Juraj Dobrila University of Pula

**"The impact of technology on the prevention of terrorist attacks"**

Research report

Pula, January 2020

Juraj Dobrila University of Pula

**"The impact of technology on the prevention of terrorist attacks"**

Research report

Students:

Direction:

Case:

Mentor:

Pula, January 2020

Content

[1.](#_Toc30455040)  [Introduction](#_Toc30455040)  [1](#_Toc30455040)

[2.](#_Toc30455041)  [Elaboration](#_Toc30455041)  [2](#_Toc30455041)

[3.](#_Toc30455042)  [Aim and Hypothesis](#_Toc30455042)  [4](#_Toc30455042)

[4.](#_Toc30455043)  [Research simulation (sample selection)](#_Toc30455043)  [5](#_Toc30455043)

[5.](#_Toc30455044)  [Validity](#_Toc30455044)  [5](#_Toc30455044)

[6.](#_Toc30455045)  [Conclusion](#_Toc30455045)  [7](#_Toc30455045)

[7.](#_Toc30455046)  [References](#_Toc30455046)  [8](#_Toc30455046)

# Introduction

Terrorism is one of the worst, if not the worst, forms of violence against civilians. It is defined as any act of violence, most often armed against innocent people. Terrorism as a construct is the result of a number of factors - political, historical, ideological, economic, social - and with its effects to this day remains an inexplicable phenomenon and the greatest threat to the security of today's society. The primary goal of terrorism is mainly socially oriented, for example of a political or religious nature, and uses direct attack on victims or various forms of threats as a method of spreading fear (hence the name terror - terrorism) among indirect victims. It is generally considered a form of political violence, although the line between military and political violence is often very fragile in cases of terrorism at a higher level. Although it often turns out that way in today's society and media, terrorism is not something new or foreign, the phenomenon itself as such has almost certainly existed since people began the first forms of political arrangements or sedentary lifestyles. In response to terrorism, its counterbalance has been created, ie counter-terrorism, which manifests itself in various ways, such as special police and military units, state programs for observing potentially critical groups or persons, and the like. The most famous example of the state response to terrorism is probably the American "Patriot Act", which resulted from one of the most influential terrorist attacks in world history, the attack on September 11, 2001 (November 9). It is just one of many initiatives to use technology to fight terrorism. Although technology has definitely helped prevent many disasters, it has also helped bring about a new type of terrorism, so-called "cyber" terrorism, using all sorts of illegal methods of exploiting people and data. The development of technology and mass media has greatly contributed to the development of terrorism. The Internet and the Mass Media have become a key means of communicating and conveying ideals. Therefore, we can say that information has become a weapon of the new age that can create many more negative consequences than conventional weapons. Despite the fact that technology can be dangerous in the wrong hands, it is proving to be an invaluable tool in the fight against terrorism, which is the subject of this research.

# Elaboration

Terrorism has changed radically in recent decades, and research from the United States shows that the use of preventive technology, as well as that for sudden security reactions, has actually relatively reduced the number of terrorist attacks. Despite this, it should be said that although the number has decreased, the attacks themselves are often more radical and more deadly than they used to be. In fact, this shows that although technology is very useful in the fight against terrorism, it is not yet at a definitive level, ie one that would completely stop terrorist attacks before they happen. The American Hoover Institute states that there are 5 main points in the fight against terrorism; sensors, technologies for identification, data collection and analysis, constant advancement of technology and the most critical ie ethical and legal barriers. It is this last problem that causes the most debates and conflicts on all sides of the political spectrum, and it is a conflict of breaking the privacy of citizens in the name of the fight against terrorism. In the aforementioned observation, published under the title "Technology for Preventing Terrorism", [[1]](#footnote-1)Sofaer comments that the role of technology should unquestionably increase because on the scale of today's imports and exports, border protection can devote approximately 2 minutes to vehicles carrying who for what or whom inside. He continues that investing in various scanners and similar preventive technologies is perhaps the only reliable way to tackle this problem without extreme measures such as closing borders or other economically destructive methods. An example is the government's response to trading and freezing international change after the 2001 attack, an approach that has proven to be minimally successful in terms of the amount of lost change and trade between legitimate and fair companies. From this very real example, we can immediately see why the advancement of prediction and stop technology is much more valuable both from the perspective of victim protection and the economic consequences of a “rough” approach. RAND is a non-profit organization that analyzes the problems faced by the global private and public sectors, including terrorism and the fight against it. "Technology Acquisition by Terrorist Groups" [[2]](#footnote-2)is an article published by RAND Corporation and the George Washington University Center for International Science and Technology Policy, which talks about the development of technology in counter-terrorism and how technology affects terrorism. They point out that the technology for the prevention of terrorism, ie scanners, metal detectors and the like, is one of the definitely invaluable tools in the fight against terrorism, at least in the past.

It is precisely because of these preventive methods that today's terrorists have switched to various forms of biochemical and even primitive nuclear terrorism, which are much more difficult to predict or stop by the scanners themselves. That is why they point out that it is necessary to develop technology that directly benefits from today's computers and their processing power. They go on to take the computational ability to process massive amounts of data and combine it with communication between various police or research stations to actually anticipate and understand threats through various sequencing algorithms and linking similar events that have already been recorded. They also explain one of the great problems of counter-terrorism today, and that is the "arms" race between governments and terrorists in terms of technology. The reason why this is complicated is exactly what makes technology what it is - connectivity. For example, in a terrorist attack with any standard weapon, often only one trained person is needed, while computers and all other "cyber" weapons require teams of experts, stable connections and other elements to work effectively. Such levels of organization are difficult to achieve and hampered by the fact that the leaders and administrations of terrorist organizations are mostly organized not by profession but by ideology and beliefs. This is one of the weaknesses that modern technology can use against extremist or isolated groups. Namely, a state organization that is connected to the rest of the world and deals with the most modern technology and experts can break through the codes and barriers of terrorist associations much easier, ie anticipate and stop potential attacks. Finally, an example of how states and legal entities in reality deal with terrorism from a legislative perspective, ie "Analysis of the positive legal National Strategy for the Prevention and Suppression of Terrorism" by [[3]](#footnote-3)Đurđica Radaković. From this perspective, we need to look at terrorism as a global phenomenon, one that ignores state borders and, as stated above, requires coordinated action by various organizations and state units. He states that counter-terrorism strategies include the following: preventing and preventing the spread of terrorist ideals, recognizing and stopping extremism before the stage of terrorism, good study and inter-state cooperation in exchanging data, experiences and practices, and strengthening technology and the direct counter-terrorism sector.

The methods for direct conflict with terrorism include the development and establishment of a system for general protection and security of infrastructures, and the most important part for this topic - the creation of a security network for the protection of civilian zones and online protection against "cyber" terrorism.

The goal of all this is not only to stop deaths and literal attacks, but also to stop material and property damage to citizens and state institutions.

One very important element of any form of public surveillance and scanning was also emphasized, and that is that despite the threat posed by terrorism, the state must never exceed the basic human rights to freedom of speech and action as well as to privacy. That is, although states have the ability to take the initiative and establish all forms of surveillance and scanners, everything they do must be within the framework of internationally agreed human rights, ie a system should be established that balances privacy and freedom of citizens and their general security.

# Aim and Hypothesis

The aim of our research is to analyze the impact of face and iris sensors on the prevention of terrorist attacks at the entrance and inside Amsterdam Airport in 2019.
This goal is in line with SMART principles:

|  |  |  |
| --- | --- | --- |
| WITH | Specific | It specifically focuses on the relationship between Technology and Terrorism |
| M | Measurable | It is measurable because one can observe the time elapsed since the implementation of new technology and terrorist attacks or the time interval between the committed terrorist acts since the use of technology |
| AND | Achievable | Preventive technology can already predict a lot of data analysis today, in the future will be able to go through mass databases and algorithms in a short time |
| R | Relevant | Implementation of observation and recording technology is already underway |
| T | Trackable | The whole action is based on data collection and analysis, so just adding some measuring devices should not be complicated as such. |

Alternative Hypothesis (H 1 ): There is a statistically significant association between the use of face and iris sensors and the prevention of terrorist attacks.

Null hypothesis (H 0 ): There is no statistically significant association between the use of face and iris sensors and the prevention of terrorist attacks

# Research simulation (sample selection)

All people who passed through Amsterdam Airport in 2019 were taken as a sample. The research is very specific, as it is not known when a terrorist attack could occur, so we test the technology of sensors to recognize faces and irises throughout the year and on all people who pass through the airport. This would mean that the sensor records all airport staff and passengers.

Construct 1 is the use of face and iris recognition sensors and is an independent variable the number of sensors at the entrance and within the airport. Construct 2 is the prevention of terrorist attacks and the dependent variable will be the number of defended terrorist attacks. Construct 2 depends on the implementation of Construct 1 as it hypothesizes that the number of terrorist attacks should fall through the use of preventive technology

# Validity

In order for component validity to be met, the selected variables must accurately measure the terms in the hypothesis. In this case, there is a link between the number of face and iris recognition sensors and the number of prevented terrorist attacks at Amsterdam Airport for 2019. To determine internal validity, a survey should be conducted to see the consequences. Without conducting research, we can assume that the use of face recognition sensors affects the prevention of terrorist attacks. Also, the internal validity is fully met if the component validity has been previously met, which is met in this case. External validity is fulfilled, since the component and internal validity are previously fulfilled, and our hypothetical relationship can be proven in other situations, ie in our case it can be generalized since the newer preventive technology serves to defend against terrorist attacks in all fields, not only at airports. There are 4 criteria of causality, ie cause and effect are related (the use of sensors to recognize the face and iris is associated with the prevention of terrorist attacks). The cause precedes the consequence, ie the use of sensors for recognizing faces and irises precedes the consequence, which in our case is the prevention of terrorist attacks.

Cause and effect occur consistently together, ie covariate, ie in the case of the cause (sensors for scanning the face and iris), we see the consequence (defense against terrorist attacks). Alternative explanations, such as that terrorism at airports has been reduced regardless of the implementation of scan sensors for the reason that anyone that has passed through the airport is being recorded and scanned so this explanation can be dismissed. There are also threats to internal (causal) validity. The first threat is with regard to participants who may mature at the time of the experiment, or that a natural change may occur. This would mean that participants who committed more serious offenses as young people now realize that it is bad for their future and change their lifestyle for the better. Such a development of the situation can lead to alternative explanations, and to avoid this, we control the situation to other people who pass through the airport. This would mean that if natural change occurs in other people passing by, we neglect in research the possibility of maturation as a possible explanation. Also, the next threat with regard to participants is selection, ie it is the difference in the characteristics of the selected subjects. Such a threat can be eliminated as people pass through the airport that we, as researchers, did not deliberately choose.

Another threat is with regard to the instruments we use when measuring. During research, it can happen that we have a low validity of constructs, ie when we measure another construct or property with an instrument, and not what we observe. The next threat is if the instrument changes during the research, then it can happen that we conclude wrongly because we have changed the method by which we measure the research. The next threat is testing (sensitivity) that affects participants. In this threat, it may happen that the participant, since he knows that the object is being filmed, can moderate his behavior. With such an outcome of the situation, we can draw completely wrong conclusions. The third threat is due to unnatural / artificial reactions. Unnatural reactions must not only have the participant but also the researcher himself - the effect of the researcher's expectations. With this threat, it may happen that we as researchers insist on finding a correlation between our constructs.This can be solved through a research design that is unknown to the researcher, ie the researcher in this case does not know what to expect from the research participants. The fourth threat is in terms of design / procedures . The threat to internal validity is an ambiguous time advantage that indicates a situation where we are not sure whether our hypothetical cause precedes the observed consequence. The next threat is history , that is, if an unforeseen event occurs during the research and is not part of the research, it can provide an alternative explanation.

# Conclusion

With this paper, we confirmed the alternative hypothesis, ie we proved that there is a connection between the use of sensors for facial and iris recognition and the prevention of terrorist attacks. At the airport, the use of advanced technology such as face and iris sensors has reduced the possibility of terrorist attacks as the sensor serves as a prevention and can be responded to right from the start even before the terrorist tries to do something.

Terrorism can affect any place on the globe, but its consequences are becoming global. We must not forget that terrorism has always been and will remain violence with the transparent goal of sowing fear, the only difference is in the way it is achieved. It is never a matter of reckless actions of individuals, behind every act there is a well-developed tactics of organization.

The mass media give terrorism a global reach, influence the way the public perceives terrorism and the threat of it, influence political decisions that respond to terrorism, but also the relationships shaped by national and international policies. Nevertheless, today's technology has evolved to the point that world-class precautions can be taken by proper handling.

# Literature

Fahmy, SS, 2017 .. Media, Terrorism, and Society: Perspectives and Trends in the Digital Age. *Mass Communication and Society* , October 24, Issue 6, pp. 735-739.

Jackson, BA, 2001. Technology Acquisition by Terrorist Groups. *Studies in Conflict and Terrorism* , p.49.

Jackson, R., nd *ENCYCLOPÆDIA BRITANNICA.* [Online]
Available at: https://www.britannica.com/topic/war-on-terrorism

Jenkins, JP, nd *ENCYCLOPÆDIA BRITANNICA.* [Online]
Available at: https://www.britannica.com/topic/terrorism

Plungis, J., nd *ENCYCLOPÆDIA BRITANNICA.* [Online]
Available at: https://www.britannica.com/topic/Reassessing-Airport-and-Airline-Security-1947186

Radaković, Đ., 2016. Analysis of the positive legal National Strategy for Prevention and Suppression of Terrorism. *Police and Security* , 25 (3/2016), pp. 244-258.

Ricijaš, N., Kovčo-Vukadin, I. & Hundrić, DD, 2017 .. *Strengthening Juvenile Justice Systems in the counter-terrorism context: capacity-building and peer-learning among stakeholders.* [Online]
Available at: https://www.bib.irb.hr/971726?&rad=971726

Sofaer, AD, nd *TECHNOLOGY FOR PREVENTING TERRORISM,* Stanford: Hoover Institution, Stanford University.

1. Technology for Preventing Terrorism - Abraham D. Sofaer, Hoover Institution, Stanford University [↑](#footnote-ref-1)
2. Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption - Brian A. Jackson, Center for International Science and Technology Policy, Elliott School of International Affairs George Washington University [↑](#footnote-ref-2)
3. Analysis of the positive legal National Strategy for Prevention and Suppression of Terrorism - Đurđica Radaković [↑](#footnote-ref-3)