Terrorism – Studies, Analyses, Prevention, 2024, no. 6: 479–497

https://doi.org/10.4467/27204383TER.24.033.20253

Article

Shaping public perception of surveillance – proposed solutions[1]

Bartosz Bochyński

Independent author

https://orcid.org/0009-0002-4180-2395

Abstract

The article presents proposals for actions aimed at shaping the desired perception of surveillance by Polish citizens. It addresses the following issues: the terminology of operational control and the public perception of specific concepts covering surveillance issues, the impact of trust in the special services and the institutions supervising them on the public's approach to the issue of surveillance, and the level of the public awareness of security. The article cites the results of a survey conducted by the author in 2023 and an analysis of material on surveillance and its public perception. Based on these, solutions are proposed to raise public awareness of the need for specific security activities.

Keywords

surveillance, security, antiterrorism, special services

[1] The article is based on a bachelor's thesis entitled *Shaping public perception of surveillance as part of increasing the effectiveness of anti-terrorist activities*, defended at the Faculty of National Security of the War Studies University in Warsaw. The author used excerpts from chapters 2. and 4. and Appendix 1. The thesis was awarded in the 13th edition of the competition of the Head of the Internal Security Agency for the best doctoral, master's or bachelor's thesis concerning state security in the context of intelligence, terrorist, economic threats.

Introduction

The emergence of information about further powers or surveillance tools used by state institutions intensifies public debate on this issue. A large number of articles, programmes and speeches then appear, outlining the shortcomings and inadequacies of such activities[2]. This leads to misunderstanding and sometimes even conflict between the public and the services responsible for state security.

A manifestation of this conflict is society's opposition to regulations authorising the services to use surveillance methods. Analysing the available materials in Polish and English, it can be seen that articles describing the negative sides and effects of surveillance predominate, while those taking into account its positive aspects are missing. This makes it difficult to obtain reliable, neutral information. Statements by experts attempting to present the benefits of surveillance activities are met with criticism, including accusations of being unrealistic, failing to see the negatives or long-term effects. There is also a lack of publications on issues related to shaping the public's perception of such activities.

The article uses a survey targeting Polish citizens over the age of 18, with varying levels of education and representing different backgrounds, including but not limited to academia and those related to the critical infrastructure of the state. The survey was prepared using the Google Forms application and conducted online in 2023. Sixty people took part in the survey.

The aim of this article is to present the problems associated with the negative public perception of surveillance and to present solutions that would enable this perception to be positively altered, thereby increasing the effectiveness of counter-terrorism operations carried out using surveillance methods.

[2] See: *Polska: Zmiany w ustawie o policji rażąco naruszają prawa człowieka* (Eng. Poland: Amendments to the Police Act grossly violate human rights), Amnesty International, 29 I 2016, https://www.amnesty.org.pl/polska-zmiany-w-ustawie-o-policji-ra%C5%BC%C4%85co-naruszaj%C4%85-prawa-cz%C5%82owieka/ [accessed: 21 VII 2024].

Connotations of the notion of surveillance

One of the problems related to operational control is that the introduction of new legislation broadening the powers of the services in this area is accompanied, as already mentioned, by unfavourable media coverage. A plethora of negative information, without a counterbalance of positives, creates an aversion to these solutions in society. The presentation of the disadvantageous aspects of operational control is often associated with the use of the term surveillance. Aleksandra Kustra stated rightly that the Polish word *inwigilacja* denoting surveillance has a strong pejorative connotation, as it is most often associated with oppression, the actions of authoritarian and totalitarian states, where the information obtained is used for political control and manipulation of society[3].

In Poland, the experience of several decades of the communist system, in which the state apparatus and the methods it used were associated with oppression, is to some extent responsible for the sceptical attitude towards surveillance activities. In the period of the People's Republic of Poland, information obtained by means of operational work, including correspondence control or wiretapping[4], was used for political purposes. Consequently, in Poland, surveillance is colloquially associated with activities aimed primarily at society and threatening individual freedom.

In a survey conducted by the author, 90% of respondents answered that the notion of surveillance had negative overtones for them (of which 55% strongly negative and 35% rather negative). In response to a closed multiple-choice question about what they associate the notion of surveillance with, respondents were significantly more likely to indicate that it is associated with control of society (55% to a very large extent and 37% to a large extent) and oppression (20% to a very large extent and 42% to a large extent) than with watching over the security (17% to a very large extent and 28% to a large extent) – (Figure 1). The original Latin word *invigilare* meant to follow, observe or supervise, as well as to watch over

[3] A. Kustra, *Inwigilacja – podstawowe znaczenia* (Eng. Surveillance – basic meanings), in: *Społeczeństwo inwigilowane w państwie prawa* (Eng. Surveillance society under the rule of law), P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński, Toruń 2003, pp. 9-11.

[4] T. Ruzikowski, *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989)* (Eng. Instructions for operational work of the security apparatus (1945-1989)), Warszawa 2004, p. 93.

someone or something and to be concerned about someone[5]. The results show that the term surveillance is more often associated negatively.

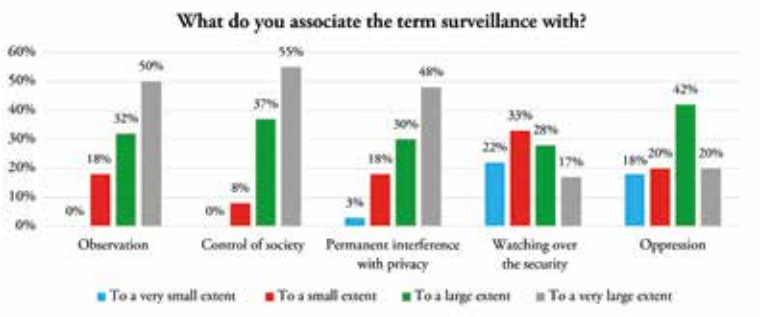

Figure 1. Associations related to the concept of surveillance.

Source: own elaboration.

As Krzysztof Chmielarz notes, the negative connotation of the term is a phenomenon that is rather present in public debate and in the public mind. In legal terminology it has a neutral meaning due to the specificity of legal jargon[6]. It can be assumed that replacing this word with another one without a pejorative connotation would allow for a more substantive dialogue on this type of operational activity. However, the associations indicated by the respondents with the word surveillance confirm that changing the perception of this issue is a difficult task.

Operational control is a specialist term less frequently used in public discourse than surveillance. In order to find a neutral (unmarked) and more commonly used substitute in everyday language to describe this set of activities, one would have to look for words that are frequently used and that refer to a similar conceptual scope. A good example might be the English word *surveillance,* which in addition to operational control in the sense

[5] P. Tomczyk, D. Mider, J. Grzegorczyk, *Inwigilacja elektroniczna jako metoda pozyskiwania informacji – ewaluacja i prognozy* (Eng. Electronic surveillance as a method of obtaining information – evaluation and forecasts), "Studia Politologiczne" 2019, vol. 54, D. Mider (ed.), p. 260. https://doi.org/10.33896/SPolit.2019.54.10.

[6] K. Chmielarz, *Prawo do prywatności a bezpieczeństwo wewnętrzne państwa. Kontrola operacyjna i dane telekomunikacyjne w kontekście inwigilacji społeczeństwa* (Eng. The right to privacy and state internal security. Operational control and telecommunications data in the context of public surveillance), Warszawa 2020, p. 78.

of data collection is also commonly used to describe the phenomenon of observation as well as video and digital monitoring systems. This may lead to the conclusion that the effective promotion of the word monitoring as a colloquial term for covert operational activities, including operational control, would make it possible to mitigate their negative public perception.

The respondents' answers to the closed question show that they overwhelmingly majority (85%) consider digital monitoring in public places as a tool for improving security rather than restricting freedom (15%). At the same time, 31% of respondents strongly believe and 26% tend to believe that monitoring in public places does not infringe on their right to privacy. This indicates that the use of the word monitoring in the context of operational control could draw the public's attention to the positive aspect of these activities and emphasise their impact on security - as is the case with video monitoring systems. To achieve this, it would be necessary to implement social projects with elements promoting operational control activities under the name of monitoring, which could help to create a counterbalance to the public's negative perception of the word surveillance.

Changing public perceptions of surveillance and the special services is difficult, especially for those who experienced repression and abuse by the communist security organs. After the fall of communism, there was a lack of action to repair the image of the services, which makes it all the more important to conduct information campaigns on the subject. They should be directed above all to young people, who not only constitute the future personnel of the Polish special services, but will also shape the environment in which these services will operate.

Trust in and oversight of special services

The desirable state of affairs would be for the public to have full confidence in the special services of its own state. However, this is difficult to achieve even in very aware societies such as Israel's[7]. Democratic governments have therefore created mechanisms to oversee the operation of the special services to protect the public from abuse. The public needs to know that

[7] An excerpt from the bachelor's thesis, on which this article was based, was devoted to providing examples of societal approaches to surveillance in states in different regions of the world, including Israeli society.

such control exists and is effective in order to be able to build a high level of trust in these services. However, independent oversight, inter alia on the issue of operational control, does not necessarily prevent the effective work of officers. This is also confirmed by the example of Israel.

In attempting to analyse the problem, it may be noted that it is not the activities themselves that are part of operational and reconnaissance activities pose the problem, but precisely the lack of effective control over them. In a substantive way, it is usually voiced by those who realise the importance of security and the role of the special services in ensuring it and are far from taking away the powers of operational control from the services. Wojciech Klicki of the Panoptykon Foundation stated that: (...) *when we talk about control over the services, we are not talking about taking away some powers from them,* (...) *so that they are not effective. What we are talking about is that the activities they carry out should be monitored, supervised by someone from the outside*[8].

Respondents overwhelmingly stated that the special services are effective in obtaining information relevant to state security, with 20% considering these activities very effective and 60% considering them rather effective.

When asked in a closed multiple-choice question about in which of the indicated aspects related to intelligence collection they consider the special services to be trustworthy, more than half of the respondents considered that in all of them (Figure 2).

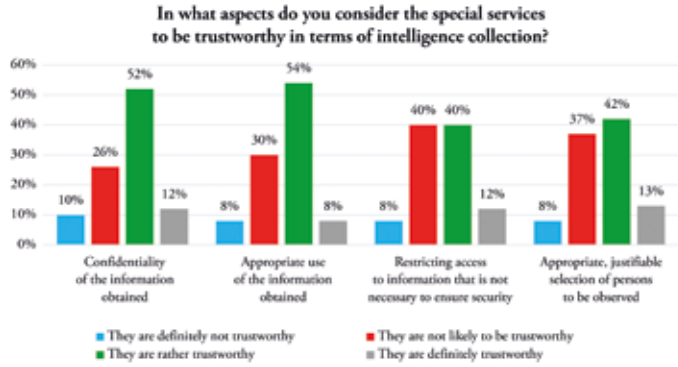

Figure 2. Trust in the special services in the field of intelligence collection.

Source: own elaboration.

[8] *Podsumowanie roku: czy 2022 r. był dobry dla wolności i prywatności?* (Eng. Summary of the year: was 2022 a good year for freedom and privacy?), YouTube, 12 I 2023, https://www.youtube.com/watch?v=TE-9QrbdDwA [accessed: 4 V 2023].

The expansion of surveillance powers, particularly concerning actions on a massive scale, however, requires far greater trust on the part of the public and a belief that these powers will be used for the sole purpose of providing security. The public must be aware that it is not they who are being targeted, but rather individuals who pose a serious threat to the security of the state. The concept of *nontargets*[9] is one of the key factors in ensuring that the public does not oppose the broad powers of their state's secret services. Among those who took part in the survey, 23% definitely and 48% rather fear that information collected about them during surveillance activities could be used against them even if they did not pose a threat to public security. This attitude makes it difficult to introduce the concept in Poland.

The conditions for developing awareness of *nontargets* can be created by adequate control to prevent operational actions being directed against the wrong people. External oversight of the services, particularly in the area of operational control, is a means of reducing the public's fear of this type of operational and reconnaissance activity and of preventing abuse more effectively. Control should be exercised by bodies or institutions that enjoy public confidence. The simplest and most obvious solution is control of the special services by their own internal units. However, this requires a very high level of public trust in the service in question as a whole institution and, as indicated earlier, unfortunately, both in Poland and in most countries, this is not high enough to rely on their self-control alone.

The specific nature of the activities of the special services means that operational work is classified and requires the secrecy of information. However, independent oversight can be carried out in a way that ensures both privacy and confidentiality of operations. It is essential that this control is exercised by appropriate state institutions, such as parliamentary and judicial bodies, which would have access to classified information of a certain classification and would be able to ensure an appropriate level of control while maintaining secrecy. In the case of Poland, these include the Council of Ministers and the Sejm's Special Services Committee.

[9] See: S.A. Duke, *Nontargets: Understanding the Apathy Towards the Israeli Security Agency's COVID-19 Surveillance*, Surveillance & Society, 5 III 2021, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14271 [accessed: 20 VI 2024]. https://doi.org/10.24908/ss.v19i1.14271. The article presents a formulation referring to the peculiar attitude of Israeli society, stemming from the awareness that it is not the target of the state special services.

However, research conducted by the Centre for Public Opinion Research (CBOS) shows that only 32% of surveyed Poles trust the government and 23% trust the parliament[10].

Operational control should be properly justified and conducted in accordance with defined procedures and standards. In Poland, permission for its introduction is granted by the courts. However, according to a survey conducted by CBOS, more than half of Poles do not trust courts[11]. Such a lack of trust does not only characterise our country, it is noticeable to varying degree in many places in the world[12].

A public that lacks confidence in the authorities carrying out oversight of the special services lacks confidence in the reliability of this oversight and is itself unable to control. Moreover, when the public's awareness of state security risks is not high enough to enable it to properly assess the necessity of certain measures by the services, it is highly likely to seek to limit the services' ability to interfere with privacy and other freedoms.

It is worth asking whether there is a chance to reconcile effective supervision of operational control services with their effective operation. This requires a balance between actual security needs and civil rights and freedoms. An important factor in making this possible is also the creation of appropriate rules and procedures and a transparent framework for action. It is possible to point to examples of security systems around the world (e.g. Denmark[13]) where oversight mechanisms such as independent control bodies, parliamentary commissions, courts or prosecutors' offices tasked with monitoring the performance of the special services enjoy the confidence of both the public and the services themselves.

At the same time as restoring public confidence in the institutions overseeing the special services, measures should be taken to shape public perception of these services. The survey shows that 20% of respondents

[10] *Zaufanie społeczne* (Eng. Public trust), "Komunikat z badań CBOS" 2022, no. 37, https://www.cbos.pl/SPISKOM.POL/2022/K_037_22.PDF, p. 9 [accessed: 20 VI 2024].

[11] Ibid.

[12] *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex Policy Environment*, OECD, 2024, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf [accessed: 25 VII 2024].

[13] *OECD Survey on Drivers of Trust in Public Institutions 2024 Results – Country Notes: Denmark*, OECD, 10 VII 2024, https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/denmark_ac5b6973-en.html [accessed: 23 VII 2024].

assess the promotion of the special services to the public as completely ineffective and 46% as rather ineffective (Figure 3). Steps must therefore be taken to change the approach to working with the public, whose acceptance and support are needed for these institutions to be more effective.

This is confirmed by the words of Col. Grzegorz Małecki, former Head of the Foreign Intelligence Agency: (...) *western political and governmental elites and intelligence services are fully aware that trust in security and intelligence structures is, in the conditions of modern democratic societies, the foundation of their activities, without which they lose their raison d'être and ability to perform their tasks*[14].

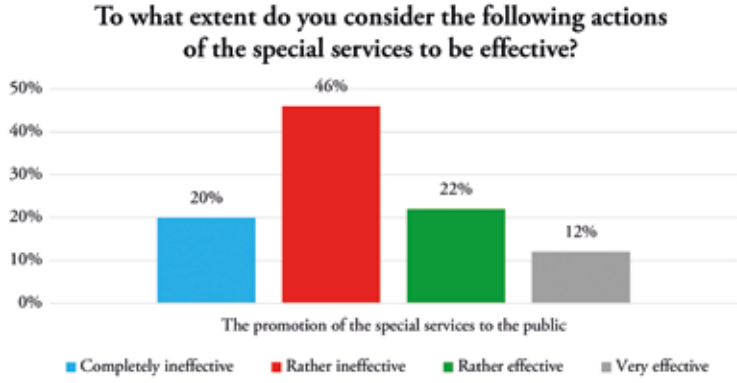

Figure 3. Effectiveness of the promotion of the special service to the public.

Source: own elaboration.

The changing environment in which the special services operate means that information on the activities of these services and their promotion should constitute a very important image element. As Major Anna Grabowska-Siwiec, an expert on internal security and data analysis, stated: (...) *the time of silence around the services is over*. (...) *To create a positive atmosphere around the services, it is necessary* (...) *to talk about what they do* (...)[15].

[14] G. Małecki, *Służby wywiadowcze między zaufaniem a kontrolą* (Eng. Intelligence services between trust and control), InfoSecurity24, 19 XII 2017, https://infosecurity24.pl/sluzby-specjalne/sluzby-wywiadowcze-miedzy-zaufaniem-a-kontrola-analiza [accessed: 2 V 2023].

[15] *Kontrwywiad jest obszarem nieznanym i niezrozumiałym* (Eng. Counterintelligence is an unknown and incomprehensible area), conversation between J. Rauby, A. Grabowska-Siwiec and S. Kuligowska, YouTube, 16 I 2023, https://www.youtube.com/watch?v=CMbE6e3qyHo [accessed: 2 V 2023].

It is important that, where possible, operations are transparent, the public is informed about them and that the services explain what procedures are in place to protect citizens' privacy.

In Israel in 2018 Nadav Argaman, director of Shabak, or the Israeli Security Agency, reported on the successful thwarting of 250 major terrorist attacks in just six months, largely enabling the agency he heads to implement advanced technological solutions, including surveillance[16]. Such activities help to shape a more positive perception of surveillance among the public, which has the opportunity to see its real, positive impact on security.

Public perception of surveillance

The survey found that just over half of those surveyed (55%) would be willing to sacrifice their right to privacy for the sake of increased security by having the Polish special services obtain powers to conduct mass surveillance of cyberspace. Respondents were asked to make their choice on the assumption that there would be no abuse and misuse of the data obtained in this way. Currently, media coverage in Poland is dominated by negative opinions on the changes related to the new surveillance powers of these services. Such a result of surveys may be related to the fact that the awareness of *nontargets* cannot be formed in a society which receives a message about the misuse of powers by the special services and which does not have the opportunity to relate it to information about the benefits of such solutions.

When asked to what extent the indicated entities use surveillance (closed multiple-choice question, Figure 4), respondents said that the companies responsible for social networks and instant messaging use surveillance the most (45% believe they use surveillance to a very large extent and 45% to a large extent) and state institutions (47% to a very large extent and 40% to a large extent).

[16] J.A. Gross, *Shin Bet says 250 'significant terror attacks' thwarted since January*, The Times of Israel, 13 VI 2018, https://www.timesofisrael.com/shin-bet-says-thwarted-250-significant-terror-attacks-since-january/ [accessed: 2 V 2023].

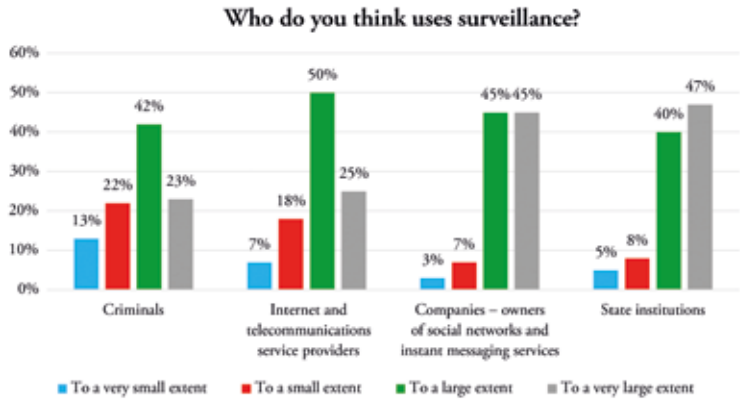

Figure 4. The scale of surveillance used by various actors.

Source: own elaboration.

The results indicate that respondents gave similar assessments of the degree of surveillance used by big techs and state institutions. However, the collection and use of user information by large well-established technology companies[17] and the collection by services are assessed differently by respondents. Companies such as Apple, Android, Google and Meta Platforms (owner of Facebook, Instagram and WhatsApp, among others) constantly report the benefits of data collection in their applications. For example, Apple released a report in 2022 informing about the impact of its app on improving the health, wellbeing or safety of users[18]. In the case of Meta, the app's terms of use include information on how the data will be used to, among other things, "personalise the use of (...) services"[19], provide measurement and analytics services and to protect users' safety[20]. Google, meanwhile, highlights how navigation data

[17] P. Armstrong, S. Balitzky, A. Harris, *BigTech – implications for the financial sector*, ESMA Report on Trends, Risks and Vulnerabilities, no. 1, 2020, https://www.esma.europa.eu/sites/default/files/trv_2020_1-bigtech_implications_for_the_financial_sector.pdf [accessed: 3 V 2023].

[18] *Empowering people to live a healthier day. Innovation using Apple technology to support personal health, research, and care*, Apple, 20 VII 2022, https://www.apple.com/newsroom/pdfs/Health-Report-July-2022.pdf [accessed: 3 V 2023].

[19] *Zasady ochrony prywatności* (Eng. Privacy protection rules), Meta, https://pl-pl.facebook.com/privacy/policy/ [accessed: 3 V 2023].

[20] Ibid.

helps to improve the company's maps and location-based services[21], which were used by more than 21 million Polish users in December 2021[22].

An example that shows the lack of control by these companies over the data they collect can be seen in Google's information on Android software for mobile devices. Even if the user deactivates the app's use of location in the device's settings, it will still record the approximate location using the device's IP address[23].

Many people consent to the surveillance activities of private companies, often without being aware of what they are actually agreeing to. When asked about reading terms and conditions that require acceptance when registering or logging into websites, 22% of respondents said they never read them and 58% said they were unlikely to do so. In addition, half of those surveyed said that when notified of data collection (e.g. cookies) while browsing websites, they usually choose the "accept all" option.

Internet shopping is very popular in Poland[24]. When making such purchases, the buyer often has to provide data such as: name, surname, telephone number, e-mail address and address of residence. Of the respondents asked about their trust in the seller to protect their data from leakage or theft, 17% indicated that they definitely do not trust the seller and 33% that they rather do not. In addition, 47% of respondents do not trust (of which 15% definitely and 32% rather not trust) that the retailer will only use the data to fulfil the order. Nevertheless, resistance to providing such data is lower than for information collected by state institutions.

This may be due, among other things, to the aforementioned difference in the perception of the effects of the use of the both surveillance types. In the case of private companies, in fact, these effects are noticeable and

[21] *Jak dane nawigacyjne pomagają ulepszać Mapy Google* (Eng. How navigation data helps improve Google Maps), Google, https://support.google.com/maps/answer/10565726?hl=PL&ref_topic=6384263 [accessed: 3 V 2023].

[22] *Czołowe platformy z kategorii Mapy i lokalizatory w grudniu 2021 r.* (Eng. The leading platforms in the Maps and Locators category in December 2021), WirtualneMedia.pl, 7 II 2022, https://static.wirtualnemedia.pl/media/images/2013/imagesnew/mapy-grudzien2021.jpg [accessed: 3 V 2023].

[23] *Zarządzanie ustawieniami lokalizacji na urządzeniu z Androidem* (Eng. Managing location settings on an Android device), Google, https://support.google.com/accounts/answer/3467281?hl=pl [accessed: 3 V 2023].

[24] *E-commerce w Polsce 2022* (Eng. E-commerce in Poland 2022), Gemius Polska, 29 IX 2022, https://www.gemius.pl/wszystkie-artykuly-aktualnosci/raport-e-commerce-2022-juz-dostepny.html [accessed: 21 VII 2024].

measurable, and users see them as benefits that make everyday life easier. In the case of the special services, although 70% of respondents believe that the purpose of surveillance methods is to prevent terrorism (of which 30% definitely yes and 40% rather yes) and 72% believe that crimes other than terrorism are prevented (of which 22% definitely yes and 50% rather yes), as many as 85% (of which 40% definitely yes and 45% rather yes) also consider political control of society to be such a purpose (closed multiple-choice question, Figure 5).

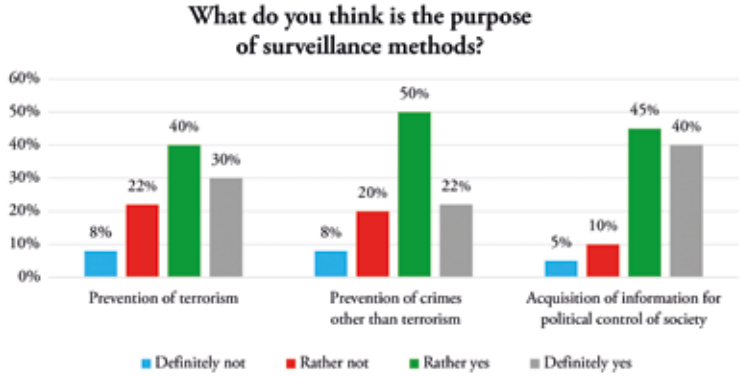

Figure 5. Objectives of surveillance activities.

Source: own elaboration.

Regarding the potential use of mass surveillance 84% of respondents believe it would noticeably affect their daily lives (of which 40% say it would definitely affect them, and 44% say it would rather affect them).

The Polish public is not adequately informed of how large part of the activities involve the use of technical means of surveillance, as is the case, for example, in Israel. If surveillance is presented as an important part of providing security, e.g. by showing in public campaigns the successes of the services achieved through operational control tools, this may reduce public resistance to it.

Level of public awareness

A factor that should be noted in the context of trying to shape a positive perception of surveillance is the level of public awareness. After analysing the issue of anti-terrorism awareness in Israeli society, it can be seen that one of the key aspects that determine attitude towards Israeli services and the methods they use is the high level of awareness regarding the reality in which this society operates. The terrorist prevention used by the Israeli authorities aims to bring about a state in which as many citizens as possible are aware of the threats and know how to act in the event of their occurrence.

An appropriate level of risk awareness among the Polish public is therefore essential for the effective promotion of preventive and protective methods. In the questionnaire survey, one of the questions concerned knowledge of the terrorist threat alert level currently in force on the territory of the Republic of Poland. Only 40% of the respondents correctly indicated one of the two alert levels (the survey was conducted between 12 and 30 April 2023, when the second alert level BRAVO and CHARLIE-CRP were in force on the entire territory of the Republic of Poland)[25]. Almost half of respondents (47%) did not know, what alert level was in place and 13% of them said that no alert level had been introduced.

The respondents' answers show that in Poland, terrorism prevention, understood in this case as organising social campaigns and training for civilians, despite the efforts and involvement of the Terrorism Prevention Centre of Excellence (hereafter: CPT) of the Internal Security Agency, has not been effective. Such actions of the services were rated as completely ineffective by 16% of respondents and as rather ineffective by 42% (Figure 6). The public awareness campaign 4U! – Uważaj! (Watch out), Uciekaj! (Run), Ukryj się! (Hide), Udaremnij atak! (Stop the attack) conducted by the CPT, implemented at a high level of content, seems to be absent from public space and debate. Only 8% of respondents have seen a TV spot of the said campaign. This is far too little to effectively communicate information and patterns of behaviour crucial to counter-terrorism security.

[25] CRP alert levels provide information about the possibility of terrorist threats of a certain magnitude affecting critical infrastructure ICT systems or public administration. See: *Rodzaje stopni alarmowych* (Eng. The types of alert states), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/mswia/rodzaje-stopni-alarmowych [accessed: 4 V 2023].

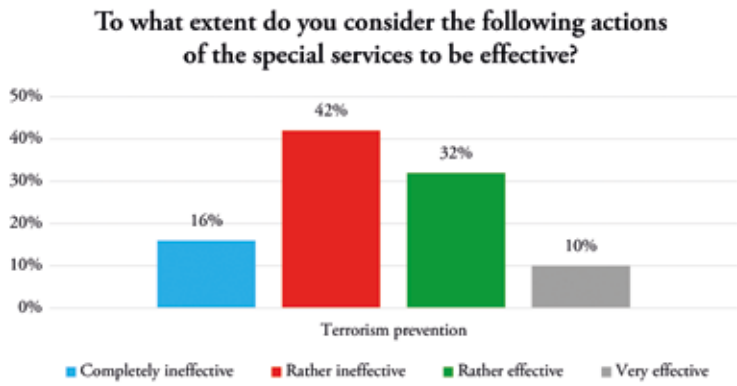

Figure 6. Effectiveness of terrorism prevention understood as organising public campaigns and training for civilians.

Source: own elaboration.

Anti-terrorism training should be available to a wide public and mandatory for employees of public institutions and critical infrastructure of the state. Of those surveyed, only 30% had ever attended such training. More than half said they did not know (15% completely and 37% rather not know) how to behave in a situation of a terrorist attack. When asked what they would do in the event of observing events of a potential terrorist nature, they mostly indicated, however, the correct behaviour. The questions focused on two situations. In the case of a shooting in a public building, 70% of respondents would first take the decision to move away from the scene, which is in line with the *Run, Hide, Fight* behaviour pattern used when threatened by an active shooter[26]. In the case of a package left on the bus, 88% of respondents would notify the driver first, which is the correct behaviour indicated by the CPT among others. In this case, however, such reactions imply reflex actions or actions based on logical thinking. In order to act in a conscious, learned manner in an emergency situation, the correct behaviour must be well assimilated.

[26] *FBI Active Shooter Safety Resources*, FBI, https://www.fbi.gov/how-we-can-help-you/safety-resources/active-shooter-safety-resources [accessed: 1 V 2023].

Summary

In the public space, efforts to shape positive perceptions of operational control are rarely made, while explicitly critical messages dominate. A solution to the problem of negative perceptions of this type of operational activities may therefore be to run wide-ranging public campaigns showing its benefits, e.g. living in a safe country.

Building public trust is a time-consuming process that requires a lot of effort. This can be particularly difficult in relation to the acceptance and understanding of surveillance activities. However, appropriate education of the public and information campaigns on the objectives and procedures associated with operational control can help to increase the level of public trust in the activities of the special services.

It is therefore important to raise public awareness of the special services' role in ensuring security, the need for specific actions and the development of anti-terrorist education in Poland. The cited example of Israel proves that these are actions that not only allow citizens to take care of their own security, but also facilitate the work of state institutions. An aware society that understands the threat from which it is to be protected, is easier to explain the need for specific powers.

A final finding of the survey is that Poles are generally not against the use of strong preventive measures such as non-targeted surveillance methods. More than half of the respondents (55%) indicate that they would be able to sacrifice their right to privacy for the sake of increased security by agreeing to the Polish special services obtaining powers to conduct mass monitoring of cyberspace. This implies that society regards security as a higher value, and that increasing security may be at the expense of privacy.

The measures proposed will make it possible to reduce citizens' suspicion and fear of service actions as well as increase acceptance of operational control. Indeed, in the modern world, cooperation with the public is the foundation of effective activity of state institutions, especially in such a sensitive area as security.

Bibliography

Chmielarz K., *Prawo do prywatności a bezpieczeństwo wewnętrzne państwa. Kontrola operacyjna i dane telekomunikacyjne w kontekście inwigilacji społeczeństwa* (Eng. The right to privacy and state internal security. Operational control and telecommunications data in the context of public surveillance), Warszawa 2020.

Kustra A., *Inwigilacja – podstawowe znaczenia* (Eng. Surveillance – basic meanings), in: *Społeczeństwo inwigilowane w państwie prawa* (Eng. Surveillance society under the rule of law), P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński (eds.), Toruń 2003.

Poradnik prewencji terrorystycznej (Eng. Terrorism prevention guide), ABW, Warszawa 2021.

Ruzikowski T., *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989)* (Eng. Instructions for operational work of the security apparatus (1945-1989)), Warszawa 2004.

Tomczyk P., Mider D., Grzegorczyk J., *Inwigilacja elektroniczna jako metoda pozyskiwania informacji – ewaluacja i prognozy* (Eng. Electronic surveillance as a method of obtaining information – evaluation and forecasts), "Studia Politologiczne" 2019, vol. 54, D. Mider (ed.), pp. 258–294. https://doi.org/10.33896/SPolit.2019.54.10.

Wójtowicz T., *Jak pokonać ISIS? Metody walki z Państwem Islamskim* (Eng. How to defeat ISIS? The method of the fight with Islamic State), "Rocznik Bezpieczeństwa Międzynarodowego" 2016, vol. 10, no. 2, p. 87–109. https://doi.org/10.34862/rbm.2016.2.11.

Internet sources

Armstrong P., Balitzky S., Harris A., *BigTech – implications for the financial sector*, ESMA Report on Trends, Risks and Vulnerabilities, no. 1, 2020, https://www.esma.europa.eu/sites/default/files/trv_2020_1-bigtech_implications_for_the_financial_sector.pdf [accessed: 3 V 2023].

Czołowe platformy z kategorii Mapy i lokalizatory w grudniu 2021 r. (Eng. The leading platforms in the Maps and Locators category in December 2021), WirtualneMedia.pl, 7 II 2022, https://static.wirtualnemedia.pl/media/images/2013/imagesnew/mapy-grudzien2021.jpg [accessed: 3 V 2023].

Duke S.A., *Nontargets: Understanding the Apathy Towards the Israeli Security Agency's COVID-19 Surveillance*, Surveillance & Society, 5 III 2021, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14271 [accessed: 20 VI 2024]. https://doi.org/10.24908/ss.v19i1.14271.

E-commerce w Polsce 2022 (Eng. E-commerce in Poland 2022), Gemius Polska, 29 IX 2022, https://www.gemius.pl/wszystkie-artykuly-aktualnosci/raport-e-commerce-2022-juz-dostepny.html [accessed: 21 VII 2024].

Empowering people to live a healthier day. Innovation using Apple technology to support personal health, research, and care, Apple, 20 VII 2022, https://www.apple.com/newsroom/pdfs/Health-Report-July-2022.pdf [accessed: 3 V 2023].

FBI Active Shooter Safety Resources, FBI, https://www.fbi.gov/how-we-can-help-you/safety-resources/active-shooter-safety-resources [accessed: 1 V 2023].

Gross J.A., *Shin Bet says 250 'significant terror attacks' thwarted since January*, The Times of Israel, 13 VI 2018, https://www.timesofisrael.com/shin-bet-says-thwarted-250-significant-terror-attacks-since-january/ [accessed: 2 V 2023].

Jak dane nawigacyjne pomagają ulepszać Mapy Google (Eng. How navigation data helps improve Google Maps), Google, https://support.google.com/maps/answer/10565726?hl=PL&ref_topic=6384263 [accessed: 3 V 2023].

Kontrwywiad jest obszarem nieznanym i niezrozumiałym (Eng. Counterintelligence is an unknown and incomprehensible area), conversation between J. Rauby, A. Grabowska-Siwiec and S. Kuligowska, YouTube, 16 I 2023, https://www.youtube.com/watch?v=CMbE6e3qyHo [accessed: 2 V 2023].

Małecki G., *Służby wywiadowcze między zaufaniem a kontrolą* (Eng. Intelligence services between trust and control), InfoSecurity24, 19 XII 2017, https://infosecurity24.pl/sluzby-specjalne/sluzby-wywiadowcze-miedzy-zaufaniem-a-kontrola-analiza [accessed: 2 V 2023].

OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex Policy Environment, OECD, 2024, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf [accessed: 25 VII 2024].

OECD Survey on Drivers of Trust in Public Institutions 2024 Results – Country Notes: Denmark, OECD, 10 VII 2024, https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/denmark_ac5b6973-en.html [accessed: 23 VII 2024].

Podsumowanie roku: czy 2022 r. był dobry dla wolności i prywatności? (Eng. Summary of the year: was 2022 a good year for freedom and privacy?), YouTube, 12 I 2023, https://www.youtube.com/watch?v=TE-9QrbdDwA [accessed: 4 V 2023].

Polska: Zmiany w ustawie o policji rażąco naruszają prawa człowieka (Eng. Poland: Amendments to the Police Act grossly violate human rights), Amnesty International, 29 I 2016, https://www.amnesty.org.pl/polska-zmiany-w-ustawie-o-policji-ra%C5%BC%C4%85co-naruszaj%C4%85-prawa-cz%C5%82owieka/ [accessed: 21 VII 2024].

Rodzaje stopni alarmowych (Eng. The types of alert states), Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/mswia/rodzaje-stopni-alarmowych [accessed: 4 V 2023].

Ustawa antyterrorystyczna to „waterboarding" dla wolności słowa w sieci (Eng. Anti-terrorism Act is "waterboarding" for online freedom of expression), Fundacja Panoptykon, 10 V 2016, https://panoptykon.org/wiadomosc/ustawa-antyterrorystyczna-waterboarding-dla-wolnosci-slowa-w-sieci [accessed: 21 VII 2024].

Zarządzanie ustawieniami lokalizacji na urządzeniu z Androidem (Eng. Managing location settings on an Android device), Google, https://support.google.com/accounts/answer/3467281?hl=pl [accessed: 3 V 2023].

Zasady ochrony prywatności (Eng. Privacy protection rules), Meta, https://pl-pl.facebook.com/privacy/policy/ [accessed: 3 V 2023].

Zaufanie społeczne (Eng. Public trust), "Komunikat z badań CBOS" 2022, no. 37, https://www.cbos.pl/SPISKOM.POL/2022/K_037_22.PDF [accessed: 20 VI 2024].

Bartosz Bochyński

A graduate of the bachelor's degree at the Department of International Security and Diplomacy of the War Studies University in Warsaw.

Contact: bbf16@interia.pl