonymous, with privacy policy details provided to participants (e.g. study purpose, survey duration, data protection, etc.). Written consent was not required, but participation implied consent to participate via the agreement section of the questionnaire. Ethics approval of this study was granted by the Ethical Committee of the University of Cantabria, Spain.

3.6. Participants

To determine our required sample size, we conducted a power analysis with a 95 % confidence level, a 5 % margin of error, an assumed population portion of 50 %, and a power rate 0.95 (Aberson, 2019). The analysis indicated we needed at least 385 responses to achieve the desired confidence level per country. A total of 1.501 participants completed the questionnaire (Table 2). They were urban residents from Spain ($n = 500$), Czech Republic ($n = 501$) and Greece ($n = 500$). The age of respondents ranged from 18 to 83 years (*Mean* ± *SD*; 44.18 ± 13.15). The questionnaire collected balanced responses from men (49.3 %) and women (49.9 %) with 0.8 % of respondents who did not identify themselves as man or woman. The education level of the sample population was high with most participants having secondary studies or higher. 5.9 % of respondents belong to a minority ethnic group. Interestingly, 8.8 % of respondents reported having been involved, to some extent, in a terrorist attack.

4. Results

4.1. General attitudes

Q1: How do terrorism threat perception and general privacy concerns impact the acceptance of surveillance-oriented security technologies? Around one fifth of participants felt in danger because of terrorism (Figs. 2–4). Most respondents were concerned about the collection (58.6 %), sharing (71.4 %) and use (59.2 %) of their personal information and around half of respondents were in favour of surveillance-orientated security technologies to foster security i.e. 47.1 % reported that technologies should be implemented, 59.1 % though that technologies improve national security and 49.3 % indicated that authorities can use such technology, if available. The key questions investigated were whether perceived threat (T) and privacy concerns (P) influence overall acceptance (A) of surveillance-oriented security technologies, and to what extent these factors have an impact on people attitudes. Consequently, two hypotheses were formulated: H1, that threat perception positively influences citizens' acceptance of security technologies, and H2, that privacy concerns negatively influence citizens' acceptance of such technologies. To address these hypotheses, we first conducted a Confirmatory Factor Analysis (CFA) to check the relationship and consistence between the observed variables (T0, T4 and T5; P1, P4 and P5; A0, A1, A3) and their underlaying latent constructs (T, P and A). Reliability was measured as well using Cronbach's alpha. The results of the CFA indicate that each item loaded on its respective underlying concept and all loadings were significant (Table 4). The following model fit indices suggest that the measurement model fits to the data: Chi square/df = 4.12; Tucker Lewis Index (TLI) = 0.99; Comparative Fix Index (CFI) = 0.99; Root Mean Square Error Approximation (RMSEA) = 0.05; Standardized Root Mean Square Residual (SRMR) = 0.02. The Cronbach alpha values were higher than 0.80 indicating a good internal consistency between the items (Table 3). Then, we developed a Structural Equation Model (SEM) to examine the linear causal relationships among the latent variables and testing the proposed hypotheses. As Table 4 shows, the standardized path coefficients (β) are significant indicating that both hypotheses are supported by the model. Hence terrorist threat perception (T) and privacy concerns (P) among citizens are significant factors for and against the acceptance (A) of surveillance-oriented security technologies.

4.2. Attitudes towards the proposed system and its technologies

Q2: How do perceived effectiveness and intrusiveness of these technologies affect public acceptance? over half of the participants had a favourable attitude towards security technologies, with 50.4 % supporting the system overall. Mobile phone location tracking had the lowest support (42.1 %) and the highest proportion of non-supporters (28.4 %). Interestingly, nearly one-third of respondents lacked a clear opinion (see Fig. 5). The security-privacy balance emerged as a key factor: About 25 % trusted the technologies, viewing them as useful with no privacy risk, while 50 % saw them as effective but privacy-invasive, considering a trade-off necessary. A smaller segment (12–14 %) found the technologies both ineffective and invasive, and less than 5 % saw them as useless but minimally intrusive (see Table 5).

Q3: What is the influence of sociodemographic factors on the acceptance of these technologies? We conducted a logistic regression analysis to assess the significant independent sociodemographic predictors of acceptability with 95 % confidence intervals (95 % CI). The variables *Ac0*, *Ac1*, *Ac2* and *Ac3* (Table 1) were considered as dependent variables with the responses recoded as “1″ if the participant accepts the technology (“agree” and “strongly agree) and “zero” otherwise (“neutral”, “disagree” and “strongly disagree”) thus allowing a clear distinction between acceptance and non-acceptance. Furthermore these variables reflect participants' support ranging from general support (Ac0: “*I support the adoption of these technologies to improve terrorist security*”) to more specific technologies (Ac1: “*I support the adoption of this system as a security measure in my city/town*,” Ac2: “*I support the adoption of mobile phone location tracking as a security measure in my city/town*,” and Ac3: “*I support the adoption of smart video as a security measure in my city/town*”). We conducted Hosmer–Lemeshow goodness of fit test to check that the four constructed models fit the data: Technology (p = 0.13); System (p = 0.90), Phone tracking (p = 0.42) and Smart video (p = 0.25). The reported odd ratios (OR) and the corresponding confidence intervals (95 %CI) in Table 6 allow the readers the possibility to identify significant independent predictors of technology acceptance (e.g. when acceptance is more or less likely to occur for individuals in one condition or another). For instance, the predictors for the acceptance of the System were being female (1.28 times more likely than being male), older than 50 years (1.45 times more likely than being < 30 years), having political ideas (1.47 more likely than those who do not) and being Greek (1.50 times more likely than Czech people).

Q4: How do knowledge, trust, intrusiveness, and effectiveness collectively influence public acceptance, and what are their interrelationships? We conducted Confirmatory Factor Analysis (CFA) to examine the relationship among: knowledge (*K*), intrusiveness (*I*), trust (*Tr*), acceptance (*Ac*), and effectiveness (*E*), regarding public attitudes towards the proposed security technology. The path diagram is shown in Fig. 6. The model was reasonably consistent with the data (TLI = 0.97; CFI = 0.97; RMSEA = 0.05; SRMR = 0.05). All factor loadings were higher than 0.70 meaning the items in the model reliably measure what they are supposed to. The convergent validity was assessed by the average variance extracted (AVE) and all values were higher than 0.50 indicating unidimensionality. Multicollinearity was addressed by removing one of two highly correlated variables (rho > 0.80) when identified. Discriminant validity was assessed by Fornell-Larcker criterion indicating that construct is distinct from others, confirming that different concepts are being measured separately. High Cronbach's alpha values were obtained (>0.85) denoting a good construct reliability. The path diagram (Fig. 6) shows how public acceptance (*Ac*) of anti-terrorism technologies is influenced by trust (*Tr*), effectiveness (*E*), knowledge (*K*), and perceived intrusiveness (*I*). Acceptance is positively associated with trust, effectiveness, and knowledge, meaning that people are more likely to accept the technology if they trust those using it, believe it is effective, and understand it better. However, perceived intrusiveness negatively affects acceptance, indicating that the more invasive a technology seems, the less likely people are to support it. The relationships between these factors are also interconnected—higher trust is linked to greater perceived effectiveness, and more intrusive technologies tend to reduce both trust and perceived effectiveness. While knowledge positively correlates with acceptance, it has little impact on perceived intrusiveness. This suggests that public perceptions of security technologies are

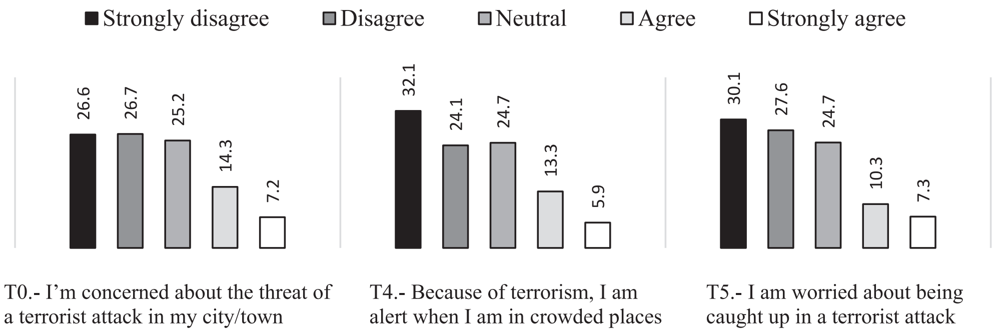


Fig. 2. Terrorist threat perceived by participants (%)

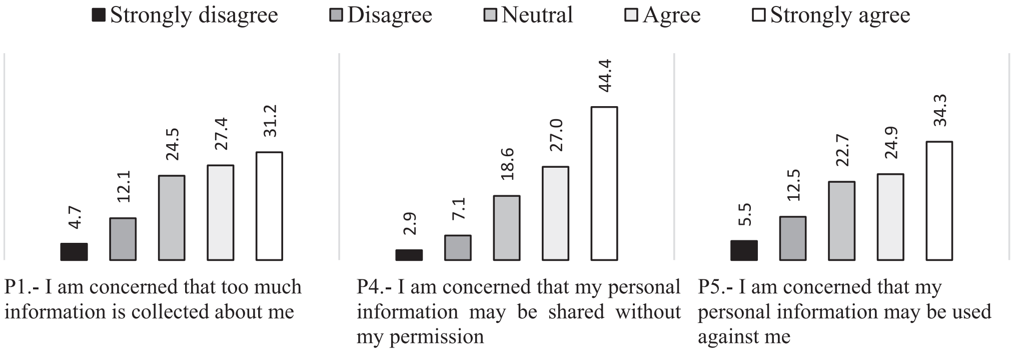


Fig. 3. Privacy concerns reported by participants (%).

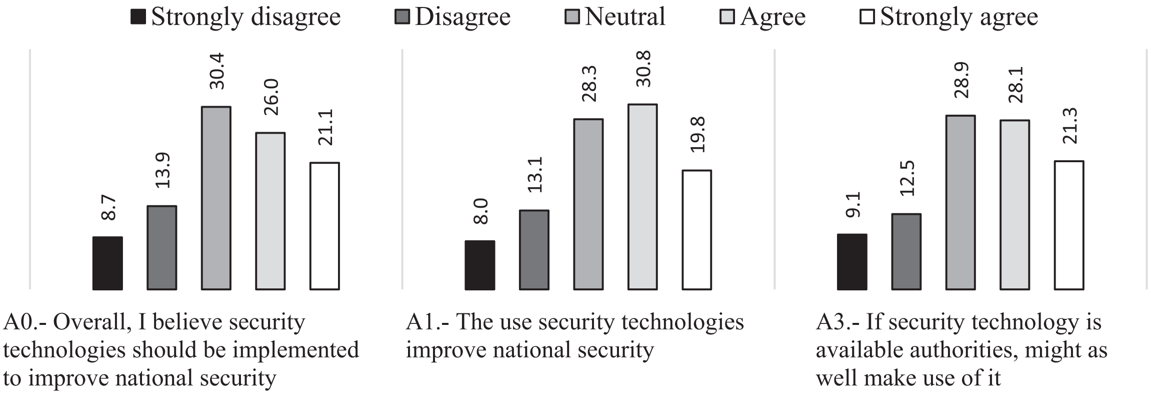


Fig. 4. General acceptance of security technologies (%).

Table 3
Confirmatory factor model fit and reliability.

Factor	Item	Factor loading	Cronbach's alpha
T.- Threat perception	T0	0.89	0.87
	T4	0.75	
	T5	0.86	
P.- Privacy concerns	P1	0.83	0.87
	P3	0.84	
	P4	0.82	
A.- Technology acceptance	A0	0.92	0.88
	A1	0.89	
	A3	0.73	

shaped not just by their functionality but also by broader concerns about privacy and institutional trust.

5. Discussion

This study aimed to explore the public acceptance of counter-terrorism security technologies, specifically focusing on a system designed to prevent terrorist attacks in urban areas within smart cities, along with two of its key components: phone tracking and smart video. The analysis was part of a Societal Impact Assessment (SIA) conducted in the S4AllCities project to ensure public accountability form the early stages of the development and innovation processes (Hempel et al., 2013). The online survey (40 items) included responses from representative urban residents (n = 1.501) in Spain, Greece, and the Czech Republic. Data collected were processed and analyzed to address the following research issues:

5.1. General attitudes

Q1: Role of threat perception and privacy concerns in technology Acceptance.- our findings show that in our sample both fear of terrorism and privacy concerns play an important role in general acceptance of surveillance technologies i.e. Before framing the proposed technologies. In our sample, 20 % of respondents reported feeling threatened by terrorism, and this perception was strongly associated with higher support for these technologies (β = 0.51). This aligns with previous research suggesting that fear can drive public support for security measures (Davis & Silver, 2004; van den Broek, 2020). At the same time, privacy concerns had a negative impact on acceptance (β = -0.25), with more than half of the respondents expressing concerns about how their personal data is collected and used. Similar findings have been reported in other studies (Thompson et al., 2020). However, the weaker effect of privacy concerns in comparison to fear suggests that many people may still support these technologies if they perceive the security benefits as outweighing the privacy risks (Strauß, 2019).

5.2. Attitudes towards the proposed system and its technologies

Q2: Impact of perceived effectiveness and intrusiveness on

Table 4
Hypothesis testing.

Hypothesis	Relationships	β	SE	z-values	p-values
H1	Threat perception → Technology acceptance	0.51	0.02	18.10	<0.001
H2	Privacy concerns → Technology acceptance	−0.25	0.03	−8.19	<0.001

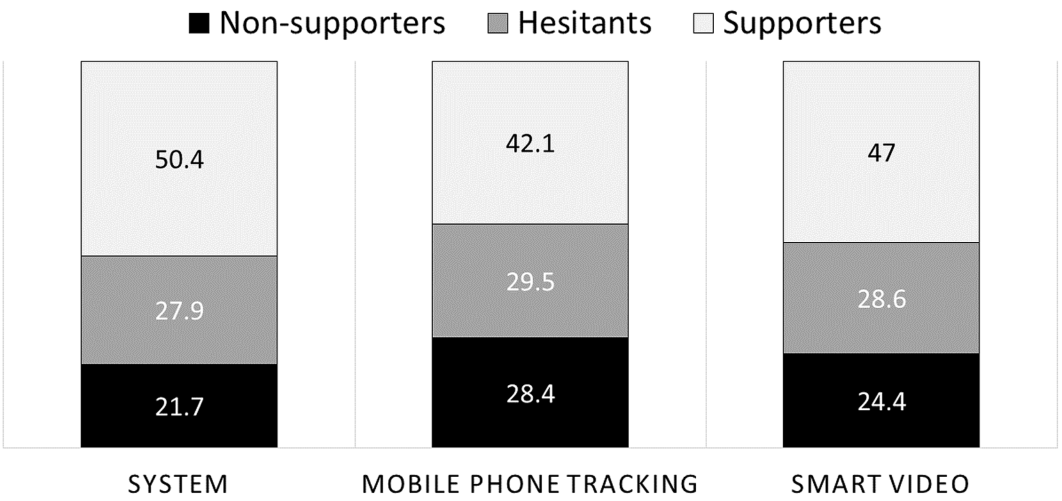
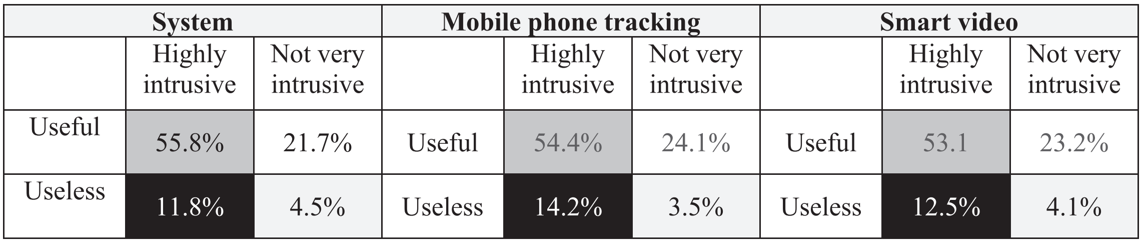


Fig. 5. Acceptance of security technologies (%). Refer to Table 1 for items i.e., System (Ac1), Mobile phone tracking (Ac2) and Smart video (Ac3). Non-supporters are those who responded either "strongly disagree" or "disagree". Hesitant are those who responded "neutral". Supporters are those who responded either "agree" or "strongly agree".

Table 5
Distribution of the perceived security-privacy balance of the proposed technologies.



System			Mobile phone tracking			Smart video		
	Highly intrusive	Not very intrusive		Highly intrusive	Not very intrusive		Highly intrusive	Not very intrusive
Useful	55.8%	21.7%	Useful	54.4%	24.1%	Useful	53.1	23.2%
Useless	11.8%	4.5%	Useless	14.2%	3.5%	Useless	12.5%	4.1%

technology Acceptance.-. The tension between appreciating security benefits and concerns over the potential misuse of surveillance technologies reflects broader debates on balancing public safety with personal privacy (Strauß, 2019). In our study, over half of respondents supported the implementation of the proposed system in their cities. However, our findings suggest that technologies perceived as more intrusive tend to receive lower levels of support, as seen in the case of smart video surveillance (47 %) and mobile phone tracking (42.1 %). When considering the security-privacy balance, approximately 50 % of respondents indicated a willingness to accept privacy risks if they believed the technology improved security. While this might suggest a trade-off between liberty and security, previous research has shown that public attitudes toward surveillance technologies are shaped by more than just this binary opposition (Solove, 2007; Solove, 2011; Friedewald et al., 2015). As Pavone and Degli Esposti (2012) argue, public acceptance of surveillance depends not only on perceptions of effectiveness and intrusiveness but also on trust in institutions, perceived legitimacy, and broader social and political contexts. Our findings align with this perspective, suggesting that the acceptance of security technologies is influenced by a complex interplay of factors beyond a simplistic trade-off model.

Q3: Influence of Sociodemographic Factors.- Sociodemographic factors such as gender, age, and political ideology also affect acceptance of surveillance technologies. In our sample women and older individuals were more likely to support the proposed technologies supporting previous findings which links these groups with higher safety concerns (Park & Jones-Jang, 2023; Ardabili et al., 2024). Furthermore, our results showed that individuals with certain political ideologies were more supportive of the proposed technologies and associated surveillance measures, likely reflecting their trust in political institutions and belief in the effectiveness of these solutions to enhance security (Pavone & Degli Esposti, 2012). Our results also showed differences in willingness to accept preventive anti-terrorism technologies among Greeks, Czechs, and Spanish participants. Country-specific background factors, such as political history and the nature of security threats may provide further explanation for these differences (Kalmus et al., 2024; Školník & Haman, 2024). Greece has faced significant security challenges, including domestic terrorism and regional instability, fostering greater acceptance of security measures. In contrast, the Czech Republic's limited exposure to terrorism may lead to skepticism or indifference, as the perceived necessity for such technologies is lower. Spain's experience with the Basque separatist group ETA, which declared a permanent ceasefire in 2006, adds complexity to public attitudes. It should be noted that Spanish participants were from the Basque Country, which has not experienced terrorism since then. On one hand, familiarity with the impact of terrorism might increase support for preventive measures. On the other hand, residents may oppose technologies that evoke memories of past authoritarian government actions. These factors highlight the importance of considering local perceptions and historical contexts when offering and implementing counterterrorist security technologies for public spaces.

Q4: Knowledge, Trust, Intrusiveness, and Effectiveness.- The path diagram model developed here provides a clear representation of the factors influencing people attitudes towards the proposed anti-terrorism technologies, with a particular focus on the relationships between perceived intrusiveness, effectiveness, trust and knowledge illustrating how these constructs interact to shape public acceptance (*Ac*). The model shows that acceptance is positively influenced by perceived

Table 6
Predictors of security technology acceptance. OR (Odd ratio); CI (Confidence Interval). Bold values are statistically significant *p < 0.05; **p < 0.01; ***p < 0.001.

Independent Variable	Technology OR (95 % CI)	System OR (95 % CI)	Phone tracking OR (95 % CI)	Smart video OR (95 % CI)
Gender				
Female	**1.33 (1.08–1.65)** **	**1.28 (1.04–1.58)** *	**1.44 (1.16–1.77)** ***	**1.37 (1.11–1.69)** **
Male (Ref.)	1	1	1	1
Age (years)				
> 50	1.20 (0.86–1.69)	**1.45 (1.04–2.03)** *	**1.62 (1.15–2.30)** **	**1.67 (1.19–2.35)** **
30–50	1.14 (0.83–1.58)	1.14 (0.83–1.57)	1.26 (0.91–1.76)	1.28 (0.93–1.77)
< 30 (Ref.)	1	1	1	1
Income (€/month)				
> 2.500	0.99 (0.78–1.26)	0.99 (0.78–1.25)	1.03 (0.81–1.31)	1.09 (0.86–1.38)
< 2.500 (Ref.)	1	1	1	1
Education				
University	1.05 (0.84–1.31)	0.84 (0.67–1.05)	0.83 (0.66–1.04)	**0.77 (0.61–0.96)** *
Secondary (Ref.)	1	1	1	1
Belong to a minority ethnic group				
Yes	1.12 (0.71–1.77)	1.18 (0.75–1.87)	1.51 (0.95–2.39)	1.21 (0.77–1.92)
No (Ref.)	1	1	1	1
Children under 16 years at home				
Yes	1.11 (0.87–1.41)	1.12 (0.88–1.42)	1.25 (0.98–1.59)	1.12 (0.88–1.42)
No (Ref.)	1	1	1	1
Involved in a terrorist attack before				
Yes	1.05 (0.72–1.53)	1.04 (0.71–1.52)	1.05 (0.71–1.54)	1.10 (0.75–1.61)
No (Ref.)	1	1	1	1
Political ideology				
Yes	1.19 (0.95–1.49)	**1.37 (1.09–1.72)** **	**1.47 (1.17–1.86)** ***	**1.48 (1.18–1.86)** ***
No (Ref.)	1	1	1	1
Country				
Greece	**1.87 (1.43–2.45)** ***	**1.43 (1.10–1.87)** **	**1.50 (1.15–1.97)** **	**1.35 (1.03–1.77)** *
Spain	**1.72 (1.31–2.28)** ***	1.04 (0.79–1.37)	1.17 (0.88–1.55)	1.19 (0.90–1.57)
Czech Rep. (Ref.)	1	1	1	1
Live in city center				
Yes	**0.77 (0.61–0.98)** *	0.90 (0.71–1.15)	0.90 (0.70–1.14)	1.00 (0.83–1.27)
No (Ref.)	1	1	1	1
Frequency in public spaces a week				
> 4 times	0.95 (0.77–1.18)	0.96 (0.78–1.94)	0.99 (0.79–1.22)	1.02 (0.83–1.27)
< 4 times (Ref.)	1	1	1	1

effectiveness (E), trust (Tr), and knowledge (K), while it is negatively impacted by perceived intrusiveness (I). Notably, the strong covariance between most of the latent variables suggests that these factors are not independent but rather interrelated in complex ways. For example, the positive relationship between trust and acceptance (*Ac*) confirms that trust in institutions and/or operators increases, so too does the likelihood of accepting the technology (Knights et al., 2001; Pavone & Degli Esposti, 2012). The strong covariance between effectiveness and acceptance further emphasizes the importance of demonstrating that the technology is valuable and useful in addressing security concerns (Sanquist et al. 200). The moderate covariance between knowledge (*K*) and acceptance suggests that a better understanding of the technology may promote greater acceptance (Jasanoff, 2004). However, this understanding might not directly influence its acceptability (Pavone et al., 2012). The negative covariance between intrusiveness (*I*) and acceptance (*Ac*) is particularly significant, as it indicates that greater perceived intrusiveness can be associated with lower acceptance, even when other factors like trust and effectiveness are considered. Furthermore, the proposed path diagram model is quite revealing in several ways. For instance, it shows a strong positive relationship between trust in institutions and effectiveness, suggesting that trust plays a crucial role in shaping how people evaluate the performance of counterterrorism technologies. Building trust—through transparency, accountability, and ethical implementation—emerges as essential to enhancing public confidence in their efficacy. Similarly, the negative covariance between trust and intrusiveness indicates an inverse relationship meaning that the more people feel their privacy is being invaded by the technology, the less they trust in authorities or those using it and vice versa. This could imply that perceived intrusiveness undermines confidence in the intentions or fairness of those implementing the technology. Another interesting relationship found was the association between intrusiveness and effectiveness suggesting that participants may not see privacy loss as a guarantee of better performance of counterterrorist technology (Pavone et al. 2015).

5.3. Limitations and future directions

The study has some strengths and weaknesses. Overall, this study adds to the body of knowledge insights into public acceptance of a novel security system to protect citizens against terrorism in urban public spaces which include surveillance technologies. However, the generalisability of these results is subject to certain limitations suggesting room for further research. First, population samples were drawn from a limited number of cities within each surveyed country. Future studies should include larger samples to allow for more comprehensive comparative analyses. Second, the study focused on specific technologies such as phone tracking and smart video surveillance. Future research could examine a wider collection of technologies, including those perceived as less intrusive, to better understand the variations in public acceptance of counterterrorism measures. Third, the study relied on self-reported attitudes based on a brief description of technology which may not fully advance the complexities and factors that shape public acceptance in real-world scenarios. Additionally, a deeper analysis of the influence of political beliefs, past experiences with terrorism, and socio-economic status which have not been analyzed in the present study could provide richer insights into the factors that shape public

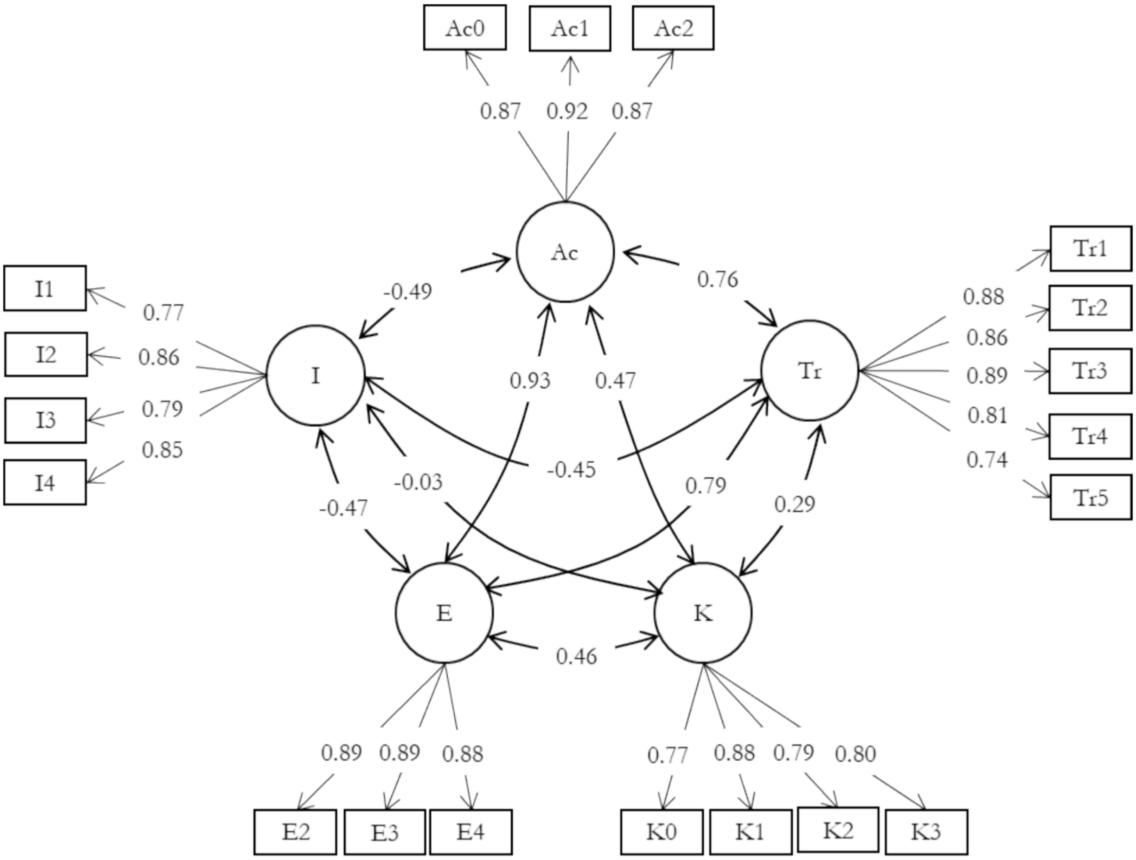


Fig. 6. CFA path diagram of factors related to the public acceptance of the security system. Ac = Acceptance; I = Intrusiveness; E = Effectiveness; K = Knowledge; Tr = Trust.

opinion on surveillance.

6. Conclusion

Public acceptance of preventive anti-terrorism technologies is shaped by a complex interplay of several factors, which policymakers and developers should address when designing and implementing this kind of solutions. Key determinants include transparency, which fosters understanding by providing clear information about the purpose of the technology and functionality; effectiveness, which ensures the technology is perceived as reliable and capable; and trustworthiness, which is built by deploying the technology through credible and ethical institutions. However, these factors alone may not be sufficient, as sociodemographic and contextual variables also influence public attitudes. Therefore, an integrated model that considers the interaction of these determinants, along with cross-cultural and societal insights, is essential. This model would help guide the design of adaptable counterterrorism technologies that align with diverse public expectations across different cultural and societal contexts.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used ChatGPT in order to improve the readability and language of the manuscript. After using this tool, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the published article

CRediT authorship contribution statement

Arturo Cuesta: Writing – original draft, Software, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Javier González-Villa:** Writing – review & editing, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Gemma Ortiz:** Writing – review & editing, Project administration, Funding acquisition. **Daniel Alvear:** Writing – review & editing, Supervision, Project administration, Investigation, Funding acquisition, Conceptualization.

Funding

This work is part of SALLCITIES project that was supported by the European Union's H2020 research and innovation programme under grant agreement No. 883522.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We wish to thank the SALLCITIES project partners for their support in translating the survey into Czech, Greek and Spanish and assisting with the pilot testing. Their contributions were instrumental in ensuring the study's accuracy, cultural relevance, and successful implementation across diverse contexts.

Author contributions

All authors were involved in the conceptualization and design of the study, AC wrote the original draft of the manuscript. GO and DA reviewed the manuscript. GO was involved in the project administration. DA supervised the project. AC and, JGV and DA were involved in the methodology, investigation and formal analysis. All authors revised and approved the final version of the manuscript.

References

Aberson, C.L. (2019). Applied power analysis for the behavioral sciences: 2nd Edition (2nd ed.). Routledge. https://doi.org/10.4324/9781315171500.

Ardabili, B.R., Pazho, A.D., Noghre, G.A., Katariya, V., Hull, G., Reid, S., Tabkhi, H., 2024. Exploring public's perception of safety and video surveillance technology: A survey approach. Technol. Soc. 78, 102641. https://doi.org/10.1016/j.techsoc.2024.102641.

Bali, V., 2009. Tinkering toward a national identification system: An experiment on policy attitudes. Policy Stud. J. 37 (2), 233–255.

Ball, K., Degli Esposti, S., Dibb, S., Pavone, V., Santiago-Gomez, E., 2018. Institutional trustworthiness and national security governance: Evidence from six European countries. Governance 32 (3), 437–453. https://doi.org/10.1111/gove.12353.

Beck, U., 2002. The terrorist threat: World risk society revisited. Theory Cult. Soc. 19 (4), 39–55. https://doi.org/10.1177/0263276402019004003.

Christensen, D.A., Aars, J., 2019. The July 22 terrorist attacks in Norway and citizens' attitudes toward counterterrorist authorities: Governance capacity and legitimacy. Societal Security and Crisis Management 323–341.

Davis, D.W., Silver, B.D., 2004. Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. Am. J. Polit. Sci. 48 (1), 28–46.

De Pauw, E., Vermeersch, H., 2017. The acceptance of surveillance oriented security technology : a framing experiment. In: Friedewald, M., Burgess, P., Cas, J., Peissl, W., Bellanova, R. (Eds.), Surveillance, Privacy and Security : Citizens' Perpectives. Routledge, London, pp. 52–70.

Degli Esposti, S., Pavone, V. and Santiago-Gomez, E. (2017) Aligning security and privacy: The case of Deep Packet Inspection. In Surveillance, Privacy and Security: Citizens' Perspectives, Michael Friedewald, J. Peter Burgess, Johann Čas, Rocco Bellanova, Walter Peissl (eds), 71- 90.

Demuijnck, G., Fasterling, B., 2016. The social license to operate. J. Bus. Ethics 136 (4), 675–685. https://doi.org/10.1007/s10551-015-2976-7.

Dragu, T., 2011. Is there a trade-off between security and liberty? Executive bias, privacy protections, and terrorism prevention. Am. Polit. Sci. Rev. 105 (01), 64–78. https://doi.org/10.1017/S0003055410000614.

Economou, A., Kollias, C., 2019. Security policy preferences of EU citizens: Do terrorist events affect them? Public Choice 178, 445–471.

Friedewald, M., Van Lieshout, M., Rung, S., Ooms, M., & Ypma, J. (2015). Privacy and security perceptions of European citizens: A test of the trade-off model. In J. Camenisch, S. Fischer-Hübner, & M. Hansen (Eds.), Privacy and Identity Management for the Future Internet in the Age of Globalisation: 9th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2, International Summer School, Patras, Greece, September 7–12, 2014 (pp. 39-53). Springer. https://doi.org/10.1007/978-3-319-18621-4_4.

Felt, U., & Wynne, B. (2007). Taking European knowledge society seriously. Luxembourg: DG for Research. EUR 22:700.

Haner, M., Sloan, M.M., Cullen, F.T., Kulig, T.C., Jonson, C.L., 2019. Public concern about terrorism: Fear, worry, and support for anti-Muslim policies. Socius Sociological Research for a Dynamic. WORLD 5 (2). https://doi.org/10.1177/2378023119856825.

Hempel, L., Ostermeier, L., Schaaf, T., Vedder, D., 2013. Towards a social impact assessment of security technologies: A bottom-up approach. Sci. Public Policy 40 (6), 740–754. https://doi.org/10.1093/scipol/sct086.

Jakobsson, N., Blom, S., 2014. Did the 2011 terror attacks in Norway change citizens' attitudes toward immigrants? International Journal of Public Opinion Research 26 (4), 475–486.

Jasanoff, S., 2004. States of knowledge: The co-production of science and the social order. Routledge, London.

Jonas, J., Harper, J., 2006. Effective counterterrorism and the limited role of predictive data mining. Policy Anal. 584, 1–12.

Kalmus, V., Bolin, G., Figueiras, R., 2024. Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. New Media Soc. 26 (9), 5291–5313. https://doi.org/10.1177/14614448221134493.

Knights, D., Noble, F., Vurdubakis, T., Willmott, H., 2001. Chasing shadows: Control, virtuality and the production of trust. Organ. Stud. 22 (2), 311–336.

Lodge, J., 2007. Biometrics: A challenge for privacy or public policy-certified identity and uncertainties. Minority, Politics, Society 1, 193–206.

Park, Y.J., Jones-Jang, S.M., 2023. Surveillance, security, and AI as technological acceptance. AI & Soc 38, 2667–2678. https://doi.org/10.1007/s00146-021-01331-9.

Pavone, V., Degli-Esposti, S., & Santiago, E. (2015). D 2.4 – Key factors affecting public acceptance and acceptability of SOSTs. SurPRISE Project (European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492).

Pavone, V., Degli Esposti, S., 2012. Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. Public Underst. Sci. 21 (July), 556–572.

Pavone, V., Santiago Gómez, E., Jaquet-Chifelle, D.-O., 2016. A systemic approach to security: Beyond the trade-off between security and liberty. Democr. Secur. 12, 225–246.

Rykkja, L.H., Laegreid, P., Fimreite, A.L., 2011. Attitudes towards anti-terror measures: The role of trust, political orientation and civil liberties support. Crit. Stud. Terror. 4 (2), 219–237.

Sanquist, T.F., Heidi, M., Morris, F., 2008. An exploratory risk perception study of attitudes toward homeland security systems. Risk Analysis: an International Journal 28 (4), 1125–1133.

Schmitt, B., et al. (2004). Research for a secure Europe. Luxembourg: Office for Official Publications of the European Communities.

Sinclair, S.J., LoCicero, A., 2006. Development and psychometric testing of the Perceptions of Terrorism Questionnaire Short-Form (PTQ-SF). New Sch. Psychol. Bull. 4 (1).

Školník, M., Haman, M., 2024. Drawing the line: Public attitudes towards warranted and unwarranted government surveillance in European countries. Secur. J. https://doi.org/10.1057/s41284-024-00426-4.

Solove, D. J. (2007). "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. San Diego Law Review, 44, 745-772. GWU Law School Public Law Research Paper No. 289.

Solove, D.J., 2011. Nothing to hide: The false tradeoff between privacy and security. Yale University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3976770.

Strauß, S. (2019). Privacy and identity in a networked society: Refining privacy impact assessment (1st ed.). Routledge. https://doi.org/10.4324/9780429451355.

Strickland, L.S., Hunt, L.E., 2005. Technology, security, and individual privacy: New tools, new threats, and the new public perceptions. J. Am. Soc. Inf. Sci. Technol. 56 (3), 221–234.

Thompson, N., McGill, T., Bunn, A., Alexander, R., 2020. Cultural factors and the role of privacy concerns in acceptance of government surveillance. J. Assoc. Inf. Sci. Technol. 71 (1), 3–14. https://doi.org/10.1002/asi.24372.

Van den Broek, T., Ooms, M., Friedewald, M., van Lieshout, M., Rung, S., 2017. Privacy and security: Citizens' desires for an equal footing. In: Surveillance, Privacy and Security, 1st ed. Routledge. https://doi.org/10.4324/9781315619309.

Veisten, K., Flügel, S., Bjørnskau, T., 2011. Public's trade-off between a new risk-based airport screening and asserted terror risk impact: A stated choice survey from Norway. Journal of Transportation Technologies 1 (2), 11–20. https://doi.org/10.4236/jtts.2011.12003.

Verhelst, H.M., Stannat, A.W., Mecacci, G., 2020. Machine learning against terrorism: How big data collection and analysis influences the privacy-security dilemma. Sci. Eng. Ethics 26 (6), 2975–2984. https://doi.org/10.1007/s11948-020-00254-w.

West, D.M., Orr, M., 2005. Managing Citizen Fears: Public Attitudes Toward Urban Terrorism. Urban Aff. Rev. 41 (1), 93–105. https://doi.org/10.1177/1078087405278642.

Wester, M., Giesecke, J., 2019. Accepting surveillance – An increased sense of security after terror strikes? Saf. Sci. 120, 383–387. https://doi.org/10.1016/j.ssci.2019.07.013.

Wynne, B., 2006. Public Engagement as a Means of Restoring Public Trust in Science: Hitting the Notes, but Missing the Music? Community Genet. 9 (3), 211–220.