Funded by the Horizon 2020 Framework Programme of the European Union
PREVISION - Grant Agreement 833115

Deliverable D1.4
Title: Predictive Policing – Psycho-sociological Models – Revised Release

Dissemination Level:	**CO**
Nature of the Deliverable:	**R**
Date:	**18/09/2020**
Distribution:	**WP1**
Editors:	**IfmPt**
Reviewers:	**PPM, HfoeD**
Contributors:	**ALL**

Abstract: In this document, various theoretical and practical approaches that can contribute to combat cybercrime, organised crime and terrorism are presented, whereby special focus is on predictive policing methods and models. To meet the requirements of the LEAs formulated in the use cases, concrete concepts of tools and services to support the fight against the mentioned crime fields are described. Since the use of predictive policing is particularly beneficial for the fight against and the prevention of terrorism (and especially radicalisation), special attention is paid to this.

**** Dissemination Level:*** *PU= Public, RE= Restricted to a group specified by the Consortium, PP= Restricted to other program participants (including the Commission services), CO= Confidential, only for members of the Consortium (including the Commission services)*

***** Nature of the Deliverable:*** *P= Prototype, R= Report, S= Specification, T= Tool, O= Other*

Disclaimer

Revision History

Date	Rev.	Description	Partner
18/05/2020	0.1	Initial Draft	IfmPt
14/07/2020	0.2	Integration of Requirements and Methods	IfmPt
13/08/2020	0.3	Writing conclusions from the Taskforce Predictive Policing and Radicalisation	IfmPt
09/09/2020	0.4	Input for chapter 4.2	IfmPt/ KEMEA,
10/09/2020	1.0	Final draft for review	IfmPt
16/09/2020	1.1	SAB Review	HfoeD
17/09/2020	1.2	Final Review and comments	IfmPT,/PPM
18/09/2020	2.0	Final Version for submission (D1.4)	IfmPT

List of Authors

Partner	Author
IfmPt	Dr. Thomas Schweer, Kira Langanki, Günter Okon
KEMEA	Eleni Darra

Table of Contents

Revision History 3
List of Authors 4
Table of Contents 5
Index of figures 7
Index of tables 8
Glossary 9
Executive Summary 10
1. Introduction 11
2. Main Definitions – Organised Crime, Extremism/Terrorism and Cybercrime 13
2.1 Organised Crime 13
2.2 Extremism/Terrorism 17
2.3 Cyber Crime 23
3. Prediction/ Forecasting Methods 24
3.1 Criminal Prognosis 25
3.2 Intuitive Method 25
3.3 The Statistical-Nomothetical Prognosis 26
3.4 The Clinical Idiographic Prognosis 27
3.5 Methodology of Criminal Forecasting 27
4. Criminological Theories 29
4.1 Criminological Theories in the context of Predictive Policing 29
4.1.1 Rational Choice Theory 29
4.1.2 Learning Theories 30
4.1.3 Routine Activity Approach 30
4.1.4 The Ecological Approach 31
4.2 Criminological Theories in the context of the use cases (in Cooperation with KEMEA) 33
5. Prediction of Criminal Behaviour – State of Research and description of methods 47
5.1 Investigation support technologies 47
5.1.1 Face Recognition 47
5.1.2 Video Surveillance 48
5.2 Predictive Models to support Security Measures 49

5.2.1 Space and Personal Approaches 51
5.2.2 Further Predictive Approaches 71
6. Concepts of Predictive Policing Tools 86
6.1 Person-related Predictive Policing System 86
6.2 Web-Monitoring System 92
6.3 Network Analysis 94
7. Ethical and Data Protection Aspects of Predictive Policing 99
8. Summary and conclusions 102
9. References 106

Index of figures

Figure 1: Victims of terrorist attacks in Western Europe [24] 20
Figure 2: Terrorist attacks in Western Europe per Year [25] 20
Figure 3: Moghaddam model of radicalisation [85] 43
Figure 4: Model of Online Terrorist Recruitment Progression 46
Figure 5: Comparison of conventional transaction and big data transaction [110] 51
Figure 6: Buffer zone 53
Figure 7: Location of the anchor point 54
Figure 8: Hot spot method 55
Figure 9: Near Repeats 57
Figure 10: Trafford Method [125] 59
Figure 11: Example for Risk Terrain Analysis 60
Figure 12: Risk Terrain-Map [127] 61
Figure 13: State-Morality and People's-Morality 73
Figure 14: Network analysis 80
Figure 15: Example of the web activity on Wikipedia for the article "Breitscheidplatz" before the terror attack in Berlin on December 19th, 2016 81
Figure 16: Example of the web activity on Wikipedia for the article “Breitscheidplatz” after the terrorist attack on December, 19th, 2016 82
Figure 17: Example of a trend visualization - graph 83
Figure 18: person-related predictive policing system 88
Figure 19: Visualization of an analysis of social networks - Ferguson 2018 [178] 96
Figure 20: Local bridges (Granovetter 1973, S. 1365) [177] 97
Figure 21: Personal meetings and telephone calls of Cosa Nostra members Klaubert 2020 [180] 98

Index of tables

Table 1: The security functions of the state [27] 22
Table 2: Explanation and Prognosis [34] 24
Table 3: Summary of relevant Theories applied to radicalisation process 36
Table 4: Analysis model by Urban 2006 67
Table 5: Types of adaption 72
Table 6: Typology of types of individual adaption [2] 74
Table 7: Types of behaviour under conditions of social change [2] 75
Table 8: Characteristics of behaviour types and social change [2] 76
Table 9: Measuring the extremist potential of society 77
Table 10: Risk factors - Person-related Predictive Policing System 90
Table 11: Risk Factors - Web-Monitoring System 93

Glossary

LEA	Law Enforcement Agency
OC	Organised Crime
RTF	Result Transferability Framework
WP	Work Package

Executive Summary

The main purpose of this deliverable D1.4. is to provide a revised report on the characteristics of deviant behaviour, because knowledge about it can be used for the detection of abnormal activities and predictive purposes. In more precise terms, concrete theoretical and practical approaches are presented that contribute to combating cybercrime, organised crime and terrorism, with a special focus on methods and models of predictive policing.

Like D1.2, this report begins with the definitions of organised crime, terrorism respectively extremism and cybercrime as the central areas of interest. The following chapters are devoted to the topics of forecasting and prediction in the context of crime. First, the different models of crime forecasting in general and their methodological implementation options are outlined. Then the central statements of criminological theories are explained and their predictive value for the defence and fight against crime is discussed. Special attention is paid to the theoretical aspects of radicalisation and radicalisation processes, which in particular result from the requirements formulated in Use Case 2.

This is followed by an overview of investigative support technologies in the abovementioned crime areas on the one hand and predictive models for supporting security policy measures against the abovementioned crime areas on the other. Furthermore, special focus is placed on spatial and personal predictive policing.

Then concrete concepts of tools that are supposed to meet the requirements of the LEAs formulated in the use cases are presented. The tools are primarily designed to combat radicalisation and terrorism, since the use of predictive policing is particularly beneficial in this field.

Finally, ethical aspects that should be considered when using predictive policing are discussed. To finalise this deliverable, a summary is provided.

1. Introduction

It is simply impossible to achieve complete safety. Every society is confronted with deviant[1] and criminal behaviour. Crime is a normal social phenomenon. Nevertheless, every state has the obligation to protect its citizens from crime and terrorist threats. This is becoming increasingly difficult against the background of globalisation and increasing technological development. Threats must be analysed quickly and objectively in order for the relevant authorities to be able to react promptly to future risks on the basis of forecasts. Predictive policing is a means of making police work more effective and efficient, but it must be integrated into the work processes of an authority or into the police culture in a longterm and comprehensive manner. Predictive policing is ineffective if it lacks the acceptance of the officers who work inside the relevant systems, or rather without the acceptance of the officers who ultimately have to implement the measures on their daily operations.

Predictive policing is still a rather young but very dynamic branch of criminological research and police work. Especially in the USA, but increasingly also in European countries such as Germany and Switzerland, more and more authorities are working with predictive tools such as Predpol, Hunchlab or Precobs. In addition to the fight against classical crime, predictive policing is becoming increasingly important in the field of combating terrorism, not only in predicting terrorist attacks but also in predicting the course of radicalisation.

The aim of this revised report is to present and elaborate the relevant possible theoretical and methodological approaches within the scope of the tasks of PREVISION, whereby special attention is paid to the benefit that predictive policing can provide. Under consideration of the requirements of the use cases, concrete application concepts are presented. Special attention is paid to Use Case 2 “Radicalisation and terrorist threat prevention”, since the potential of predictive policing can be exploited especially with regard to this Use Case. In concrete terms, concepts of applications, which can be used for the detection of radicalisation and the fight against terrorism and extremism, were developed. These is a person-related predictive policing system and a website-related predictive policing system.

In the phenomenon areas of cybercrime (UC 4) and organized crime (UC 3,5), the possibilities of network and trend analyses are shown. The requirements of the LEA`s for the actual predictive policing were not so clearly formulated here.

Note:

As announced in D1.2, it was considered to be useful to hold a workshop on predictive policing with the LEAs, since the subject area “Predictive Policing” is underrepresented in the use cases. The workshop was held during the 3rd Plenary Meeting in Toulouse in February 2020.

[1] According to Peuckert, deviant behavior is defined as behavior “which violates the social norms of a society or of one of its substructures and which, when discovered, provokes social reactions aimed at punishing, isolating, treating or correcting the person displaying such behavior.“ [179; translated by the author from German] In this context it should be noted that a distinction must be made between the natural, criminal and sociological concept of crime [31].

After the workshop it became clear that the possibilities and restrictions of predictive policing are not so common. The use cases described in the project are primarily aimed at investigation support measures. Only UC 2 Radicalisation & terrorist threat prevention contained defined requirements for prediction in the area of radicalisation. For this reason, this is the main focus in the development of possible solutions.

2. Main Definitions – Organised Crime, Extremism/Terrorism and Cybercrime

For a look into the future, there is the need to look into the past. Predictive policing requires crime data from the past in order to make statements about future crimes. One problem with police data is that it is often incomplete and unstructured or of poor quality. In addition, information is kept in different databases and cannot be brought together due to technical or data protection hurdles. Cooperation between authorities on both national and international level is also often inefficient.

Ultimately, however, the decisive factor is which criminal phenomena are defined as organised crime or terrorism. There are very different perceptions of this among the police and judiciary, but also in society and politics. Security authorities are part of the political system and the political system has a defining power; thus, organised crime and terrorism are also defined as such. This attribution process depends on political opportunities, the influence of economic elites and the position of the perpetrators in the social system. The “crimes of the powerful” [1]2 is often not reflected in data, because although it is threatened with punishment, it is not prosecuted. As one police officer said in a personal conversation with the author: "You don't have to analyse the cases we investigate. You must analyse the cases we are not allowed to investigate!"

So before dealing with the topic of "predictive policing", it makes sense to take a closer look at the terms "organised crime", "terrorism" and "cybercrime". Even if no methodological and technical implementation options and possibilities regarding cybercrime are considered here, it is also defined in the following sections for the sake of completeness.

2.1 Organised Crime

In the media, the terms *mafia*, *organised crime*, *international crime syndicates, racketeering* or *mob are* dealt with in a very undifferentiated way. This is usually associated with criminal groups that are tightly organised and have a high level of criminal energy. The Mafia is usually cited as a classic example of organised crime. This also explains why ethnically homogeneous criminal groups are like to be called the "Red Mafia" (organised crime in Russia; „thieves in the law“) or the "Yellow Mafia" („yakuza“, „triads“) and, in the case of serious crimes, the perpetrator groups are referred to as the "Environmental or Beef Mafia"[3].

"This may be because there has been a lot of talk about the mafia for a very long time and that it is a term, just as in advertising there are terms that stand for one thing, although there are many others from the brand, Maggi, Tempo handkerchiefs [....] Tempo stands for paper handkerchiefs (...) and I could imagine that Mafia is also such a term, and when you say Mafia, then everyone knows that this is something quite dangerous, and with a lot of brutality, and very suspicious, very conspiratorial."

(Excerpt[4] from a qualitative interview conducted by the author with an official of a department responsible

[2] Translated by the author from German
[3] This section was published in advance [2].
[4] Translated by the author from German

for combating organised crime as part of a study on organised crime between 1999 and 2002)

The confrontation with organised crime is exciting and laborious at the same time. It is difficult because there are many hurdles to overcome. First problems already arise with the definition of terms. Klaus von Lampe states that there is a lack of generally accepted criteria and yardsticks "by which the question of the nature or basic character of organised crime could be answered" [3][5]. One can only say "what is associated with it, and one can try to bring halfway order into the confusion" [4][6]. Hobbs states that organised crime is a constantly changing palette of a complex phenomenon and refers to Kelly [5], who emphasizes that the search for an exact definition is neither possible nor desirable. In this context von Lampe emphasizes that "no matter what one understands by organised crime, one is always dealing with networks of criminally useful contacts" [3][7].

Previous research in this field has shown that organised crime groups in Germany are in most cases not "organisations" but criminal networks. Nevertheless, there are groups, especially in the international arena, for whom the label "criminal organisation" seems quite appropriate. Criminal networks differ from criminal organisations in that

"a network [...] is a network of similar bipolar relationships between two or more persons. In contrast, an organisation is characterised by a minimum of integration, i.e. the participants subordinate themselves to a collective will, there is a collective consciousness and a more or less differentiated structure, which is described by terms such as 'division of labour' and 'hierarchy': In short: a network consists of the sum of its parts, an organization is more than that" [3].[8]

Criminal organisations can fulfil several functions: on the one hand economic (profit making), on the other hand social (feeling of togetherness, granting of status in the criminal milieu etc.) and quasi-state functions (e.g. conflict resolution, granting of protection).

Similar to society as a whole, the criminal world is also hierarchically structured. The position in this hierarchy is measured not only by the social and economic, but also by the cultural and symbolic capital of the respective actors.[9] In this respect, the upper world is a reflection of the lower world. While some may be protected by political reputation, others have language barriers and cultural peculiarities that complicate police investigations. In this respect, Kinzig [7][10] is right when he advises to speak about "crime that is difficult to ascertain" instead of "organised crime". It is also difficult to identify because in many cases it is a question of victimless crimes or because countless members of society and institutions benefit from the activities of organised crime or its media and political construction [2].

The integration of a criminal organisation into society and its culture is an important factor. This makes it much easier for local criminals from the middle and upper classes to win over social elites for their illegal

[5] Translated by the author from German
[6] Translated by the author from German
[7] Translated by the author from German
[8] Translated by the author from German
[9] According to Bourdieu [6].
[10] Translated by the author from German

activities than it is possible for minorities. Their radius of action is limited from the outset due to cultural and social barriers. "High-quality" corruption therefore plays no or only a subordinate role in most OC procedures, since "the degree of danger to society increases with the degree of social integration" [3][11] (see also Arlacchi [8], who in this context speaks of "double integration").

Organised crime is not a parallel society, the upper and lower worlds are closely intertwined. Criminal networks involve "respectable" businessmen, politicians and lawyers as well as people who appear primarily through illegal activities. The last link in the chain are the customers, millions of people, who use goods and services of organised crime. The popular term "parallel society" only distracts from the fact that many people ultimately benefit from the activities of organised crime (prostitution, cigarette smuggling, product piracy, etc.).

"In the field of organised crime, there are no personalized victims at all. The drug smuggling across the border. Who is affected in person. Who could press charges? No one. The arms trade, the illegal smuggling. There are no personified injured parties. No one could come and say 'something bad happened to me'. In subsidy fraud, in a lot of other things. It is the anonymity of the community that is affected. But that will be caught."[12]

(Excerpt from a qualitative interview conducted by the author with an official of a department responsible for combating organised crime)

What has been said implies that organised crime cannot be interested in the abolition of prohibitions, because regulations are the way to create the enormous profit margins that organised crime generates in its business fields. The "freeloader" always has a genuine self-interest in the welfare of the "host" [9]. An existential threat to the state and society consists above all in the fact that the boundaries between the upper and lower worlds are becoming increasingly blurred, but not in the open confrontation between the state and organised crime, from which organised crime has always emerged as a loser in the past (the fate of Pablo Escobar impressively proves this). Organised crime is always most dangerous when you hear little about it.

In summary, none of the common definitions of organised crime can be convincing. Illegal markets are characterised by a variety of different forms of organisation, which Besozzi describes as follows. While mafia-like groups can still rely on subcultural legitimacy today, he understands *connections* and *networks* to mean more or less fixed, more or less permanent groups between offenders who act in a project-oriented manner in regionally limited milieus. The *gangs must be* distinguished from this, in which the focus is less on criminal acts and more on social ties, while the division of labour is a priority for *teams*, *mobs* and *crews*. *Scenes* are places "where like-minded people meet undercover or openly"[10][13]. In turn, (legal and illegal) companies distinguish themselves from this. Illegal companies are primarily oriented towards criminal activities (which does not exclude the possibility that they also conduct legal business), while legal companies "*use only partly illegal means (corruption in the award of contracts, circumvention*

[11] Translated by the author from German
[12] Translated by the author from German
[13] Translated by the author from German

of economic regulations, smuggling, etc.) to achieve their objectives, finance illegal business or contribute to the laundering of illegally acquired profits"[10][14].

In order to be able to forecast, data is needed. However, police data reflects less the criminal reality - it is more a reflection of the police construction of crime. In the area of organised crime, the dominance of blue-collar crime is striking, while white collar crime is still clearly underrepresented. Furthermore, the influence that social changes can have on criminal structures is often underestimated. As diverse the structures and business areas of organised crime are, so stereotypical is our thinking about the role of women in this type of crime. For many investigators, organised crime is still a purely male domain. However, there are many indications that a paradigm shift is also taking place within the structure of criminal organisations. Female members of mafia families seem to limit themselves less and less to the role of wife and mother, but rather to discover the law of action for themselves [11][12]. Raith attributes this, among other things, to the growing repressive pressure by the security authorities, which has pushed more and more *mafiosi* into the underground. The times of "locking away" had also become considerably longer, with the result that the "family" bosses had rethought the traditional strategies. There are indications, for example, that during the "absence" of their husbands, wives take over the business in a "fiduciary" manner, quasi taking over management tasks. Kreisky notes that, unlike *Cosa Nostra,* the structures of the mafiosos organisations of *Camorra* and `Ndrangheta are more open to women. Since the latter two organisations are organised less hierarchically and the position of the individual within the organisation depends to a large extent on the individual's assertiveness or charisma, women could advance far up the hierarchy. This also has to do with the social position of women in Neapolitan society: "*In this region of Italy, women assume numerous positions of power in the public sphere and do not remain limited to the radius of action of the domestic sphere*" [13][15].

These examples illustrate that women in organised crime can not only be reduced to the victim role or the passive role of mother and wife, but that their field of activity within criminal organisations also goes beyond the typical manual labour. This is how Max Mermelstein [14], former drug dealer and chief witness of the US authorities, describes the story of Griselda Blanco de Trujillo in his book *The Man with the Snow,* an extremely violent woman who was called the "Ma Barker" of Medellin's cocaine trade and who was decisively responsible for the cocaine wars in Miami at the end of the seventies. In their study of large-scale dealers and smugglers in California, Adler and Adler [15] also found evidence that women were also involved in cocaine trafficking at higher levels. However, while the actors at this stage of drug distribution were predominantly white middle class members who had "previously hardly been involved in criminal activities" [15][16], the crack dealers in East Harlem, who Bourgeois [16] observed in his field studies, belonged predominantly to the black underclass. Here a "gender dynamic" comes into play to the extent that the "culture of the street" forbids men to "publicly subordinate themselves to the opposite sex" [16][17].

[14] Translated by the author from German
[15] Translated by the author from German
[16] Translated by the author from German
[17] Translated by the author from German

At this point, the role of the mother in mafia-like structures will be discussed once again. It is often forgotten that it is the mothers who pass on the mafia ethics to their children in the course of the socialisation process [13]. In this context the question arises how high is the probability that children who grow up in criminal subcultures have a chance to not become criminals? The sociologist Richard Berk has developed a computer program that calculates, even before a child is born, how high its probability is that it will later become a criminal - the database is based on various risk factors, including the legal behaviour of the social environment in the past. But what is the benefit of such "knowledge"? Can people be locked up just because an algorithm says that there is a high probability that they will commit a crime at some point in the future? [17]

In summary, it can be said that organised crime is such a complex phenomenon that no definition has been able to establish itself either in science or in police practice. In addition, society in general and organised crime in particular are subject to constant change. This is especially important with a view to medium- and long-term forecasts – and must always be kept in mind.

2.2 Extremism/Terrorism

Terror as a tactical tool is ideologically neutral and its nature therefore can be secular and religious, ethnic and national. Terror can originate from criminal and political groups, both individual and collective. Terror with a purely criminal background can be used, for example, to protect illegal markets or to extort protection money [18]. Already the saying “One freedom fighter is another terrorist” refers to the difficulty of a uniform definition. There have been countless examples in the past of how people who were a thorn in the side of the powerful were arbitrarily called terrorists to silence them politically. This indicates the theoretical link to the labelling approach.

"Terror is not the same as terror. We can't generalize it. There are many different forms of terror. It has many different causes and strategies, and just as diverse are the methods of combating terrorism and the qualifications of the people who carry them out."
(Ephraim Halevy, Head of the Israeli Secret Service MOSSAD 1998-2001 [19])

The quote from Ephraim Halevy makes it clear that it might be difficult to ever formulate a generally accepted definition that encompasses all facets.

"Terrorists resemble a fly trying to destroy a porcelain store."[20][18] This saying by Yuval Noah Harari sums up the problem of modern counterterrorism. Whoever uses the method of the terrorist is usually the "weaker part". The devastating effects of terrorist attacks often do not consist in the act of terrorism as such, but in the reactions of those affected.

"If the angry enemy uses its massive power against them, it will create a much more violent military and political storm than the terrorists themselves ever could. During every storm many unforeseen things happen. Mistakes are made, atrocities are committed, public opinion fluctuates, neutrals change their attitudes, and the balance of power shifts [...] In these ruins the Islamists now thrive magnificently. And

[18] Translated by the author from German

there is no shortage of easily irritable bulls in this world" [20][19].

First of all, "terror" is a method and means the spreading of fear and terror by means of physical and psychological violence. Terrorism is not primarily about material damage, not even about the number of victims. It's about symbolic power and arbitrariness. Anyone can be affected at any time. It is about luring the opponent into the trap, forcing him to overreact so that he throws his own principles overboard and becomes morally vulnerable.

"The first mistake of the attack on Afghanistan was still excusable. The second mistake, the Iraq war, was inexcusable. And the third mistake, leaving the legal framework, is perhaps understandable, but fatal. This war - the term is actually wrong - this fight between the western world and the jihadists is not a war between the good and the bad. It is a war between different values and cultures. If the Western countries act in such a way in this war that they disregard their own values, their culture, then they make themselves extremely vulnerable. Because the opponents could very quickly use this against them and say: 'You don't believe in your values yourself'"[20].

(Pierre Brochand, Director General of the French Secret Services DGSE 2002-2008) [19])

In state terror, political regimes resort to the method of "terror" in order to support their generally totalitarian system (Nazi dictatorship). In these cases, the state apparatus can practice terror itself or tolerate it [21]. Hess describes the former as *repressive terrorism of state apparatuses*, the latter as *repressive terrorism of para-state and non-state groups*. This example shows that terror can have not only a destabilising, but - in a negative sense - also a stabilising function. Governments can also wage proxy wars by financing terrorist groups.

The method of state terror is not only used by autocracies and dictatorships, but occasionally also by democracies. Famous examples are the Black Sites of the USA, the Guantanamo prison camp or the torture scandal in Abu Graib. Democratic states have not only the right, but also the duty to protect their citizens against terrorist attacks; but exclusively with the means of the rule of law and on the basis of humanistic and democratic values.

Unlike state terror, revolting terrorism [21] by non-state groups and organisations attacks an existing system in order to change social conditions or to overthrow the system. But the more established a social order is, the more difficult it will be for terrorists to find acceptance for their demands among the general public. Only when a social order is regarded by many citizens as not legitimate, systems can start to falter. Revolting terrorism also calls into question the claim to power of political and economic elites.

If “terror” is a method, then extremism is an attitude. Political extremism is characterised by “lack of plurality”, “ideological dogmatism”, “friend-enemy stereotypes” and “mission consciousness”. But what is the difference between extremists and terrorists? Terrorism expert Hoffman [22] cites the “violence” factor as an outstanding differentiation criterion: the acceptance of radical positions alone, even

[19] Translated by the author from German
[20] Translated by the author from German

membership in forbidden political organisations, is not enough to describe an individual as a terrorist. Only when it uses violence to assert its political convictions it can be regarded as a terrorist. In this context, it should be critically noted that not every person who politically exaggerates their acts of violence necessarily has to be a terrorist. An extremist could be described as someone who carries his radical political convictions (sometimes violent) to *the outside world,* but who still acts *visibly* in contrast to the terrorist. An "autonomous" may wear a balaclava during a street battle with police officers, but in the end, he moves in the upper world. The terrorist, on the other hand, "disappears from the scene" and dives into the underworld; terrorists do not tend to present themselves to the security authorities at demonstrations.

In addition, there are individuals and groups who, although they hold radical positions, do not use illegal means to spread their political messages. They avoid open calls for violence and do not commit acts of violence themselves. They try to win new followers for their ideas and goals through missionary work.

Global terrorism is increasingly replacing national and international terrorism. This is not least a development in the course of globalisation, in which the nation states are increasingly losing political influence and social conflicts are being communicated worldwide. For the security authorities this means a rethink. In the context of national terrorism, both the perpetrators and the victims are nationals of the same state, so the conflict is conducted domestically. Forms of international terrorism must be distinguished from this. In the case of international terrorism, attacks are carried out outside the reference country and thus the damage suffered by foreign citizens is deliberately accepted. "*The aim is to attract the attention of the world public and to put particular concerns on the international agenda*" [23][21].

Global terrorism does not focus on a single sovereign state, but on a specific cultural value system. This circumstance has made it considerably more difficult for the respective national security authorities to combat terrorism. The perpetrators are both indigenous people and people with a migration background, "home-grown-terrorists" as well as "flown-in-terrorists". Citizens of the affected nations can become victims of terrorist attacks not only at home, but also many thousands of kilometres away at their holiday resort. The number of (potential) perpetrators has thus increased many times over, as has the number of possible targets.

The "world is a village", and in this "village" terrorists can operate largely unhindered thanks to state-of-the-art communication technology, worldwide migration flows and the liberalisation of border traffic. The groups are usually small and only loosely networked with other cells. This new type of terrorist is as ephemeral as modernity itself.

Global terrorism not only operates worldwide, it also recruits across national borders. It finds its followers both in the ghettos of Cairo and in the ethnically segregated districts of major German cities. Ethnicity, skin colour, language and social class are not obstacles, the connecting element is hatred of the common enemy. Chats and social media accelerate this development enormously. In the modern world, physical contact with comrades-in-arms is obsolete. Radicalisation processes, indoctrination and the

[21] Translated by the author from German

accompaniment in the phase of preparation of a terrorist act are nowadays in many cases carried out via the World Wide Web. This makes it so difficult for the security authorities to find the needle in the haystack in the flood of communication.

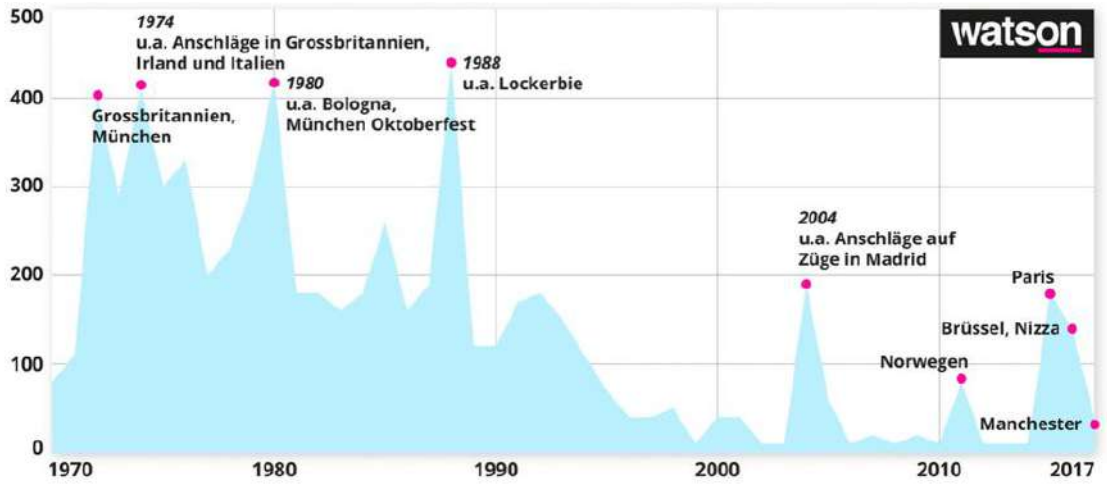

Figure 1: Victims of terrorist attacks in Western Europe [24]

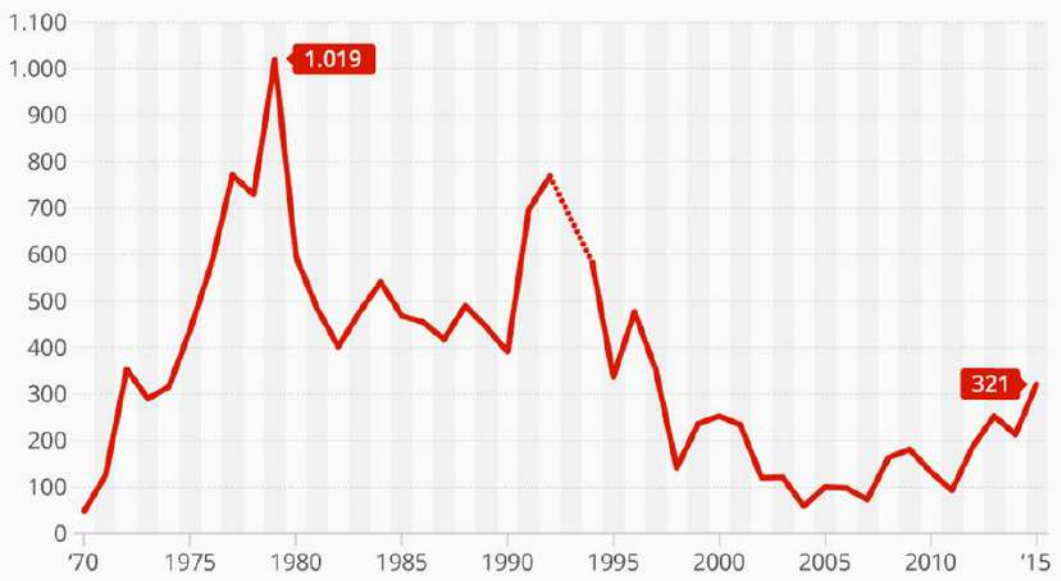

Figure 2: Terrorist attacks in Western Europe per Year [25]

Some basic aspects of the terrorist threat will be now addressed. As it can be seen in Figure 1 and Figure 2, the number of terrorist attacks in Europe and the European Union is "manageable" - also in terms of the number of fatalities. This means that even if each victim is too much, the number of terrorist attacks and victims of terrorist attacks is rather small, and yet there is a great subjective fear of terrorist attacks in society. By far the largest proportion of terrorist attacks perpetrated worldwide concern emerging

markets or developing countries such as Iraq, Afghanistan or Syria. There are (civil) war-like conditions there, caused to a not inconsiderable extent by the military actions of recent years. One can certainly argue that the current strategy in the fight against international terrorism has not defused the problem, but on the contrary has aggravated it. Because terrorism is a form of asymmetrical warfare; terrorism cannot and must not be fought with military means, because ultimately the military always emerges as the loser from such a conflict. In addition, phrases such as "the war on terror" enhance terrorist groups because such language usage suggests that one is dealing with equal enemies.

"War means increasing the political importance of the organizations that threaten us. How do they treat like a serious opponent, something they're not really?" [22]

(Sir Richard Dearfore, Head of British Intelligence MI6 1999-2004) [19]

In Europe, terrorist attacks are rare events, and therefore not predictable due to their low base rate. It seems much more sensible to develop a set of instruments to retrospectively analyse security policy misconduct and its consequences, to be able to make predictive statements about the terrorist threat in the future and to not repeat strategic mistakes of the past.

The probability of becoming a victim of a terrorist attack is minimal. The already low probability has further decreased in recent years as the number of terrorist attacks has decreased. The power of terror lies in the art of "triggering availability cascades". Horrible images of terrorist attacks are omnipresent, media coverage distorts our perception of this phenomenon and thus prevents a rational handling of the subject [26].

With a view to international and global terrorism, the question arises of the agreement of measures to protect internal and external security [2]. By "state-induced security threats and risks" Zangl and Zürn understand interstate wars and state terror, while terrorist acts and crimes fall under "social (non-state) sources of insecurity" [27]. Zangl and Zürn define security as "the desired state of continuation of the physical existence and integrity of a social actor"[23] and distinguish six types of insecurity in the following:

"On the one hand, there are threats by which we want to describe the uncertainties deliberately caused by identifiable social actors (...) On the other hand, dangers exist independently of decisions by social actors (...) Finally, risks should be mentioned which are characterised by the fact that, although they are the result of decisions taken by social actors - i.e. they are not naturally present as dangers, but are socially caused - these decisions - in contrast to the threat - were not taken with the aim of damage (...) Both threats and dangers and risks can affect the physical existence of social actors both insidiously and abruptly") [27].[24]

The original task of the state is to fulfil its security function in such a way that it guarantees external and internal security, which primarily refers to the reduction of socially caused insecurities. Zangl and Zürn give concrete form to the security functions of the state as follows [27] (also see Table 1):

[22] Translated by the author from German
[23] Translated by the author from German
[24] Translated by the author from German

1. the defensive function,
2. the rule of law function,
3. the function of domination and
4. the protective function.

With regard to terrorism, the protective function is particularly relevant, i.e. "the protection of individuals against the risk of harm from the actions of other social actors" [27][25]. The individual nation state is no longer in a position to deal adequately with the dangers that global terrorism poses to its citizens. This requires coalitions that make compromises unavoidable. As the example of Afghanistan shows, the various security functions can then compete with each other. Measures taken by the state to ensure its external security (fight against terrorism - defence function) can at the same time jeopardise internal security (toleration of drug trafficking and thus promotion of organised or drug-related crime).

Table 1: The security functions of the state [27]

	State is affected	Society is affected
Threats and risks emanate from the state	Interstate war *(defensive function)*	State terror; disrespect human rights *(rule of law function)*
Threats and risks come from society	Terrorism; Civil War *(ruling function)*	(Violent) Crime, environmental destruction *(protective function)*

The fight against terrorism inevitably leads to conflicts of interest between the protective function and the rule of law. For example, with the adoption of the Counter-Terrorism Act in 2002, the competences of the Office for the Protection of the Constitution and the Federal Intelligence Service were considerably extended [28]. The aforementioned institutions now have "the authority to obtain information from banks, postal service providers, aviation and telecommunications companies on sensitive personal data (e.g. account movements, travel routes, etc.)" [28][26]. According to Kutscha, this has given the secret services an almost "police-like investigative competence", which is diametrically opposed to the original intention of the separation order. The extension of police powers to operate by "intelligence means" would also lead to a situation in which the separation requirement would dwindle to a "purely organisational shell" [28][27].

Pelzer and Scheerer [29] comment on the rule of law of prognostic instruments[28] in the field of terrorism to the effect that far-reaching interventions in the fundamental rights of the individual should only be

[25] Translated by the author from German
[26] Translated by the author from German
[27] Translated by the author from German
[28] The term “rule of law of prognostic instruments” refers to the requirement to bring prognostic instruments into line with the regulatory framework of a state.

carried out on the basis of very specific prognoses and that a case-by-case examination should be carried out relatively early on. In the area of terrorism, the fundamental issue was the balancing of the requirement to do justice to a person as a legal subject and successful danger prevention and prosecution.

2.3 Cyber Crime

The use of the Internet has become an integral part of the everyday lives of millions of people. The diverse offer on the Internet, with which the user is able to satisfy different needs [30], can be used almost always and everywhere via mobile devices. This development is also of great relevance from a criminological point of view. The Internet offers a suitable platform for carrying out various criminal activities. [31] According to the definition of the German Federal Criminal Police Office, the term "cybercrime" refers to offences "committed against the Internet, data networks, information technology systems or their data [...] or by means of this information technology" [32][29].

Cybercrime can be realized in different ways. According to the German Federal Criminal Police Office, currently, the common forms of cybercrime are those that include computer systems infected and manipulated with malware for the purpose of tapping personal data, extortion of "ransom" or remote control and use for further criminal activities [32]. Other manifestations include sex and violence (e.g. child pornography, bomb-making instructions, decapitation scenes, etc.), fraud and scamming [31].

The relevance of this phenomenon is also made clear by the German Federal Criminal Police Office on the basis of the results of a study by the digital association BITKOM. Accordingly, every second German Internet user has already become a victim of cybercrime in the period of the year preceding the investigation [32].

The spread of digital information and communication networks not only opens up new illegal markets for organised crime, but technological innovations also enable criminal groups to better coordinate and seal off their illegal activities. Through the accumulation of large amounts of capital, criminal groups are often able to make use of technological innovations, which is not possible for the police in this way. Also, thanks to modern information and communication technologies, people can now participate in criminal activities for whom the risk of detection was previously too great. In this context, the illegal export of capital should be mentioned. Many citizens now take advantage of the opportunity to transfer untaxed money abroad. Very few of them are likely to have a sense of injustice, not to mention the fact that they hardly consider themselves part of criminal networks.

In addition, technological developments have led to the de-personalisation of the criminal act, which has advanced new strategies for legitimising criminal behaviour and guilt is no longer felt. Virtual markets open up the possibility for citizens to use criminal services anonymously and without risk. Furthermore, legal regulations are often missing. As a result, lawless areas are created with all the problems that this entails.

[29] Translated by the author from German

3. Prediction/ Forecasting Methods

The term prognosis comes from the Greek and means prediction. The term "*forecast*" refers to future developments or events. Compared to irrational predictions, forecasts can be rationally justified and verified. A basic distinction is made between growth forecasts that predict the "value of a time series at a future point in time" [33][30] and forecasts that involve a qualitative change or development.

Table 2: Explanation and Prognosis [34][31]

	law	boundary condition	Explanandum
explanation	sought	sought	given
prognosis	given	given	sought

The difference between an explanation and a prognosis is that in an explanation the event (the Explanandum) has already occurred (see Table 2). The scientist's task is to find out the laws and framework conditions that led to the Explanandum. With a forecast it is different: the laws and the boundary conditions are known and on the basis of this knowledge the forecast is made.

Forecasts can relate to different time periods. Hess distinguishes between short-term forecasts, medium-term orientations and long-term prophecies, short-term forecasts and medium-term orientations make use, according to Hess, of n "if-then hypothesis", whereby the precision of the forecast inevitably decreases with the length of the forecast time frame. Hess criticises long-term prophecies as "historicism" in reference to Popper and denies their scientific nature [21].

It should be noted in this context that, in contrast to scientific systems, social systems are generally characterised by a much lower degree of stability. In addition, both the forecaster and the forecast object can consciously or unconsciously influence the (non-)arrival of a forecast. This is particularly relevant in the area of crime. If a hazard is predicted, the safety authorities react preventively so that the prognosis is not true (***self-destroying prophecy***). In the opposite case, efforts can be made to design the forecast in the sense of the forecaster (***self-fulfilling prophecy***).

Pelzer and Scherer point to further problems [29]: Social science prognoses, carried out for the security authorities, served to combat and prevent crime, which, however, limits the research scope of the scientist. This should first and foremost "contribute to the containment or elimination of the corresponding risks, disruptions and threats […] to perform"[32]. Only in second place is its interest in knowledge, although - strictly speaking - the quality of the prognosis ultimately depends on the robustness of the legal statements, which ultimately requires well-founded research.

[30] Translated by the author from German
[31] Translated by author from German
[32] Translated by the author from German

Furthermore, personnel and material resources could be acquired by the security authorities with dramatic forecasts. Thus, it could not be ruled out that interested parties might influence the preparation of the forecast. On the other hand, an oversubscription of the danger has the advantage for the forecaster that the sanctions in the event of non-impact would probably not be as negative as if he had erroneously underestimated the danger "

"Firstly, one can always claim that the result was prevented precisely because of the warning, but that the prognosis was basically correct, but fortunately had an al self-destroying-prophecy effect through its pre-warning effect, and secondly, too much politically desired dramatization and stigmatization is sanctioned less than too little. Therefore, error predictions in the form of 'Doomsday' predictions are more frequent than error predictions of a trivializing kind" [29][33.]

Forecasting is a method that is also becoming increasingly important in the social sciences. The reasons for this are the ever-increasing amount of information available, the rapidly developing technical possibilities for processing large amounts of data (BIG DATA), but also the increasingly complex social relationships.

3.1 Criminal Prognosis

According to Schwind, the term "crime prognosis" means "(well-founded) probability statements about the (total) *future* development of crime (or about the development of individual forms of crime) in the total population (or in parts of the population)" [31][34]. This is how particularly Schwind defines a collective prognosis. In contrast, individual prognosis aims at predicting the future delinquency of a single person. With the help of crime forecasts, it will be possible to counteract the future development of crime at an early stage, as measures can be planned in good time [31].

Three different methodological approaches to criminal prognoses can be distinguished: the intuitive prognosis, the statistical-nomothetical prognosis and the clinical-idiographic prognosis. The three forecast types are presented below.

3.2 Intuitive Method

The intuitive method is about the emotional assessment of an individual. Personal and professional experience play a role here. The term "feeling" is often used in this context. We usually associate "feeling" with "intuition", i.e. something that is difficult to grasp objectively (the so-called "good feeling").

The intuitive method is closely linked to the expert system. If we dare to look into the future, we like to rely on the knowledge of experts. For many people it is inconceivable that a machine or algorithm can deliver higher quality analyses and forecasts than experienced people who have been dealing with a phenomenon area for years. Nevertheless, numerous studies prove the superiority of algorithms. The psychologist and Nobel Prize winner Daniel Kahneman comments as follows:

"The number of studies comparing clinical and statistical predictions has increased to about 200, but the

[33] Translated by the author from German
[34] Translated by the author from German

state of competition between algorithms and humans has not changed. In about 60 percent of the studies, the algorithms proved to be much more accurate. The other comparisons resulted in a draw, but a draw is tantamount to a victory for the statistical rules, which are generally much less expensive than expert judgment. No exception has been credibly documented."[26][35]

The reluctance to make decisions about algorithms has to do not least with the fact that we give too much weight to the statements of experts. In this context, Kahneman refers to a study by his colleague Tetlok that exposes the "competence illusion" of experts:

"Tetlok interviewed 284 people who earn their living as 'commentators or advisors on political and economic trends. He asked them to assess the probabilities that certain events would occur in the not too distant future, both in regions of the world they had specialized in and in regions they knew less about. Would Gorbachev be overthrown by a coup? Would the United States go to war in the Persian Gulf? Which country would become the next big emerging market? In total, Tetlock collected over 80,000 predictions. He also asked the experts how they arrived at their conclusions, how they reacted when refuted, and how they assessed information that did not substantiate their position. Respondents should in any case assess the probabilities of three alternative events: the persistence of the status quo, more of a thing like political freedom or economic growth, or less of it.

The results were devastating. The experts showed a worse performance than if they had simply rated all three results with the same probability. In other words, people who spend their time - and make a living - thoroughly studying a particular subject make worse predictions than dart throwing monkeys who would have distributed their "decisions" evenly across all options. Even in the field they knew best, experts were no better than non-experts" [26][36]*.*

The above refers to the problems of forecasting processes in which experts play a major role (e.g. scenario technique), as they often misjudge the development of factors. To make matters worse, "those with the most knowledge […] are often less reliable". This is because someone who acquires more knowledge develops an increased illusion of his abilities and overestimates them in an unrealistic way [26] [37].

3.3 The Statistical-Nomothetical Prognosis

The statistical-nomothetical prognosis is a rule-guided procedure for the compilation of individual criminal prognoses using predefined algorithms. The basic objective of this method is the identification and systematic compilation of personal and factual characteristics that are empirically significantly related to recidivism [35].

With the statistical-nomothetical prognosis, a deductive conclusion is drawn from empirically proven average correlations, which are determined within the framework of large-scale relapse studies, to the individual case [36]. Various forecasting instruments are used, such as forecast tables, in which individual characteristics are taken into account unweighted, or structural forecast tables, which also include

[35] Translated by the author from German
[36] Translated by the author from German
[37] Translated by the author from German

interrelationships between the individual characteristics. Using algorithms or the summation of risk and protection factors the risk analysis is carried out [37] in which the adjustment to the individual case is carried out exclusively by allocation to a standardized risk group [37][35].

The statistical-nomothetical prognosis includes relapse predictors whose predictive quality is empirically proven, which is why an objective assessment of the case is possible with this type of prognosis method [37]. However, since they are based on group statistical average experiences, individual and case-specific peculiarities cannot be taken into account [38].

3.4 The Clinical Idiographic Prognosis

The clinical-idiographic prognosis strategy is geared to the individual case and serves to assess the individual personality of the perpetrator and to clarify the content of individual contexts [38]. This is based on rules and standards, although the exact procedure does not follow precisely defined rules but can always be adapted to the individual case [37].

In the first step of the clinical idiographic prognosis, the relevant condition factors of the delinquency of an individual as well as their backgrounds and framework conditions are identified, from which an individual theory of action (previous delinquency of the considered individual) can be derived [37][35]. The second step is to examine the changes in these factors since the last act in order to identify any personality changes or therapeutic effects. This step is of particular importance if the person under consideration has spent the time after the last offence in prison, since the question then arises as to the therapeutic responsiveness of the risk potentials of this person. Personal factors that are stable over time are particularly relevant here, since they determine a person's individual risk potential [35]. At the analyst's discretion, the factors are weighted and integrated into the forecast, which is to be understood as an estimate of the future risk potential for relapses of the individual under consideration [37].

3.5 Methodology of Criminal Forecasting

Crime prognoses are to be implemented with different methodical procedures. These include, for example, the simple extension of time series into the future or qualified approaches that can be used to make statements on the future development of crime, taking into account demographic developments and social influencing factors that may favour criminal development [31]. In addition, expert surveys, such as the Delphi method and the scenario approach, should also be mentioned [31]. Within the framework of the Delphi method, experts independently give their opinions on various issues [39]. Instead of considering individual expert opinions on future developments in isolation, the Delphi method will be used to achieve more accurate forecasts via structured group processes [40]. In concrete terms, the first step is to conduct an expert survey, for example on the probability of an event occurring. In a second step, the responses are aggregated and returned to the respondents, giving them the opportunity to revise their responses based on the feedback received. This iterative process is continued to a defined endpoint, which may refer to the number of iterations, a consensus reached or a confirmed dissent, for example [40]. The basic idea of the scenario approach is to develop a scenario that is to be understood as a picture of the future, taking into account quantitative and qualitative influencing factors. The aim is to record and illustrate all possible courses of action, alternatives and their probable consequences [41]. As a rule, three scenario types are developed. These include an exploratory scenario in which current developments are

also assumed for the future and two contrast scenarios corresponding to the best case and worst case [41].

At this point, the creation of trend models will be discussed in more detail. With the help of a time series analysis as a form of regression analysis, one of the aims is to predict the future values of a time series in order to be able to make statements about future developments on the basis of this data. The continuation of temporally collected data series, which can relate to a wide variety of application areas, enables forecasts to be made. In the context of time series analyses, data series are used which consist of interdependent observation values, as these are obtained in chronological order [42].

Time series analysis can also be a suitable method for forecasting crime. In this case, the data basis represents the offence quantity per day, per month, per quarter or per year over a certain period in a limited geographical area. On the basis of this data it will be possible to make predictions about future crime incidence and thus future crime development for this geographical area.

At first glance, the prediction of terrorist attacks by means of time series analyses seems problematic, in particular due to the low data basis. In addition, the occurrence of terrorist attacks appears to follow neither trends nor seasonal fluctuations. For this reason, the quality of a time series analysis for predicting terrorism must be subjected to empirical verification.

4. Criminological Theories

Some basic sociological and psychological theories investigate in different ways causes and manifestations of crime or investigate themselves with the prevention, investigation and fight against crime. The reference sciences of criminology include law, sociology, pedagogy, ethnology, anthropology and economics. Also, geography plays an increasingly important role in criminology, as shown by "predictive policing", which has gained importance in criminology in recent years.

First, in this chapter psychological, sociological and criminological theories that play a prominent role in predictive policing will be examined in general terms. Afterwards it will be discussed which concrete factors and indicators can be derived from theories and further empirical research and how they can be used to meet the requirements of the LEAS formulated in the specific use cases (especially use case 2).

4.1 Criminological Theories in the context of Predictive Policing

In the following chapters, the theories that play a prominent role in predictive policing will be examined in more detail.

4.1.1 Rational Choice Theory

Systematically acting perpetrators act according to a cost-benefit principle. They weigh up whether they can successfully carry out an act without having to fear criminal consequences for themselves. The Rational Choice Theory is thus quite capable of explaining certain forms of crime. In principle, the approach is based on the consideration that not only standard-compliant behaviour of a cost-benefit analysis but also deviant and criminal actions are determined by cost-benefit considerations [43].

The problem is that, for example, criminal offences committed out of affect cannot be explained using the rational choice approach. Another criticism is that hardly any individual has all the relevant information at his or her disposal to carry out an objective cost-benefit analysis. In addition, it should be noted that framing effects can significantly influence perception and decision-making processes [26].

The advantages and disadvantages of action do not necessarily have to be of a material nature. The desire for social status within a criminal subculture, which can be achieved by committing crimes, can be a motivation for criminal behaviour. This applies to mafia groups as well as rockers and violent football fans.

The social objective must therefore be to increase the cost of crime and minimise its usefulness in order to prevent it from being committed. Formal and informal sanctions serve this purpose, i.e. by punishing socially undesirable behaviour and rewarding socially desirable behaviour.

What is the value of Rational Choice Theory for predictive policing? The aim is to identify the benefits and costs of specific criminal activities. By identifying characteristics which are conducive to an offence and thus recognising exemplary behaviour, it is not only possible to forecast future offence behaviour, but also to prevent it by means of appropriate police measures. Even an increase in the penalty level for gang burglary can induce perpetrators to relocate their operating room.

4.1.2 Learning Theories

Learning theories assume that deviant and criminal actions are learned through interactions. Lamnek explains that in the context of the learning process "*not only the actual behaviour patterns are learned, but also the attitudes, motives and rationalisations which make this possible or produce it in the first place*" [44][38].

In the sense of learning theory approaches, every member of a society or a group has the opportunity to orientate himself towards conforming or deviating behaviours, to identify with conforming or deviating persons or to experience an intensification of conforming or deviating behaviours through reactions [44]. Individuals identify themselves in different ways with conform or deviant or criminal behaviour patterns and learn these through interaction with other members of society or groups. Deviating and criminal behaviour occurs when in situations the learned deviant behaviour patterns outweigh the conformal behaviour patterns [44] and individuals identify more strongly with the deviant behaviour patterns within a society or a group [44].

The theory of differential association according to Sutherland represents one of the most important approaches to learning theory [45]. Sutherland's central argument, according to Lamnek, is that "*a person becomes delinquent when violations of the law outweigh favourable attitudes towards attitudes that negatively evaluate violations of the law*" [44][39]. Overall, Sutherland assumes that criminal behaviour is learned through interaction, especially in intimate groups, and thus cannot be inherited. The learning of techniques for the execution of a crime takes place in the context of such a learning process in the same way as the internalization of motives and attitudes [44][31]. In addition to contact with criminal milieus, the opportunity to carry out deviant and criminal acts also plays an important role, as does the intensity of the needs of the (potential) perpetrator and the lack of legal alternatives [44][46].

With the help of the theory of differential amplification according to Burgess and Akers [47] the statements of Sutherland were concretised. The authors argue that the frequency of certain behaviour is influenced by amplifiers. A positive influence in this context is, for example, attributed to praise or money [44]. With regard to deviant or criminal behaviour, an uncovered execution or prey can act as a positive booster.

4.1.3 Routine Activity Approach

The Routine Activity Theory goes back to Cohen and Felson [48]. The intention of formulating this theory was, in particular, to explain how social change processes change the opportunities for criminal action and thus cause fluctuations in the crime rate. Thus, this concept, whose line of argument lies at the macro level, assumes that crime depends significantly on opportunities [49]. Within the framework of Routine Activity Theory, Cohen and Felson examined the spatial and temporal conditions under which victims and perpetrators come into contact and thus a criminal act occurs, with special consideration of everyday routine activities. Routine activities in this context are, for example, employment and leisure activities.

[38] Translated by the author from German
[39] Translated by the author from German

According to Cohen and Felson, the following central factors must be present for a criminal act to occur:

1. A motivated perpetrator,
2. a suitable victim or object of crime or opportunity, and
3. the absence of a protector. [48]

A motivated perpetrator is important for the occurrence of crime in the sense that, normally, he lacks legitimate alternatives to the criminal act, so that he decides to exercise it. The attractiveness of a potential victim or object of crime is also decisive for the occurrence of crime [50]. With regard to the victimization risk of objects, Felson and Clarke formulated four risks that increase it [51]: Value, Inertia, Visibility and Access (VIVA). The value of a property determines its attractiveness for the potential perpetrator. Smaller and lighter objects (inertia) as well as clearly visible objects (visibility) are also more attractive. In this context, the possibility of access to the object ultimately plays a decisive role (access) [50][52]. It can be assumed that potential perpetrators are often looking for opportunities in their immediate environment [49]. Siegel noted, for example, that criminals usually pursue crime opportunities on their everyday journeys, for example between work and home.

The presence of a suitable protector in the form of persons or technical aids can prevent the occurrence of a criminal act.

A motivated perpetrator, a suitable victim and the absence of a protector make the occurrence of crime likely, which also increases the risk of victimisation. If only one of these conditions is not met, the offence may not be committed [50].

The validity of this theory has already been proven by numerous studies. Cohen and Felson extended their theory to the effect that they identified, for example, women's increasing employment and the existence of single households as factors that had a positive effect on the rise in crime rates. This is because households are more often unattended for longer periods of the day [50].

4.1.4 The Ecological Approach

The relationship between space and delinquency has been the concern of criminologists for a very long time. The roots of criminal geography[40] can thus be traced back to the [1]8th century. Even the Frenchman Guerry and the Belgian Quetelet dealt with the spatial distribution of crime in a descriptive way, but without going into the causes of the unequal distribution of delinquency that they found. The French

[40] There are numerous definitions in the literature concerning the term "criminal geography". Herold understands this to mean "the science of the relationships that exist between the specific structure of a space and the crime that occurs in it locally and temporally". For Schwind, criminal geography is the "branch of criminological-criminalistic research which records criminal behavior in its spatial-temporal distribution and attempts to explain it by means of specific spatial-temporal patterns of distribution and linking of demographic, economic, social, psychological and cultural factors of influence, with the aim of (primarily) preventing crime" (translated by the author from German)[31].

sociologist Emile Durkheim also used criminal-geographical analyses in his famous work "The Suicide" [53].

The descriptive approach was also a feature of the early works of the Chicago School, whose subcultural studies had a decisive influence on American and international (criminological) sociology. Researchers such as Trasher [54] and Whyte [55] were mainly concerned with the question of how space favours socially deviant behaviour. In terms of methodology, the researchers primarily used qualitative methods, including participatory observation and open ethnographic interviews.

The zone model of Ernest W. Burgess, also a representative of the Chicago school, became famous [56][57]. Burgess stated that cities spread out in a circle around their centre, with the social status of the citizens increasing with distance from the core. He described the two outer zones as *community zone* and *residential zone*. While the community zone is mainly inhabited by middle-class people, the residential zone is mainly inhabited by very well-off commuters.

Hoyt, a Burgess student, modified the zone model and designed the so-called *sector* model [58]. On the basis of his studies of the rental structure in various metropolises in the USA, he came to the conclusion that cities are spreading along transport routes, with the higher-status population being the main driver of urban development. Furthermore, Hoyt explained that in rooms that are abandoned by higher status population groups, next lowest groups follow.

The *multicore model* was developed by Harris and Ullman [59]. Unlike Burgess and Hoyt, whose models were still based on one urban centre, Harris and Ullman emphasised that with the size of the cities the number of centres and cores also increases. These included, for example, shopping centres, cultural centres and parks.

Of the three classical models of urban development, the multi-core model is likely to come closest to the reality of life in modern (large) cities. Especially in the Ruhr area, where many - formerly independent - municipalities have been incorporated over the years, the multi-core model can better describe and explain the geographical distribution of crime than the zone and sector model. However, this does not mean that zone and sector models are obsolete per se. If cities grow organically (such as Chicago), one can very well assume that there is only one centre, but this does not apply equally to the development of every city.

Shaw and McKay founded the so-called ***ecological approach*** (***area approach***) on the foundations of the Chicago School of Sociology [60]. According to Lamnek,

"After that, the ecological situation of a residential area (lack of infrastructure, slums, etc.) determines the personality and behaviour of a criminal. Other regions act as attractive forces for the commission of crimes (e.g. centres with department stores, gambling rooms, railway stations, etc.). Ecological hypotheses of deviating behaviour are aimed at the spatial distribution of this behaviour - they are therefore statements about areas, i.e. aggregates" [61][41].

[41] Translated by the author from German

Residential areas and city districts are therefore characterised by different crime rates. The reasons for this can be both social and economic. For example, social disorganisation due to a lack of formal control can encourage criminal behaviour. Affected social spaces then threaten to develop into so-called ***delinquency areas.*** These are often residential areas characterised by an unfavourable social structure (high unemployment, lack of leisure opportunities for young people, high proportion of migrants, etc.). In criminology such spaces are also called **"*breeding areas*".** This term refers to the fact that an above-average number of people with a criminal background live there, i.e. the proportion of *offender residences* is high. The concentration of "multi-problem groups" makes their social integration more difficult and favours the development of criminal subcultures (*gang-lands*), whereby it must be noted in this context that it is less the architecture than the social structure that is the determining factor for deviant behaviour. For the representatives of the Chicago School, the focus was not so much on research as on fighting crime and improving people's lives. The "Chicago Area Project" was founded with the aim of preventing the causes of crime. The "Chicago Area Project" documents the interest of the responsible scientists in linking criminological findings with concrete criminal policy measures.

The Routine Activity Theory was further developed by Felson and Clarke [51] within the framework of the Crime Pattern approach and – as said before - deals with the question which spatial-ecological and temporal characteristics influence the delict-rates [50][51]. Based on the central assumptions of Routine Activity Theory, Crime Pattern Theory has identified factors that can be used to characterize crime patterns. These include nodes, paths and edges [50].

Nodes are places between which individuals move, for example, public transport points and their immediate surroundings, and, according to Felson and Clarke, an increased crime rate can be expected at these points. The link between the nodes and the daily paths of an individual provides information about the individual's risk of becoming a victim of a crime. For example, an increased risk of victimisation can be assumed on everyday routes between work and home, since individuals are targets for potential perpetrators on these everyday routes. This is a close link to the assumptions of the Routine Activity Theory. The risk of victimisation is particularly high in the edges between the place of residence and places of work and entertainment, as individuals are foreign in these areas and are very likely to meet strangers, and their areas of activity may therefore overlap with those of potential perpetrators [50].

Overall, it can be stated that in the light of Crime Pattern Theory it can be assumed that space and time influence the occurrence of crime and that the movement patterns of individuals play an important role in this context.

The Crime Pattern Theory has contributed significantly to changes in urban planning. Thus, for example, the alignment of windows to the street side for a better overview of the living environment has its starting point among other things in the central statement of this theory [50].

4.2 Criminological Theories in the context of the use cases (in Cooperation with KEMEA)

This chapter aims to elaborate theoretical aspects in relation to the use cases. Since a predictive benefit exists in particular with regard to use case 2 and thus radicalisation, the focus in the following is especially

on this topic. Here, it is aimed to present those theoretical aspects that can explain (individual) radicalisation processes and it should be clarified which concrete indicators can be derived from these theories and further empirical research for the detection of radicalisation and extremism. In this way, a corresponding understanding of radicalisation processes should be created among the end-users.

Radicalisation is a complex phenomenon of major concern not only in Europe but also in Middle East and North Africa [62]. Having not a universally accepted term along countries [63], radicalisation can be defined from an academic, operational, policy, political and sociological point of view, being given a violent or a non-violent, a political, a religious, an extremism, a behavioural and/or a revolutionary framework resulting to the rejection or undermining of the status quo or contemporary ideas and expressions of each society [64][65]. Radicalisation causes are usually sought on a micro-, meso- and macro- level, with the first to refer to the individual (e.g. identity problems, problematic integration, alienation and depression, marginalization, discrimination, humiliation, rejection and feelings of outrage and revenge), the second to social surroundings and groups dynamics (feelings of social injustice especially among young people) and the third to the broad societal and political environment both in home and abroad (lack of political, economic, cultural opportunities, tense etc.) [66]. Since 2004, the term 'radicalisation' has become central to terrorism studies [67], with the borderlines between these two concepts to be several times blurred and problematic. Several academics have proposed certain radicalization process which escalates and conceptualize the radicalization path towards terrorism [64].

According to Costanza's definitions, "The path of radicalization is the process or progression which enables to understand how an individual or a given group moves through time towards radical beliefs, in a volatile social environment which is constantly evolving" [68]. A great volume of radicalization studies from both academic and policing agencies have underlined the development of an indicators-based approach towards the prediction of the potential individuals could engage themselves in radicalized behaviors and violent acts [69]. More in particular, since 2008 [70] researchers merely focused on the way radicalisation occurred and not on the reasons why this happened.

There is ongoing social reflection on the causes, challenges, and prevention strategies of radical behaviour and there are various theories trying to interpret this phenomenon. A great volume of scientific disciplines such as criminology, anthropology, sociology, political science, legal studies etc.-, have been impactful to radicalization theories and models proposed to explain the radicalisation process. Three generic theoretical approaches have been utilised among scholars and practitioners to identify and explain radicalised behaviours; cognitive theories that try to identify the root causes from a cultural-pathological point of view, behavioural theories that direct their attention on identifying the activation of incentives inside social networks and narrative approaches that expand the search of indicators to a wider social and political context [69]. Social Movement Theory (SMT) has been one of the theoretical backgrounds that have been largely proposed to explain radicalisation processes [71]. According to Zald and McCarthy Social Movement Theory is "*a set of opinions and beliefs in a population, which represents preferences for changing some elements of the social structure and/or reward distribution of a society*."[72]. Its roots go

back to 1940 and they have been affected by the main premises of Strain Theory[42], discussing that radicalisation stemmed from irrational processes of collective behaviours that occurred under stained environments. Each individual could participate to a specific movement as they wanted to oppose to specific social oppressions. Moving forward, this theory evolved, incorporating a more rational approach especially from the aspect of the perpetrators, in terms of recruitment. They formed specific mobilization potentials, creating and motivating recruitment networks with social bonds and relationships among the participants, which tended to arouse motivational incentives for participation eradicating in parallel cognitive barriers. The two contemporary mutations of this theoretical school are "New Social Movement (NSM) Theory, which focuses more on macro/structural processes, Resource Mobilization (RM) Theory[43], which focuses more on contextual processes like group dynamics" [69] and Framing Theory (FM)[44], which focuses particularly on the "social production and dissemination of meaning and on how individuals come to conceptualize themselves as a collectivity" [75].

Moving to the field of social psychology[45], theories and empirical research of this field have outlined specific key lessons, summarised as such [75]:

- ✓ When different opinions and attitudes are conveyed from an individual point of view to a group context then they become more extreme and polarized
- ✓ Group decision making tends to be biased and irrational compared to individual one
- ✓ All the perceptions stemming from a group perspective tend to be biased towards existing group members and negative for the individuals outside the group
- ✓ There is the concept of shared and not individual responsibility among group members, thus participants feel less responsibility for any violent act
- ✓ Acceptance and other "rewarding" behaviours may be the incentive that lead people to join certain groups
- ✓ Groups have internal norms and rules that control member behaviour.

Based on some studies conducted by McCauley and Moskalenko [77][78], five mechanisms of group radicalisation related to socio-psychological factors have been identified, namely as:

1. Extremity Shift in Likeminded Groups—Group Polarization
2. Social Reality Power of Isolated Groups—The Multiplier

[42] Robert K. Merton, in his article back in 1938 "Social Structure and Anomie", he argues that anomie is not the result only of unregulated goals but from the state where a person is unable to attain his goals by socially acceptable means, thus turning to illegal and unacceptable activities. The gap between the cultural goals of a society and the structural means to achieve these, such as education, employment, social acceptance, has led to the formation of Merton's Strain Theory [73].

[43] Based on the DIIS Working paper no.2008/2, the unit of analysis under this theory includes social movements. meso-level organizations such as Schools, mosques, charities, and micro--level mobilization such as everyday social circles [74].

[44] Based on the DIIS Working paper no.2008/2, the unit of analysis under this theory includes Individual, group, society interaction -[74].

[45] Social psychology is the scientific study of how the thoughts, feelings, and behaviors of individuals are influenced by the actual, imagined, and implied presence of others [76].

3. Group Radicalization in Competition for the Same Base of Support— Outbidding
4. Activist Radicalization in Competition with State Power—Condensation
5. Group Radicalization from Within-Group Competition—Fissioning

Another theory, stemming also from sociology, psychology as well as religion is the Conversion Theory (CT), focusing more on the individual process of transforming beliefs and ideologies and proposing a seven-stages model (Context, Crisis, Encounter, Interaction Commitment and Consequences), where each component is interlinked and can affect the others [79]. Different approaches of the Conversion Theory focused not only to "psychopathological explanations for religion conversion and participation, assuming some combination of individual abnormality, deficiency, or trauma to be the primary causal factors", but also on "strain and deprivation as possible causes of religious seeking and conversion", underlining also the notion of self-radicalization among individuals [80].

Finally, Table 3, summarizes in brief all the relevant theories, derived form a large methodological study conducted in September 2010 by Crossett and Spitaletta for the John Hopkins University [81].

Table 3: Summary of relevant Theories applied to radicalisation process

General Theoretical Concept	Specific Theory	Relevance to Radicalization
Sociological Theories	**Relative Deprivation Theory:** Economic disparities cause violent political behaviour	- Applied to violent acts (political and other) in the developing world and lower socio-economic groups. - It requires a set of environmental conditions, a specific interpretation of those conditions, and a violent reaction to that interpretation to be present in causal linkage
	Social Network Theory: social relationships are viewed as individual actors (nodes) (relationships)are being tied between them	- The size and structure of a social network determines its usefulness to each individual - Closed and smaller networks are more useful to radical groups

		- Feelings of isolation and lack of social connection may lead to participation to radical (religious mostly) groups
Psychological Theories	**Social Movement Theory:** psychological and sociological process whereby external social or political conditions motivate individuals to challenge the status quo	- Radicalization is conceived with an explicit focus on the broader dynamics and processes of political mobilization, especially through specific social networks - The interaction between state and out of state groups may result to escalated behaviours, as w response to suppression - Analysis of the arguments inside of each radical group may lead to better understanding of the main core ideology of the group
	Symbolic Interactionism: a sociological perspective that places emphasis on microscale social interaction as it relates to self-concept.	- Assisting in the identification the salience of a specific narrative and/or objects that resonate with an individual, group, or society - Develop a level of comprehension for any novel stimuli around sociocultural and religious aspects and the way these can be exploited by groups for recruitment.
	Group Dynamic Theory: the study of two or more individuals connected by social relationships and how they interact and influence each other	- Explanation on increased group cohesion, respect for the in-group leaders and idealization of group norms - Formulation of group thinking, a process that could be also considered as a disadvantage of the radical group, if appropriately addressed without

	motivating further violent behaviours as a response to perceived threats.
Social Learning Theory: individuals learn new behaviour through observing and learning the social factors in their environment.	- Socialization within radical organizations facilitates the use of violent behaviour through learning specific mechanisms of moral disengagement - An individual may join a group for multiple reasons, evolving its personality inside the group, shaping their ideology, and escalating their behaviour to potential violent acts.
Social Identity Theory: membership in a group that helps to define a person's self-concept and provide self-esteem	- The process of shaping a collective identity is critical - The personal pathway model suggests that radicalization stems from a population that has suffered from early damage to its self-esteem, making them believe that they unsuccessful in obtaining their place in society, leading them to frustration, and participation to a radical group
Terror Management Theory: existential anxiety (or the fear of death) is assuaged by adopting a worldview that makes death comprehensible and manageable	- Explain suicide terrorism and the willingness for people to participate in such acts - There is little empirical evidence to support that this theory could be an important explanation for radicalisation

	Uncertainty reduction theory: an application of communications research, puts forth the idea that group affiliation is motivated by the desire to alleviate uncertainty	- Potential explanation for affiliative behaviour - There is little empirical evidence to support that this theory could be an important explanation for radicalisation
	Identity theory: psychosocial concept of development that focuses on the individual's concept of the self across the stages of life.	- Potential candidates for radicalization are young people who either lack self-esteem or who have a need to consolidate their identities - Participating to a radical group may reinforce the positive feelings of one's identity - Individuals follow a charismatic leader motivated by the desire to embrace the missing parent in their lives
Psychoanalytic Theories	**Narcissism theory:** a psychoanalytic theory that holds that primary narcissism (or self-love) in the form of the grandiose self does not diminish as the individual develops and expands his or her social network.	- little empirical evidence to support that radicals meet the clinical threshold for Narcissistic Personality Disorder - individual radicalised people may show relevant symptoms such as desire for admiration and attention. - Leaders of radicalised groups under this spectrum usually combine narcissism, paranoia, and sociopathy. They show grandiosity and suffer from poor self-esteem. They suspect and blame others, have no compunction regarding the use of violence, and lack empathy or concern for the impact of their actions on others.

Paranoia theory: violent radicalism is the result of a particular personality trait that predisposes one to mistrust of others and display aggressive behaviour.	- The paranoid position inflames the terrorist with suspicions that justify bloody acts of "self-defence" against his victims - Paranoid Personality Disorder, a clinical malady characterized by marked suspiciousness, irrational mistrust of others, rigidity in beliefs, and unwillingness to compromise, has been associated with terrorists
Absolutist/Apocalyptic Theory: a combination of disrupted psychodynamic development and atypical cognitive style that results in extreme polarizing, idealization of a messianic figure, and impaired social learning	- Radicals have most of the time absolutist/totalistic moral thinking, which helps motivate terrorism via its seductive appeal to young adults with weak identities - Such terrorists defend themselves from normal emotional responses to violence through denial, psychic numbing, or isolation of affect

	Antisocial/psychopathic/sociopathic theory: violent radicals are either mentally ill or somehow biologically, psychologically, and/or sociologically predisposed to violence	- lack of certain personality traits that make certain individuals more susceptible to joining terrorist organizations and engaging in terroristic behaviour - this type of personality is largely the result of a dysfunctional childhood that fosters an impoverished sense of self and hostility toward authority - Many individuals with APD share certain characteristics with violent radicals, such as a sense of social alienation, early maladjustment, impulsivity, and hostility - The characteristics of a sociopathic leadership style include lack of empathy, absence of moral constraints, and the consideration of violence as a tool to accomplish a goal, including a history of criminal activity not motivated by politics and the projection of personal desire for violent action onto the establishment
Cognitive Theories	**Novelty or sensation seeking:** a personality trait related to chemical activity in the brain that results in a preference for high-risk behaviour.	- Radical behaviour is far away from norms and ordinary experiences and political violence may satisfy innate, perhaps genetically determined, needs for high-level stimulation, risk, and catharsis

Humiliation-Revenge Theory: a psychological factor that has been suggested to predispose one to violent behaviour	- Explain the logical reaction to a personal or political grievance or a misapplication of the law of social substitutability (e.g. the killing of any member of the in-group is considered a group offense and can be avenged by the killing of any member of the offender's out-group) - Application to Al-Qaeda and its affiliated networks to include American citizens, who, as taxpayers, support the U.S. government's oppressive and exploitive policies toward the Muslim world

A shared objective both of the proposed the radicalization theories has been to develop models of the radicalisation process that trace cognitive and behavioural changes as indicators radicalised behaviours, interpreted as patterns of belief and action that develop into a threat of violence, thus into terrorist acts.

To begin with, for an individual to be radicalized, is not a process that happens at an instance [82]. As Campelo et al. [83] propose, "*there is no predefined pathway leading to radicalisation: radicalised individuals come from various backgrounds, have different origins, different family beliefs, social status or gender*". Radicalisation can occur to both men and women, to all different educational and occupational backgrounds as the whole process is triggered by a combination of various risk factors and external and internal incentives that could affect each individual, stemming from their family, friends, occupational as well as societal environment. Moghaddam had proposed a model inspired by Islamic communities in both Western and non-Western societies that described the radicalisation process as an ascending step-shaped model with six steps, including dispositional situational and environmental factors [84]. As Figure 3 illustrates, each individual questions the treatment they receive from the society and wonder if they worth such behaviours. From this ground statements, some people start climbing up the stair searching to change the unfair situation they are found in, presenting aggressive behaviour as they continue to move up to the staircase. A moral disengagement from the society, a legitimate acceptance of terrorist acts and the final recruitment to commit final acts of terrorism summarize the pathway of a small number of individuals towards the fifth step of the process [63].

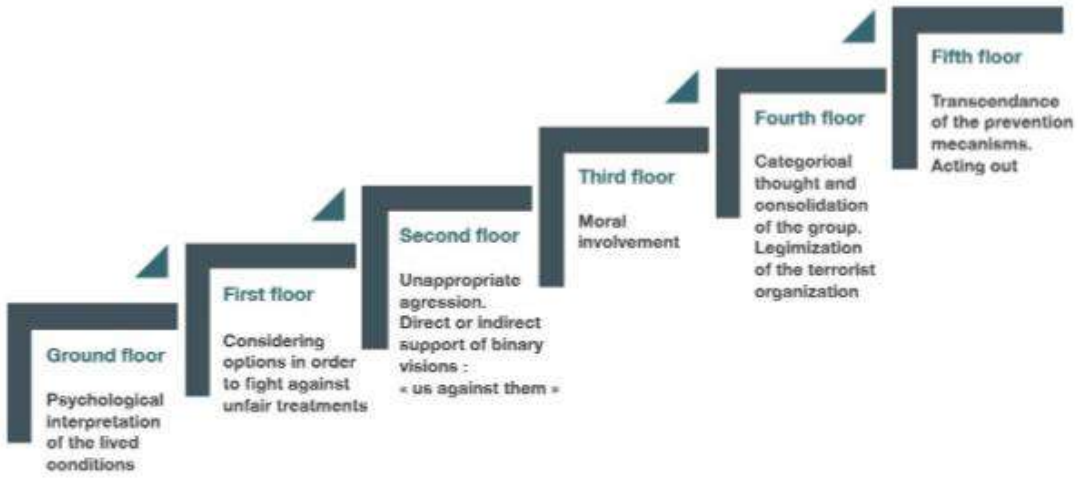

Figure 3: Moghaddam model of radicalisation [85]

Sageman's model evokes the "feeling of a moral outrage caused by perceived rights violations" [86]. According to him, feelings and personal experiences are in the forefront of the radicalisation process, identifying four distinct factors that could assist on a better understanding of the process: (a) Feeling of a moral outrage due to human rights violation, (b) monomeric interpretation of these violations as a war against Islam, (c) resonance with personal experiences and (d) networking and mobilization for terrorist acts. Another model proposed by Sinai outlines three distinctive phases of radicalization towards acts of terrorism: (i) Radicalisation, (ii) Mobilisation (a form of active engagement) and (iii) Action (i.e. terrorism) [87]. A handful of six group factors have been proposed backing up the first stage of the aforementioned model namely: (a) personal factors, (b) political and socioeconomical factors, (c) ideological factors, (d) community factors, (e) group factors and (f) enabling factors. Specific triggers act as catalysts for the second phase, making the vulnerable individual to move forward, driven by opportunities (e.g. specific contacts to terrorist groups), capabilities (training, brainwashing etc.) and readiness for action. The final component works as a connecting indicator of the second to the third and final stage.

As it can be understood from the different models, the process is a rather complex issue that entails multiple factors. According to FBI (2020) [88], there is no single reason for a person to become radicalised rather than a combination of unmet personal needs (Power, Achievement, Affiliation, Importance, Purpose, Morality, Excitement) that could lead to radicalised behaviours. Based on the 2010 Report on "Guidance for Identifying People Vulnerable to Recruitment into Violent Extremism" [89], each individual mainly experiences three distinct phases till they reach the final stage of extremisms and/or terrorist acts. The first is passive recruitment, where daily events build upon the willingness of each individual to participate in violent acts in order to combat their grievance feelings. The second phase is the active recruitment, occurring when an individual actively seeks out and/or is sought out by violent extremists, adopting simultaneously the belief that violence is the key answer to all their problems. The third phase is the act of terror itself "best described as instrumental behaviour that is used to coerce the state or groups and individuals within it". Another volume of scientific literature, impacted by school shootings, searched the radicalisation incentives among childhood experiences and personal crises, which triggered

the use of violence as an answer to injustice and fame acquisition [90][91]. More in particular, Böckler et al. [92] proposed a radicalization procedural model consisting of five stages, starting from grievance (personal, political, economic) and identification with other similar social groups, formed with same ideologies and opinions, moving to the psychological turning point of re-definition of self, planning and preparation of violent act and escalating to the violent act itself. According to Crossett and Spitaletta [81] the following sixteen factors may be considered as risks identified from the literature, that could lead an individual to radicalized behaviours:

1. Emotional vulnerability
2. Dissatisfaction with the status quo of political activism
3. Personal connection to a grievance
4. Positive (or at least non-negative) view of violence
5. Perceived benefit of political violence
6. Social networks
7. In-group de-legitimization of the out-group
8. Views on (and histories of) violence
9. Resources
10. External support
11. Perceived threat
12. Conflict
13. Humiliation
14. Competition
15. Youth
16. Resonant narrative

All these factors can incite certain radicalization mechanisms (mass, group and individual) that could lead to the final radicalisation process of a certain individuals. Internet, one of the most widespread information infrastructures of the contemporary global society that has on the one hand ameliorated several aspects of human's life, but on the other provided new opportunities for criminal activities, has been widely used from extremists and terrorist groups for further recruitment and proliferation of their networks. Online radicalisation has been a focus for rigorous scientific academic research, especially for the study its potential influence on the radicalisation process [93]. According to two studies among convicted UK terrorists and attack plotters [94], 54% utilized the Internet to learn around certain aspects of their intended activities, 32% planned their attacks using online sources (e.g. bomb making, suicide vest etc.) while 44% of them downloaded extremist media (audio lectures, videos and photos). Von Behr et al. in 2013, in his study among 15 radicalized individuals suggested that Internet was a key source of information, communication and of propaganda for their extremist beliefs" and provided a "greater opportunity than offline interactions to confirm existing beliefs" [95]. In addition to that, a study of Gill, Horgan and Deckert in 2014, showed that 35% of 119 lone-actor terrorists interacted in a virtual way with a wider network of political activists, with 46% of them learning attack methodologies from online social networking [96]. Parallel to the previously mentioned function of the Internet, it also offers perpetrators an unregulated and unrestricted place where they can disseminate their propaganda, through in

numerous social media platforms and websites, in a low-cost, easily accessible, fast, anonymous way. Since 1990, terrorist organisations have started using the Internet for fundraising and publicity purposes, while by 1999, this mean of communication had become the most prominent arena for jihadist propaganda. Till 2005, more than 40 terrorist organisations had an online presence to more than 4500 websites, while from 2000 they also utilized social media for mass recruitment and propaganda dissemination, along with training, and incitement [97]. According to a review paper of 88 existing studies (2000-2019) on the role of the Internet in a) right-wing extremism and b) radical jihadism, "available studies show that extremist groups make use of the Internet to spread right wing or jihadist ideologies, connect like-minded others in echo chambers and cloaked websites, and address particularly marginalized individuals of a society, with specific strategies for recruitment. However only a handful of studies recently published have already started to create causal designs and explain (rather than describe) online radicalization processes" [98]. In addition to that, Liebermann (2017) [99] outlines nine ways Social Media platforms have changed the way that terrorists use it for their purposes, namely as:

1. They assist terrorist to spread their content to in numerous websites without using a third party
2. They provide efficient recruitment techniques to large audience with minimal effort
3. Individual can access without any effort terrorist propaganda
4. Internet postings are not regulated as sources of news, and thus terrorists can post inaccurate information with almost no oversight or regulation
5. Anonymity can be the "trojan horse" for terrorists to broadcast their messages to respective individuals, evading detection by law enforcement.
6. Terrorists can gain knowledge about social media in order to distort the prevalence and ranking of their messages on search results
7. Internet and Social media can assist multidirectional communication
8. Terrorist groups can use social media to search for and target individuals who might be particularly vulnerable to their ideology
9. Encryption allows private communication networks and secret recruitment efforts

Finally, Guadagno in 2010 proposed a model of online terrorist recruitment progression as depicted in Figure 4.

Behavior	Social Identity Process	Self-Perception Process	Computer-Mediated Communication (CMC) Factors
Initial request: Invitation for recruit to visit website.	Social identity as a member of terrorist group is not salient to the recruit.	Recruit perceives him- or herself as an ordinary individual.	Initial request can be made face-to-face, via CMC, or through religious magazine, journal, or flyers.
Initial commitment: Recruit visits website, just to look around.	Social identity as a member of the terrorist group is made salient as the recruit explores the website. The group is portrayed as an exclusive ingroup with a virtuous mission. The recruit begins to identify with the group.	Recruit perceives him- or herself as someone willing to learn about the terrorist group from the source.	Commitment is anonymous, at a safe distance, with time/pace controlled, and no complications from nonverbal cues.
Escalating commitment: Recruit expresses desire for more info/access through site "membership" or login codes; it's granted. Access and information is provided.	Social identity as a member of terrorist group becomes more salient as the recruit begins to support the group and see him- or herself as a member of the ingroup with shared religious and political beliefs.	Recruit perceives him- or herself as a new member of an important online community that supports the political agenda of the terrorist group.	Commitment is primarily anonymous, based on login usernames & aliases. Communication is still at a safe distance, with time/pace controlled, and no complications from nonverbal cues.
Escalating commitment: Recruit proves loyalty by posting in online forums, disseminating radical propaganda, videos, etc.	Social identity as a member of the terrorist group becomes more salient and important to the recruit as he or she becomes a terrorist sympathizer. Internalization of the group's beliefs starts to occur.	Recruit perceives him/herself as a full-fledged terrorist sympathizer who supports the group's larger mission.	Desire for anonymity within ingroup dissipates. Anonymity remains as protection from the outgroup. Communication is still at a safe distance, with time/pace controlled, and no complications from nonverbal cues.
Final commitment: Recruit meets face-to-face with other terrorists, engages in group prayers, foreign travel, and training exercises.	Social identity as a member of the terrorist group is most salient and important, as recruit becomes established member of the terrorist ingroup and fully internalizes group's beliefs.	Recruit perceives him- or herself as a full-fledged terrorist group member, willing to carry out violence on command to meet organizational goals.	Anonymity remains as temporary protection from the outgroup. Recruit gives up control of own behavior to authoritative terrorist leaders.

Figure 4: Model of Online Terrorist Recruitment Progression

However, there is no easy offline versus online violent radicalization dichotomy to be drawn [100] as the Internet does not accelerate the process but rather seems to act like a catalyst by facilitating the process [101].

It became clear that the course of radicalisation is strongly related to the individual situation of persons, in which different factors play important roles. These include personal feelings or group processes that cannot be automatically recorded, analysed and evaluated by algorithms. Otherwise, there would be a risk of bringing persons under general suspicion. This chapter is intended to provide a deeper understanding of radicalisation processes among the end-users, since, as it will be described in the following (chapter 6), operators are significantly involved in determining the level of radicalisation of persons and also of websites. However, this chapter is clearly distinct of those chapters that describe the technical realisation possibilities of tools (chapter 6).

5. Prediction of Criminal Behaviour – State of Research and description of methods

Criminology not only has the task of explaining crime, it must also develop criminalistic methods and instruments to support security authorities in the analysis, investigation and prevention of crime. A distinction must be made here between predictive, investigative and preventive functions. Facial recognition, Journey to Crime or video surveillance are methods that primarily support security authorities in investigating or clarifying criminal offences. While methods from the field of predictive policing should enable the security authorities to "get ahead of the situation".

The following chapters focus on facial recognition and video surveillance as methods that primarily have an investigative support function. Even if face recognition and video surveillance tools can be significant contributions to crime prevention and fight against terrorism and organized crime, no concrete methods and implementation options are formulated here due to data access issues.

Subsequently, the concrete possibilities of using predictive policing and predictive policing tools to meet the requirements of the LEAs formulated in the use cases are discussed.

5.1 Investigation support technologies

5.1.1 Face Recognition

Video surveillance and face recognition are playing an increasingly important role in security and risk management as digitalisation progresses.

Facial recognition can be used to "identify people who can be seen in photographs or videos by their faces. This identification is based on visible, individual anatomical features in the area of the face or head" [102][46], making it a biometric recognition method. For the purposes of crime prevention or prosecution, for example, surveillance footage of a perpetrator at a crime scene may be compared with images of possible suspects held by the police, for example as a result of identification procedures [102].

Since February 2019, for example, the Bavarian State Criminal Police Office has been using a specially developed, nationwide facial recognition system (GES) with the aim of identifying wanted persons by comparing them with images from identification service treatments and current search images. The image material for the searches carried out comes from various sources, including surveillance cameras, seized photographs of unknown persons, surveillance shots and the Internet in general and social networks in particular [103].

From a technical point of view, the recognition of persons by means of camera images is problematic, since the same face can produce very different images, which is mainly due to variances in the recording conditions. Possible differences depend mainly on the following factors:

- "Position of the face in the picture
- Distance from camera or magnification factor

[46] Translated by the author from German

- head orientation
- facial expression
- background
- Partial occlusion
- lighting
- Camera type and setting" [104][47]

Changes in these factors must be factored into the process of facial recognition and captured in order to make reliable statements about the identities of the faces of different images [104].

In addition to the identification of suspects and the identification of potential danger within crowds, image recognition algorithms are also used to detect criminal tendencies (physiognomics). The latter, for example, is based on the assumption that criminals can be distinguished from non-criminals on the basis of external characteristics, i.e. genetic dispositions manifest themselves in the external appearance of a human being. This thesis is worth discussing and should be critically questioned. It essentially goes back to Lombroso's doctrine of the born offender, according to which offenders are recognizable by physical stigmata [31]. He assumed that the "*physical, inherited stigmatisation in the investment factors [...] was causally responsible for the deviant, criminal behaviour*" [44][48]. A number of other biological theories of crime have emerged from Lombroso's assumptions that crime is the result of individual behaviour determined by certain biological factors [44].

However, the thesis that facial recognition systems can read human characteristics, such as criminal tendencies, from external features in faces via artificial intelligence is controversial. Artificial intelligence generally searches for similarities in pictures, whereby certain characteristics in the face do not necessarily have to be decisive. For example, correct identification of offenders may be based on the system deducing commonalities from similar lighting, clothing or shooting angles, since images of offenders are usually taken by law enforcement agencies. [49] In this context, very general questions arise about the use of artificial intelligence. From a certain stage it is no longer comprehensible how the algorithm came to its result, which is not only legally and ethically questionable, but also the acceptance of a software solution with the security authorities can be damaging.

5.1.2 Video Surveillance

In Europe, video surveillance is used in public spaces as a "multifunctional tool for various forms of risk management" [106][50] in various areas. Video surveillance has a particularly important role to play in preventing crime and increasing the subjective sense of security of the population. The secondary objectives of video surveillance in this context are to use video surveillance to investigate criminal offences and prosecute criminals.

[47] Translated by the author from German
[48] Translated by the author from German
[49] See also Wolfangel [105]
[50] Translated by the author from German

However, the recent terrorist attack in London on 29th November 2019 calls into question the effectiveness of video surveillance in preventing crime. Although London is regarded as the capital of video surveillance in Europe and where an extensive network of surveillance cameras is in place, terrorist attacks have occurred in the past and continue to occur in the present. The attack on the Boston Marathon on 15th April 2013 also shows that video surveillance of the public space is not necessarily suitable to prevent crimes or terrorist attacks in particular, but in the past, it has been proven to be more useful for the investigation of a crime. Especially for terrorist attacks, the preventive purpose of video surveillance seems to have been missed. For terrorists who often pursue the goal of reaching a large public with the perpetration of attacks, the risk of being recognized by video cameras often plays a secondary role.

A crime-reducing effect of video surveillance in public spaces is also questionable from a scientific point of view. According to Feltes and Ruch the question as to whether video surveillance of the public space is suitable for reducing or preventing crime through a deterrent effect cannot be answered with certainty, since studies available have found either no or only a conditional effect of video surveillance, particularly in relation to property offences [107].

The use of video surveillance for preventive purposes makes sense when (in real time) video cameras can be used to detect suspicious behaviour by persons under suspicion of terrorism and emergency forces can thus be targeted at these persons in order to prevent criminal offences. However, it should be borne in mind that mix-ups can have serious consequences.

5.2 Predictive Models to support Security Measures

Predictive policing means

"when police authorities use software that [...] uses historical crime data (mostly in combination with current criminologically relevant situation data) to create forecasts of future crime areas or future offenders and use these for operations planning" [108][51].

Egbert and Krasmann understand forecast-based police work as analytical-digital procedures "*to generate and implement operational forecasts regarding the probable origins, times and places of future crime*" [109][52]. Meanwhile, algorithmic systems are used to support police work worldwide, increasingly in the United States of America, but also increasingly in Europe. These include the software Precobs (Pre-Crime Observation System) of the Institute for Pattern-Based Prediction Technology (IfmPt), which is based on the Near-Repeats approach, and police-internal developments such as Skala or KrimPro. Systems like Predpol and Hunchlab originate from the USA.

While some associate predictive policing with a panacea in the fight against crime, others see it merely as the famous look into the glass ball. The highly emotionalised discussion of recent years offered hardly any room for a factual examination of the topic of predictive policing. Long before the introduction of software solutions such as Precob's there had been "foresighted police work", which in police jargon is understood as "getting to the bottom of the situation". But even today, predictive policing solutions encounter with

[51] Translated by the author from German
[52] Translated by the author from German

reservations and scepticism. Many officials believe that they already know where their presence is needed because of their experience within the crime scene (you could also call it "good feeling") - which is not fundamentally wrong. However, critics overlook "*that feelings are in reality calculations [...] feelings are [...] biochemical mechanisms that all mammals and birds use to quickly calculate probabilities of survival and reproduction. Feelings are not based on intuition, inspiration or freedom they are based on calculation*" [20][53].

Harari calls feelings biochemical algorithms and his statement makes it clear that we humans have much more in common with computer algorithms than we are aware of or fond of. And what we have in common with computers - computers also make mistakes. There can be various reasons for this: missing data, poor data quality, programming errors or unclear objectives on the part of the specialist departments or management levels. Especially with regard to the handling of data, it is a positive effect of predictive policing that police authorities have to put their data sources and their internal structures and processes to the test.

*"What goodness do police data have and how complete are they? What can be changed in transaction processing systems [...] in order to improve the quality and completeness of the database? What other sources of information are needed to obtain the desired insights and to produce robust model*s?" [108][*54*].

And Knobloch further explains,

"the types of internal cooperation in terms of situational awareness, resource planning and evaluation must also be disclosed and, if necessary, questioned if software is to be used. Because if machines are to support us, they still need explicit instructions in many areas. For authorities whose mission is to ensure the safety of the population and their property, it is a good starting point for improving their work - regardless of how you stand on predictive policing" [108][*55*].

[53] Translated by the author from German
[*54*] Translated by the author from German
[*55*] Translated by the author from German

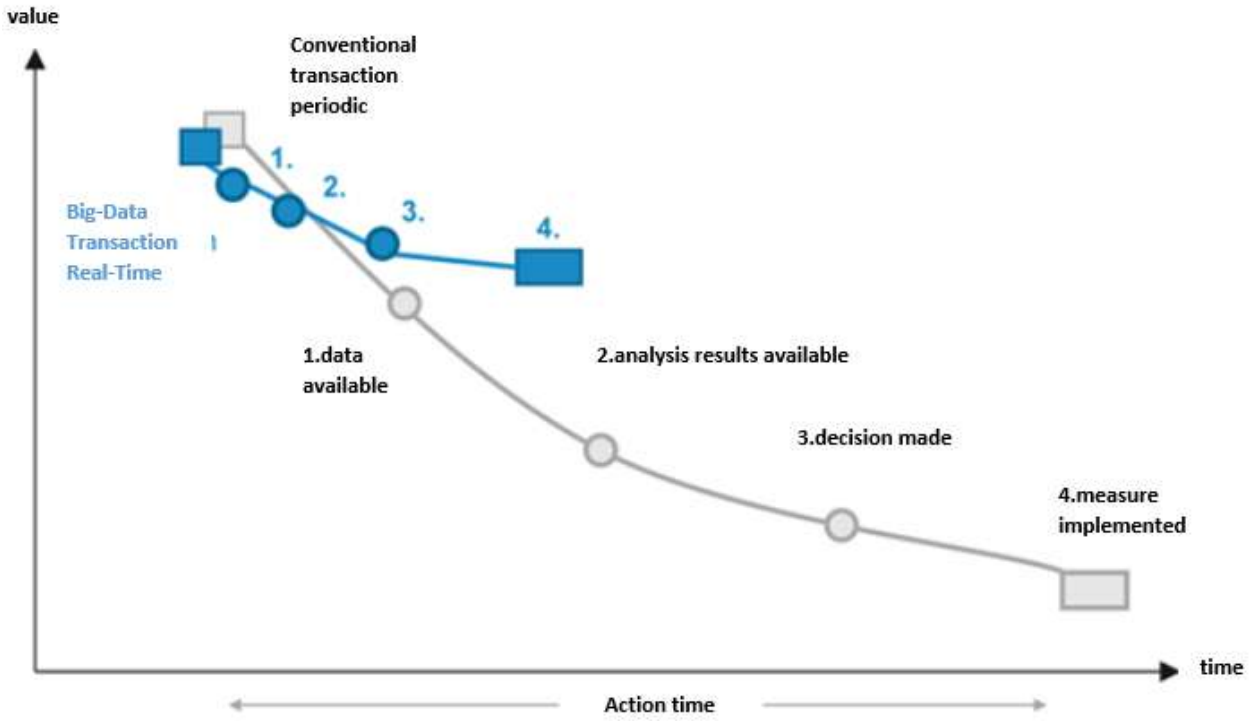

Figure 5: Comparison of conventional transaction and big data transaction [110]56

As indicated above, policemen have always been looking for ways to see the future. They used wall maps for example, and due to their criminalistic experience they were quite capable of recognizing series. The essential difference between man and machine is not that the machine does a better job than the criminologist, but it is much faster [111]. As Figure 5 illustrates, "Predictive Policing" considerably shortens the action time. Data and analysis results are available more quickly, so that decisions can be made more quickly, and measures be implemented more quickly.

5.2.1 Space and Personal Approaches

Predictive policing distinguishes between "spatiotemporal" and "personal" risk predictions. Spatial risk predictions provide information on "when" and "where" an above-average risk of crime can be expected. Personal data do not play a role in the spatiotemporal risk prognosis.

In “personal risk predictions” a distinction must be made between “perpetrators” and “victims”, i.e. personal risk predictions indicate the likelihood that an individual or a group will become a perpetrator or a victim. One form of personal risk prognosis is the individual prognosis, which is often prepared for courts.

Note:

There are no demands or specifications formulated by the LEAs that require the implementation or realization of spatial oriented predictive policing tools as part of PREVISION. But in the following a description of these is provided for the sake of completeness.

[56] Translated by the author from German

An overview of personnel-oriented predictive police instruments that conform to the requirements of the LEAs will be provided afterwards.

5.2.1.1 *Spatial Approaches*

In spatial approaches, reactive, proactive and predictive approaches can be distinguished. Journey to Crime presents a forensic-geographical approach that can rather be counted among the reactive approaches.

Journey to Crime

Geoprofiling involves, among other things, the computer-aided determination of the anchor point of serial offenders by means of crime scenes. The basic prerequisite is that there is clear evidence that the crime scenes selected for analysis belong to one and the same perpetrators. For this reason, the selection of offences to be included in geoprofiling is of great importance.

The anchor point does not necessarily have to be the offender's home; it can also be the workplace, the partner's home or the parents' home. The anchor point is characterised by the fact that the perpetrator often stays there. Since perpetrators do not like to act in the immediate vicinity of their anchor point - the danger of discovery would be too great - the so-called buffer zone is used for geoprofiling. Within the buffer zone, the probability that the perpetrator will become active there is rather low. The size of the buffer zone can vary, ranging from 200 metres to 1 kilometre in radius. Population density, for example, plays an important role in the calculation of the buffer zone. The higher the population density, the smaller the buffer zone, as metropolitan milieus have a high degree of anonymity and lack of social control, enabling perpetrators to commit crimes even near their anchor.

The concept of the buffer zone thus means that perpetrators are reluctant to commit crimes in the immediate vicinity of their place of residence or workplace. On the other hand, criminological research shows that a disproportionate proportion of crimes occur in relative proximity to the perpetrators' homes [112], i.e. the frequency of crimes decreases with increasing distance from the anchor point (distance decay). If the approaches "buffer zone" and "distance decay" were combined, this would mean that from the anchor point to the edge of the buffer zone the number of offences would increase, then with increasing distance from the anchor point the number of offences would decrease (see Figure 6).

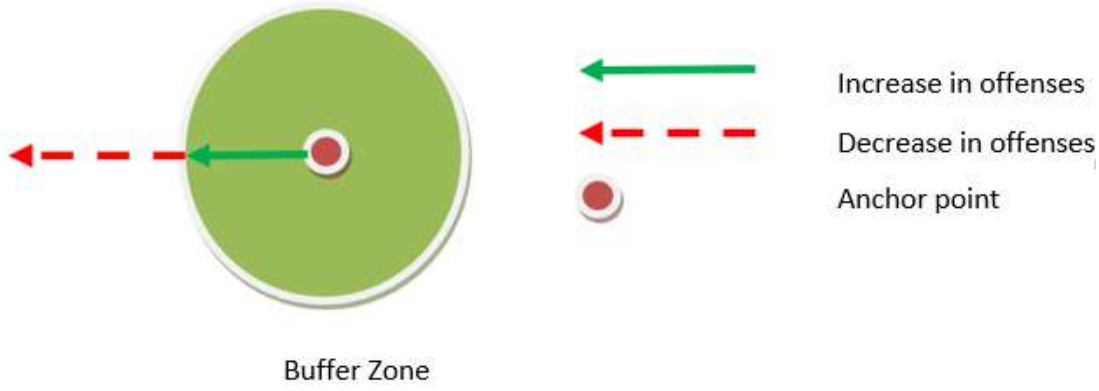

Figure 6: Buffer zone

The regional affinity of the perpetrators is due not least to the fact that criminals are habitual people and often act on the basis of rational considerations and "hardcore" routines, i.e. like to become active in spaces that they know and feel safe in (comfort zones). The more familiar the perpetrator is with his area of action, the better he knows potential escape possibilities and can assess the behaviour of the police forces operating there. In this context, it is also important that the space chosen by the perpetrators offers sufficient or lucrative objects. Travelling perpetrators also like to return to the rooms in which they had been successful in the past. This explains the phenomenon of repeat victimization and the emergence of near repeats.

Journey to Crime also includes elements of proactive police work. In contrast to perpetrators close to home, traveling perpetrators come from outside and usually have no anchor point. But the geoprofling can also provide initial investigative approaches for perpetrators from abroad. In such cases the calculation of a peak area is recommended. In the early stages of a series, the space is determined where the density of crimes was highest in the past. Thus, the future area of action of the perpetrators can be "evaporated" into an area to be monitored by the search forces.

Peak areas can not only be used for investigative measures, for regional perpetrators they can also provide evidence to the anchor point of the perpetrator

"Twenty percent of the crime series data analyzed through a journey-to-crime function of CrimeStat 3.3 successfully identified the anchor point of the offender's home within in a peak profile Area. In 40% of the cases, the offenders home was just outside of the peak profile Area of the journey-to-crime analyses. In the other 40% of the cases, the offenders reported home address was nowhere near the peak profile Area" [113].

The former patrolman Rossmo is considered one of the pioneers of the Geoprofling. But Rossmo was not only a policeman, he is also a mathematician and a Doctor of Criminology. Rossmo's vita shows how

important it is to combine criminalistic experience with the know-how of natural and social sciences in order to fight crime effectively and efficiently.

With a modified variant of Journey to Crime, the whereabouts of (potential) terrorists could be identified. Perpetrators often communicate with mobile phones that are only switched on when they believe they are far enough away from their anchor point. If it is possible to locate the locations from which the telephone calls are made, these landmarks can be placed in a spatial (and temporal) relation and analysed according to patterns or anchor points can be calculated (Figure 7).

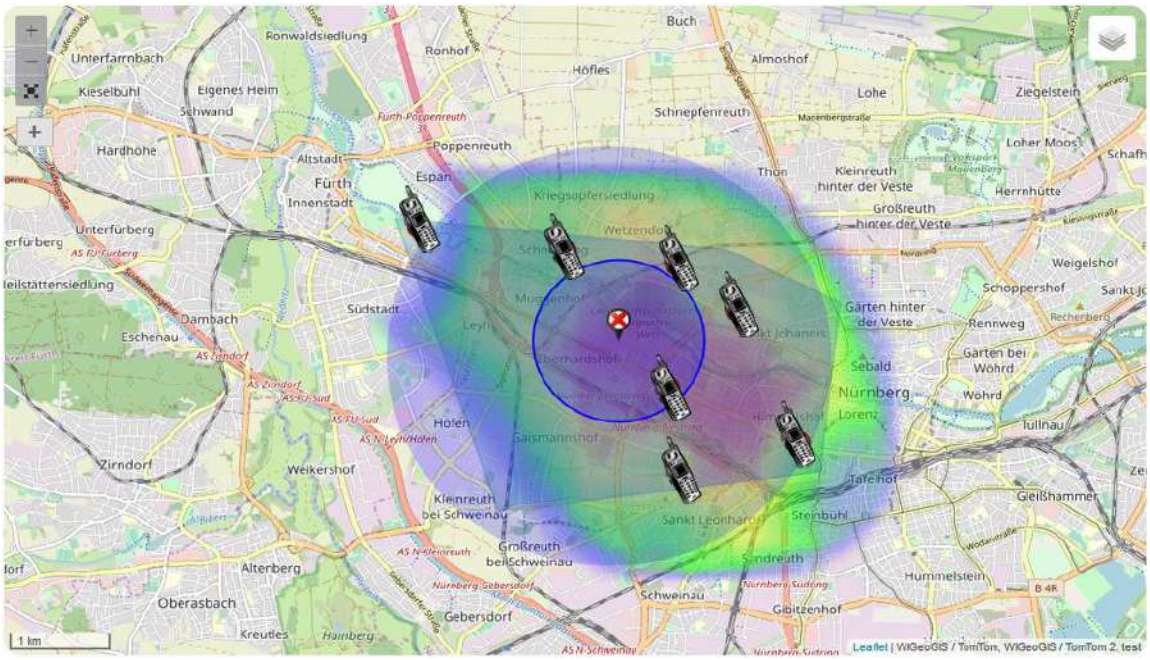

Figure 7: Location of the anchor point[57]

The modernisation of police work has led to the establishment of new methods alongside standardised police practices. These include community policing (neighbourhood- or neighbourhood-oriented police practices) and problem-oriented policing (problem-oriented police practices) as well as hot spots policing. Predictive policing is also gaining more and more importance in everyday police work in order to enable space-oriented and timely police intervention.

Hot spot method

The spatial procedures distinguish between hot spot methods, near repeat approaches and risk terrain analysis (Figure 8 illustrates an example of the hot spot method). Hot spot methods fall under the category of "proactive police work". Over time, crime concentrations can develop into focal points of crime, so-called *hot spots*. In this context, continuous and alternating hot spots can be distinguished.

[57] PRECOBS E

Figure 8: Hot spot method58

Constant hot spots are usually so-called "crime generators", i.e. places "that continually generate crime [...] by attracting large audiences (and also potential perpetrators) and accordingly producing crime opportunities" [114][59]. In addition, geographical areas in which subcultural milieus are established can become focal points of crime, i.e. "crime attractors" (e.g. open drug scenes) - with all the associated forms of crime (drug trafficking, violent crime, burglary, etc.).

To be distinguished from this are unsteady or *alternating hot spots*. There are districts in which hot spots can form for a limited period of time, for example caused by intensive offenders or travelling gangs. Often these hot spots disappear after a certain time, namely when perpetrators have "grazed" these areas [114][60]. The arrest of intensive offenders on the basis of observations (perpetrator-centred measures) can also lead to an abrupt end to series of burglaries. (Unsteady) hot spots can also overlap, e.g. when two independently acting perpetrators or gangs are active at the same time in almost the same area.

At this point, the terminology needs to be concretised. As already described above, unsteady hot spots dissolve themselves after a certain time. With regard to burglary, this means that the perpetrators concentrate on other areas and the focus shifts. One could speak of "wandering hot spots" in this context. This does not mean, however, that the same perpetrators will not return to this room after a certain time. For example, Balogh refers to a study by Ericson which states that "76% of the burglars with whom he conducted interviews return to houses they had already broken into after different periods between two

[58] PRECOBS E
[59] Translated by the author from German
[60] see also Townsley et al. [115].

and five times. Another recent study shows that "at least 37% to possibly 97% of all attacks on a particular target are committed by the same perpetrators" [114].

In this way, *continuous hot spots* can be distinguished from *near-repeat-affine areas.* In a constant hot spot, there is a similar incidence of crime every season, but in a near-repeat-affine area the incidence can fluctuate seasonally. It should also be borne in mind that a hot spot can affect different social spaces, so that both parts of socially deprived areas and parts of socially well-off residential areas can belong to the same hot spot. What they all have in common is that they are *delinquency areas*.

Bertozzi makes an interesting distinction [116]. She distinguishes between *supercritical* and *subcritical* focal points. Police operations in supercritical hot spots will only lead to a relocation of crime to other areas, while increased police presence in subcritical hot spots will lead to a long-term containment of crime.

In principle, a hot spot is not necessarily a near repeat area. A near repeat area can be a hot spot but does not have to be a hot spot in the criminological sense. Predictive policing also makes sense, especially to identify or forecast unsteady hot spots. Predictions of crime in areas with a constant crime rate do not represent a major challenge - in the predictive sense.

Near Repeat Approach

The Near Repeat Approach is a concept which has been transferred from epidemiology[61] [117] to the field of criminology and which is based on the assumption that after an initial event there is an increased probability of subsequent events within a limited geographical space and a short time interval and that this risk decreases with increasing temporal and spatial distance to the initial event [118][119]. In more concrete terms, near repeats are geographical districts in which an offence has been committed and in whose surroundings and at short intervals of time subsequent offences are to be expected: "offenders [...] commit further burglaries in the vicinity of burglary sites and in temporal proximity, simply for the sake of maximising their yield while at the same time minimising the expenditure" [108][62], which can be derived, among other things, from rational choice theory.

The Near Repeat phenomenon is a derivative of the concept of Repeat Victimization [120] and encompasses “the recurrence of crime in the same places and/or against the same people” [121]. In the context of the flag and boost hypothesis, the reasons why the existence of repeat victimization is assumed are formulated [122]. The *flag hypothesis refers to* the attractiveness of an object for the perpetrator. The hypothesis is that repeated victimization occurs in particularly attractive or vulnerable targets. Accessibility, discovery risk and prey expectations play an important role in this context. According to the *boost hypothesis,* perpetrators penetrate the same object several times and at different times in order to minimize their effort. They prefer apartments and houses in which they had already successfully broken into in the past.

[61] The Near Repeat phenomenon originated as an epidemiological concept to investigate the transmission of infectious diseases.
[62] Translated by the author from German

The concept of repeat victimization thus assumes that crimes have both a spatial and a temporal relation to each other, namely "particularly through the process of 'exposure' resulting from proximity to where offenders live and to areas with criminogenic characteristics, and through the process of 'diffusion' of crime effects arising from sequences of social interactions" [115]. Based on this, Morgan derived the Near Repeat phenomenon from his study of burglaries in a suburb of Perth [123], which can be understood as a special case of Repeat Victimization [115]. As part of his investigation, he observed that "'one-time victims' tended to cluster around a repeat victim in certain instances" [115] and that "the repeat victim addresses occurred first and the one-time victims were burgled shortly after, suggesting some form of 'contagion' process at work" [115].

The near-repeat phenomenon identified by Morgan is closely related to Pease's concept of "virtual repeats" [121], according to which criminal acts can be linked because of the similarity of victims or targets [115]. Townsley et al. justify the consideration of criminal incidents as repetitions by the fact that all offences were committed by one and the same offender and that the targets were chosen because of their similarity [115: "The logic on the part of the offender is understandable - *target suitability can be assessed in terms of similarity to prior targets*" [115]. Nevertheless, it should be noted that "near repeats differ from virtual repeats with respect to the spatial component" [115]. Whereas in the light of the "Virtual Repeats" hypothesis "targets are selected solely on the basis of their similarity to previous victims", the Near Repeats approach also takes into account the spatial proximity of the targets [115].

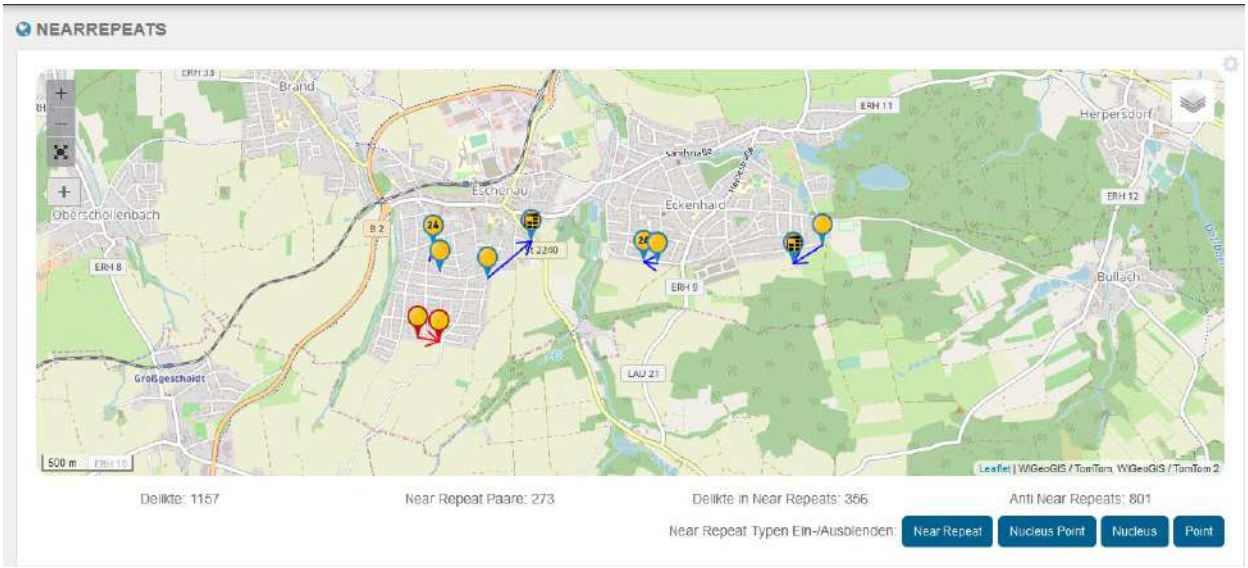

Figure 9: Near Repeats[63]

Townsley et al. identify two concepts on which the Near Repeat phenomenon is based: (1) "Homogeneous Areas" and (2) "Contagion Process".

The concept of "homogenous areas" is based on the idea that areas with homogeneous residential areas are more often affected by crime than heterogeneous residential areas, since offenders in these

[63] PRECOBS E

residential areas are offered a large number of their preferred targets and can be burglars with little effort due to similar characteristics of the targets [115]. The concept of the "Contagion Process" states that victimization risk is related to distance from previous goals and "victimization can be ‘passed’ from victim to victim in a similar way to which in diseases" [115]. This circumstance can be explained on the basis of Routine Activities Theory [48] and Lifestyle Exposure Theory [124], according to which the probability of becoming a victim of a crime increases with the availability for potential perpetrators in the absence of suitable protective mechanisms. Overall, the authors attribute the greatest effectiveness to the infection processes in homogeneous areas [115].

IfmPt has developed a method to combat (organised) domestic burglary using the near repeat approach (see Figure 9). The Near Repeat Prediction is based on the concentration of offences in narrow temporal and geographical areas. With the help of this method, areas in which the risk of crime is above average in the coming days can be promptly identified. Police authorities in Germany and Switzerland have been working with this form of predictive policing for several years (Precobs).

In addition to domestic burglary, Near Repeat Prediction can also be used to combat other phenomena of mass crime (e.g. theft from vehicles, theft of vehicles).

Empirical analyses of crimes from the field of mass crime suggest that a similar pattern exists alongside the familiar Near Repeats phenomenon - that of **Far Repeats**, which are mainly produced by traveling perpetrators and follow other spatial parameters. Like Near Repeat Prediction, Far Repeat Prediction, developed by IfmPt, assumes a "space-time reference", except that trigger and follow-up offences lie in different reference areas that can be miles apart. With the Far Repeats method, it is possible to successfully forecast in rural areas in particular.

The Trafford method is very similar to the Near Repeat approach. This approach also focuses on spatial-temporal relationships between offences. The Trafford Method describes a study conducted in the city of Trafford (UK) to reduce burglary. This was applied in the years 2010-2012 and led to a significant reduction in the number of deeds.

The Trafford method consists of several analysis options:

- Risk maps,
- major crime periods, and
- Super cocooning.

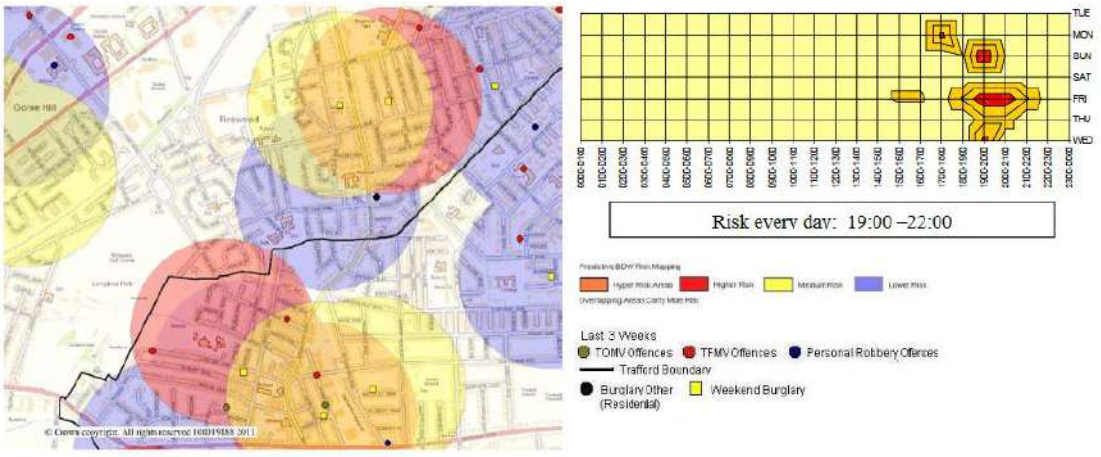

Figure 10: Trafford Method [125]

The risk cards are drawn up on the basis of the offences committed in the last three weeks, always on Monday (for the next four days) and Friday (for the coming weekend). In addition to home burglary offences, other types of offence can also be displayed on the map, but they do not play a role in the evaluation.

The evaluation of the selected home burglary offences takes place as follows (Figure 10): A circle of 400 metres in diameter is drawn around each offence. Depending on the time of the crime, these circles are coloured differently.

- Three weeks → blue.
- 2 weeks → yellow.
- 1 week → red.

Intersections between red and yellow are coloured orange. Intersections between blue and yellow or between blue and red are represented by shades but do not lead to any coloration. If identical colours overlap, they are not shaded but displayed as one area. The colours represent the risk assessment:

- Orange → hyper risk area
- red → higher risk
- Yellow → Medium Risk
- Blue → lower risk

The orange and red areas are of interest for operational and preventive measures. These rooms can also be evaluated statistically.

To support the police measures in the selected areas, the main offence time is calculated and divided into a graph according to weekdays and hours. Red areas represent a high risk, orange areas represent a medium risk.

Risk Terrain Analysis / Risk Terrain Modelling

Risk Terrain Analysis enriches police data with infrastructural, socio-economic and socio-structural data. Other data sources can also be included, such as weather data. Risk terrain analysis is about identifying risk areas in order to give police officers a (timely) indication of "when" and "where" they can expect "what" forms of crime. In addition to threshold values and trends, parameters such as the effectiveness of operational measures (patrol efficiency) or the severity of an offence (severity weight) can also be included in the calculation of risk areas (Figure 11 illustrates an example for the Risk Terrain Analysis in PRECOBS E).

Gebietsname	Methodik	Grund	Einsatzempfehlung	Aktiv	Details
Suche...					
Brandschenkestrasse	RG	Hohes Risiko, dominierender Delikttyp Wohnungseinbruch	Bestreifung	☑	
Brunaustrasse	RG	Hohes Risiko, dominierender Delikttyp Wohnungseinbruch	Bestreifung	☑	
Oetenbachgasse	S	Schwellenwertüberschreitung seit 7 Tagen	Bestreifung	☑	
Hegibachstrasse	S	Schwellenwertüberschreitung seit 15 Tagen	Bestreifung	☑	
Witellikerstrasse	T	Mehrere Wohnungseinbrüche in den letzten 2 Wochen	Bestreifung	☑	

5 Gebiete ⏮ ‹ 1 / 1 › ⏭ 10 Zeilen

Figure 11: Example for Risk Terrain Analysis[64]

Risk Terrain Modelling (RTM) is very similar to Risk Terrain Analysis. It represents an approach to the risk assessment of a geographical area. Geographic information systems can be used to provide locations on digitised maps with qualitative features of the real world [126] in order to identify areas of a city with an increased risk of crime [113]. Caplan and Kennedy describe the operation of the RTM as follows [126]:

„It operationalizes the spatial influence of crime factors to common geographic units, then combines separate map layers together to produce risk terrain maps showing the compounded presence, absence or intensity of all factors at every location throughout the landscape".

In concrete terms, characteristics are identified which make it possible to commit crimes and thus increase both the risk of a crime and of victimisation. The maps show those places that offer favourable conditions

[64] PRECOBS E

for the occurrence of criminal events [126]. For example, places where there are many shopping opportunities and shops speak for a high probability of shoplifting.

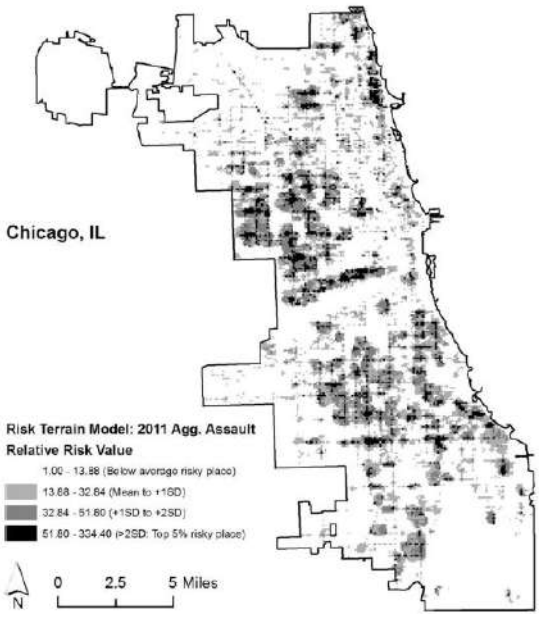

Figure 12: Risk Terrain-Map [127]

The main objective of this method is to identify crime-promoting factors in order to be able to predict crime without having to know where crime has occurred in the past [113]. RTM is based on the principles of hotspot mapping and offers a statistically valid way of identifying criminogenic and endangered areas of a city [126] (see Figure 12 for an example for a Risk Terrain-Map).

Unlike the hot spot method, the near repeat approach and risk terrain analysis belong to the category of "predictive police work".

Collados also takes a spatial approach. With his methodology he wants to predict where and what kind of crime is to be expected. The aim is to use police patrols as effectively as possible. The predictions are recalculated for each shift. Various data are included in the analysis, including the number of offences in the last hours before the forecast is made. This form of predictive patrolling aims to strengthen crime prevention in order to reduce the number of crime victims [128].

In summary, it can be said that various predictive policing solutions are now in use worldwide. The United States of America is the leader in this field, but predictive policing is also becoming increasingly popular in Europe. Spatial approaches include hot spot policing, the near-repeat approach and methods of risk terrain analysis.

In this context, a distinction must be made between more theory-driven and more data-driven approaches. PredPol, Precobs and SKALA belong to the more theory-driven approaches, Hunchlab and Risk Terrain Modelling to the more data-driven approaches. However, many programs have in common

that the Near Repeat approach is an essential basis for their forecast calculation, whereby the tendency in the future will probably go from a pure Near Repeat approach to a more complex Risk Terrain Analysis, since the theory and data basis of Risk Terrain Analysis is considerably more extensive and includes considerably more crime fields. Furthermore, socio-economic and infrastructural data are likely to play an increasingly important role in the future, in addition to pure police data.

An important role in the acceptance of predictive policing software is the traceability of the algorithms. While systems such as Precobs or SKALA are not black boxes and prediction is transparent for police officers, PredPol, for example, works with complex machine learning algorithms. In this context, the question arises to what extent self-learning algorithms (keyword: artificial intelligence) will advance predictive policing in terms of content or will have a rather counterproductive effect on the quality of the forecasts and their acceptance by users.

Finally, a distinction must be made between partially and fully automated systems. In semi-automated systems, the forecast is always validated by a police officer. This validation is not necessary with fully automated systems.

5.2.1.2 *Person-Related Approaches*

Person-related prediction approaches are especially necessary to meet the requirements of the LEAs, which are especially formulated in use case 2.

When it comes to the analysis of criminal careers, one often speaks of typical criminal careers. However, a number of criminological theories show "different, often contradictory courses" [129][65]. Within the criminological research of the last decade, there is a tendency to resort to the group-based trajectory model within the framework of empirical investigations of criminal careers. Although this method promises the identification of typical criminal careers, no uniform picture of typical criminal careers could be determined on the basis of previous analyses, which raises the question of whether there are patterns in criminal careers that can be used for forecasting purposes [129].

The Max Planck Institute for Foreign and International Criminal Law in Freiburg has also conducted an empirical investigation into the question of whether the existence of typical criminal careers can be assumed. For this purpose, data from the Freiburg cohort study were used. The study includes data on the frequency and development of criminal behaviour and on judicial responses to this behaviour. In the sample analysed, the judicial registrations of German men born in 1970 were taken into account. The sample consisted of a total of 21,093 men with at least one so-called criminal offence [129].

A group-based trajectory analysis was carried out, taking into account the three parameters of entry age, frequency of registrations and length of career [129]. Grundies formulates the aim of this method as follows:

"Their aim is to extract typical progressions over age on the basis of individualised longitudinal data. This method uses and checks a structure consisting of the group sizes and the associated progressions for their

[65] Translated by the author from German

overall adaptation to the data (i.e. the individual progressions) and varies them successively until this adaptation becomes optimal. The result is a structure of group (-sizes) and the associated processes, which capture the structures contained in the data as well as possible" [129][66].

In the context of the analysis described, a total of seven groups could be identified, whereby the individual persons could not be clearly assigned to the respective groups, but rather often belonged to several groups [129]. Grundies comes to the conclusion that the "recorded criminal careers [...] were characterised by a large but evenly distributed diversity of individual courses"[67] and differed in terms of the three parameters mentioned, but that no typical courses or criminal careers could be identified [129]. Against this background, Grundies concludes that the groups determined represent "fictitious approximation points of a continuous distribution" [129][68].

Thus, it can be stated that the existence of typical criminal careers must be questioned. It cannot be assumed that patterns in criminal careers can be empirically proven, which makes it very difficult to forecast criminal life courses. For Grundies, the cause of crime lies in a disturbed balance between the individual and society. "Even if such disturbances accumulate in adolescence, the lack of patterns indicates that this balance can in principle be disturbed at any age" [130][69].

Biographical perspective

One way of opening up the future is biographical research, i.e. dealing with the biographies of people who had appeared in the police force in the past because of (politically motivated) crimes. In this way, "typical" biographical patterns can be identified on the basis of which statements on future perpetrator behaviour can be made. Biographical research has meanwhile become a common empirical instrument in criminology [131][132], which has already been used in both extremism and mafia research.

Against this background, it should be noted that politically motivated criminals differ from “ordinary criminals” in two key respects: Besides the concrete victims, i.e. people who are injured or killed by politically motivated acts of violence, e.g. terrorist attacks, the social order of a country is damaged (abstract victim). In addition, the extremist also feels himself to be a victim, a victim of state exploitation, arbitrariness and repression. Ultimately, by assuming the role of victim, the terrorist legitimizes the use of force to achieve a political goal. In this sense the politically motivated criminal may see itself as an “altruist” who turns against social grievances for which he holds the state or social elites responsible [22][133][134].

The aim of biographical research is to reconstruct the life course of people in order to subsequently combine people with similar life courses into clusters, whereby there should be a high degree of homogeneity within the cluster but significant differences between the clusters. The following are central topics of biographical research:

[66] Translated by the author from German
[67] Translated by the author from German
[68] Translated by the author from German
[69] Translated by the author from German

family situation

- Parents (age, occupation, social class, relationship to respondent)
- Brothers and sisters (number, sex, relationship to subject)
- Problems in the family (violence, addiction, unemployment, divorce etc.)
- Political Activities/Delinquent Behaviour of Individual Family Members

School career (chronological order)

- which *types of school* were attended *when* (reasons for possible change of school)
- Problems at school/type of problems

Training (chronological order)

- which *training(s)* were started/completed *when*?
- there were problems at the training place, and if so in which form
- Professional career (chronological order)
- what jobs did the test person take up?
- the test person was (several times) unemployed

Political activities (chronological order)

- political understanding
- in what form was the subject politically active?
- the test person was involved in a party or informal group (e.g. skinheads)
- the respondent can understand the motives/actions of members of other extremist groups
- Similarities/differences to other extremist groups
- Opinion on 11 September; can the respondent put himself in the position of the assassin's motives/actions?

Criminal career (chronological order)

- when the first time delinquent
- when the first time is conspicuous by the police
- when first sentenced
- how often convicted
- prison sentences (when first imprisoned)
- which forms of delinquency

Social deprivation

- addiction problems
- understanding of violence

Circle of friends/acquaintances

- Role/influence of the circle of friends/acquaintances with regard to the criminal or political activities of the test person
- recreational activities

One hope associated with biographical research is to obtain a kind of socio-psychological profile that can be used to identify perpetrators of violence - especially terrorists - in advance. What is problematic is that many extremists/terrorists are not at all psychologically conspicuous or have any (social) problems. Of course, there are also people among terrorists with mental illnesses or fractures in their biographies. In addition, there are quite a few former petty criminals among terrorists. On the other hand, there are countless mentally ill or socially conspicuous people who will never commit politically motivated crimes. Here there is a danger of suspecting these people wrongly. Also, most criminals do not become political activists [135].

What can be derived from previous biographical research regarding the personality profile of extremists/terrorists for predictive police work?

- Extremist / terrorist careers have many coincidental moments, both in the choice of extremist milieu and in the course of the extremist career. Thus, the former left-wing street fighter Joschka Fischer became Foreign Minister of the Federal Republic of Germany, from the well-known journalist and mother of two Ulrike Meinhof a co-founder of the Red Army Faction (RAF). The members of different extremist milieus are also similar in terms of psychosocial dynamics.

- Extremist milieus offer social identity and social belonging. Individual problems are pushed into the background, one's own existence gains in importance. Not only does one fight for a good cause, the fight is also dangerous and exciting, which attracts young men in particular.

- The ideological orientation is often overestimated by experts. The interest in or knowledge about politics or religion is often rudimentary, ideological patterns of argumentation and views are often adopted without reflection. Membership in a terrorist group can also have monetary reasons.

- There are no significant differences in the socio-demographic (e.g. educational level, gender, socio-economic status) characteristics between extremists/ terrorists and other delinquents. [136]

Just how difficult it is to create a socio-economic profile can already be seen in the foreign fighters. While the German and Scandinavian fighters are primarily socially underprivileged petty criminals, the British foreign fighters were "a clear majority" of students or academics. "What unites them is not a demographic or socio-economic characteristic, but the lack of identification with the Western societies in which they were (mostly) born and raised" [137][70].

It is very unlikely in the future to distinguish terrorists from other people on the basis of personality traits. Causes and motives that lead people into extremist milieus are very different. Apart from life crises, the search for identity or the longing for adventures, pomposity, psychological problems or broken families can also be responsible for this.

[70] Translated by the author from German

Although previous research suggests that it is difficult to distinguish biographies of extremists and terrorists from ordinary criminals or irreproachable citizens, nevertheless, the methodology of a system, which should be used for the detection of potentially dangerous persons, was conceived (see chapter 6). A detailed description of this and an explanation of the system that should be realised within the framework of PREVISION will be given later (already previously mentioned At this point, instruments already in use for the risk assessment of persons are first listed and explained.

Instruments for risk assessment of extremist violence

A further approach to predicting terrorist acts would be the early detection of radicalisation processes or the risk classification of already known perpetrators. The study of radicalisation processes and factors and the forecasting of terrorist and extremist crimes is of growing public interest. With the discussed personal prognosis methods and risk assessment an attempt is made to "determine a risk of crime for both perpetrators and victims and to make this usable in police practice"[137][71]. According to Logvinov [138], a risk assessment is "a prognostic statement limited to a defined period of time about the probability of occurrence of a certain negative or damaging event in a target population"[72] and is composed of a quantitative (probability) and qualitative (type of violent behaviour) variable. In the context of extremist violence, Borum defines risk assessment as follows:

„The process of collecting and considering information about a person and the situations and contexts that the person will encounter in order to describe and evaluate the potential that the person will engage in jeopardous behavior and prevent or mitigate the behavior and its adverse consequences" [139].

In Germany, for a long time there were no operationalizable models that allowed a systematic examination of the dangers and risks emanating from extremist actors, with the exception of the analysis scheme of Pfahl-Traughber [140][138]. He developed the so-called AGIKOSUW scheme for the risk assessment of extremist violence (offenders), which includes the following explanatory variables: Activists, intensity of violence, ideology, communication, organization, strategy, environment and impact. It provides "a precise and uniform record of terrorist activities" and "contributes to the establishment of a more precise profile of terrorist groups" [138][73].Urban also developed an analysis model (Table 4) in which some risk factors were assigned to the study levels "actors", "ideology", "reference group" and "framework conditions" [141]:

[71] Translated by the author from German
[72] Translated by the author from German
[73] Translated by the author from German

Table 4: Analysis model by Urban 2006[74]

Variables	Factors
actors	aims capabilities resources Leadership/Cohesion Readiness to use violence/methods goal orientation
ideology	Reach/anchoring of goals in ideology tolerance for violence Dissemination in the reference group attractiveness traceability
reference group	Size ideologization support readiness dissemination distinctiveness anchoring
framework conditions	Living conditions of the reference group Enabling factors and process conditions Vulnerability and defensiveness of the opponent

Thus, for example, the dangerousness of a terrorist actor depends on its objectives, its operational and strategic capabilities and its access to necessary resources. In addition, the internal cohesion or leadership

[74] Urban [141] cited after Logvinov [138], own presentation, translated by the author from German

ability of the actor in the sense of strategic planning and implementation of the objective are decisive for the danger emanating from the actor. The readiness to use violence and the methods pursued by an actor are also important for a risk-oriented analysis of terrorist efforts [138].

In extremism research, there are various procedures for assessing risks. The various criminal prognostic methods, models and instruments can be grouped into five ideal categories [142]:

"1) intuitive criminal prognosis based on subjective experience; 2) standardized actuarial prognosis instruments with mostly static biographical risk factors (second generation); 3) third-generation actuarial prognosis instruments that record both static and dynamic risk factors; 4) structured clinical prognosis instruments and instruments; 4) structured clinical prognostic instruments and instruments; 4) standardized and standardized prognostic instruments. Checklists subsumed under the term 'Structured Professional Judgement' (SPJ) and 5) clinical-idiographic prognosis models combining empirical and idiographic methods or SPJ instruments" [138][75].

However, the effectiveness of purely statistical (actuarial) approaches is frequently questioned against the background of the low base rate in the phenomenon areas of interest: "Specifically, it is questionable whether generalizable statements on the existence of correlations and the effect of hypothetically risk-minimizing/risk-reducing factors are possible due to the low base rate and the additional high complexity of the object of investigation" [143][76]. Against this background, SPJ tools have primarily established themselves in practice.

Software solutions

In practice, various software tools are used. In the following, the objectives and functionality of some tools are presented.

- **RADAR-iTE**

The RADAR-iTE software used by the Federal Criminal Police Office represents a statistical approach (also referred to as "acturial method" or "acturial tool") and differs from "Structured Professional Judgement Tools" (SPJ). The software is one of several examples of personal predictive policing [144].

Since the beginning of 2015, the German Federal Criminal Police Office (BKA), together with the Forensic Psychology Working Group at the University of Konstanz, has developed the risk assessment tool RADAR-iTE (rule-based analysis of potentially destructive perpetrators to assess the acute risk of Islamist terrorism). This set of instruments is based on already established risk assessment instruments for the assessment of offenders [145].

The Federal Criminal Police Office Germany formulates the aim and function of radar-iTE as follows:

“RADAR-iTE assesses a person for whom there is a minimum amount of information on events in his or her

[75] Translated by the author from German
[76] Translated by the author from German

life with regard to the risk of committing a serious act of violence in Germany and assigns it to a risk scale in order to prioritise intervention measures" [145][77].

RADAR-iTE compares the behaviour of a person with previous findings on the behaviour of assassins. The actual risk assessment is carried out using a risk assessment form with 69tandardized question and answer categories that reflect both risk-increasing and risk-reducing characteristics. The risk potential emanating from a person classified as hazardous or relevant is defined as *high*, *conspicuous* or moderate [145].

The use of Radar-iTE shall make use of information already available or data which may be collected under the current legal situation and which relates exclusively to observable behaviour and does not include characteristics such as religion or belief of a person [145]. In particular, the behaviour of a person in the radical (militant-salafist) scene is of particular interest [146]. All in all, RADAR-iTE is based on 73 characteristics "which have been determined in studies to be valid, to differentiate the group of persons targeted by the instrument with regard to their risk of committing a serious violent crime" [146][78] and which can be assigned to the following seven subject areas in terms of content: Violent crimes committed so far, experiences in dealing with weapons or explosives, involvement in the radical scene, stays in war zones and participation in combat operations there as well as aspects of a problematic personality such as diagnosed psychological abnormalities. Using standardised answer categories "yes", "no" or "insufficient information", an assessment is made as to whether these characteristics are present or not [146]. The RISKANT project will evaluate, validate and possibly adapt RADAR-iTE [146].

- **VERA-2R (Violent Extremism Risk Assessment 2 Revised)**

Vera-2R is one of the best-known risk assessment instruments and has been developed with the help of research results, expert knowledge and user feedback [143]. Vera-2R works with 34 indicators and risk factors to assess a person. These indicators are rated on a three-level scale - low, moderate and high [143]. In terms of content, they cover the following risk factors:

- Beliefs, attitudes and ideology
- Social context and intention
- History, actions and competencies
- Commitment and motivation

In addition, the protective factors such as the support of non-violence by the family and other relevant persons as well as the rejection of violence are taken into account as goal achievement [138].

- **ERG22+ (Extremism Risk Guidance 22+)**

ERG22+ is mainly used in Great Britain. It is a tool for the evaluation of detained persons. An evaluation of the offenders is carried out on the basis of 22 predictors, which run along three relevant dimensions (commitment as identification with the group or thing, intention as readiness for commitment and

[77] Translated by the author from German
[78] Translated by the author from German

relevant abilities) [138]. The further development of ERG, VAF, serves to assess target groups outside the prison system [143].

- **TRAP-18 (Terrorist Radicalization Assessment Protocol 18)**

TRAP-18 is a theory-based SPJ tool and is also based on the experience of the developers in the risk assessment of the FBI. The objective shall be to assess the risk of targeted violence by individuals [143]. It is less an instrument for identifying dangerous persons than an aid in case handling. TRAP-18 is based, on the one hand, on factors that imply the need for closer examination and, on the other hand, on indicators that speak in favour of risk management measures [138]. The former include, for example, personal grievances and moral indignation, professional failures, instrumental violence or the absence of a sexual partner and the sexualisation of violence [138]. The latter represent the following warning behaviour indicators:

1. "Development process or path (research, preparation, implementation)
2. Fixation (pathological occupation with a person or thing)
3. Identification (self-categorization as command, militarization of thinking)
4. New aggression (independent of development path, initial violence)
5. Energy outbreak (increase in activities with a view to the target or victim)
6. Leakage (communication of intent to third parties)
7. Last resort ('force imperative' and 'time imperative')
8. Directly communicated threat" [138][79].

- **SAVE (Structured Assessment of Violent Extremism)**

SAVE is based on the assumption that a person's risk of extremism depends on his or her perceptions and beliefs, which is why an assessment of perception, world view and thought patterns is based on 30 cognitive risk factors. A 3D risk surface and a 2D risk contour are created. Within the framework of this approach, persons are located within the data points *estimated risk, calculated risk* and *temporal* risk [143].

Screener Islamism

Böckler et al. stress "that terrorist violence always represents the end point of a development process" [147][80]. In addition, they emphasize "that terrorist actors often show striking behavioural abnormalities in the run-up to their actions. Such assassins do not only attract attention in the official or police context, but also frequently appear in their social environment and professional life”[147][81].

Against this background, it makes sense to develop instruments to detect radicalisation at an early stage and to be able to exert a preventive influence. The "Screener Islamism" represents such an instrument for

[79] Translated from the author from German
[80] Translated by the author from German
[81] Translated by the author from German

recognizing possible radicalization processes, but according to its developers it is not an instrument for investigating crimes [147]. The Screener is used when a person is conspicuous by certain behaviours, such as the public endorsement of the Islamic State. The instrument consists of 13 different items, which can be evaluated with "Yes" and "No". The content of these items can be assigned to the following five areas of behaviour: 1) personal crisis, 2) attachment to Islamist ideology, 3) violence-related communication, 4) empowerment and 5) social environment (online and offline). Finally, a classification is made into "No Danger", "Possible Danger" and "Acute Danger". If the screener comes to the conclusion that a "possible" or "acute danger" exists, an in-depth case analysis or even a case management follows [147].

The problem with such a predictive approach is that even people who have never radicalised themselves can be considered positive. In addition, the assessment of the social environment is always subjective (there must always be a form of "suspicion" at the beginning) - what for some is already highly problematic behaviour can be an age-related form of rebellion for others. With individual forecasts there is always the problem of "false positives". Wrongly labelling someone as a potential threat or extremist can have serious implications for their fundamental rights and freedoms [148].

Strategic Subjects Lists

Another method of personal Predictive Policing are the Strategic Subjects Lists (SSL), so-called "Heat Lists". Risk factors are used to calculate the likelihood that someone will commit serious acts of violence. The simple logic of the system: those who live in a violent environment are more likely to become perpetrators or victims themselves. The people on the list are then contacted by the police and warned - even though they have never committed a crime themselves.

The problem of this kind of prediction is that it can be used as a mass surveillance instrument. In Chicago alone, more than 400,000 people were at risk, with an above-average number of black people. In such cases, predictive policing can promote stereotypes [149].

5.2.2 Further Predictive Approaches

5.2.2.1 *(Social) Media Monitoring*

To a large extent interpersonal communication currently takes place online. Criminals, extremists and radical groups also communicate via the Internet and use it for their own purposes, such as spreading propaganda or recruiting new supporters. Thus, radicalization processes are increasingly taking place in the context of social media.

Within the framework of social media monitoring, radical content can be tracked down and people who radicalise themselves can be identified. The networking and interconnection of extremist flows are tracked, for example, by the so-called LEA algorithm. This recognizes certain word combinations with reference to extremism and filters them out from comments and contributions on the internet. Thus, insights into extremist tendencies gained from these data can be used to sensitise citizens [150].

Monitoring systems are also used in Hessen to document events and occurrences in the area of right-wing extremism and to gain an overview of them. Provided Monitoring reports can support various authorities, such as the police, in their daily work and in preventive measures [151].

For dropouts or victims in the field of extremism, monitoring also offers a supportive option. Victim counselling centres use the observation of right-wing extremist, anti-Semitic, anti-Muslim and/or racist incidents in order to be able to offer direct assistance in victim counselling to cope with the consequences and restore the victims' ability to act. On site, Mobile Consulting teams develop strategies against the dominance of right-wing extremist groups. In addition, (social) pedagogical work aims to promote distance from this thematic area and to counteract ideological consolidation. In this context, model projects are funded by the Federal Government that make use of the topics of distance and exit assistance [152].

5.2.2.2 *Anomie Monitoring Model*

Anomie theory can also have a predictive benefit and is therefore relevant for predictive policing. This chapter serves to clarify to what extent the central statements of anomie theory can be used for monitoring in the field of (organised) crime and extremism/terrorism. At this point, the anomie monitoring model is presented, which is based on the principles of anomie theory.

According to Merton, anomie is to be understood as the consequence of the gap between "the social goals recognized as legitimate and the reduced possibilities of access to the means necessary to achieve these goals" [31][82]. Here, differences specific to different social classes can be discerned. Schwind illustrates this in the example of unemployment [31]. For example, access to the labour market may be hindered or completely blocked by a lack of formal qualifications or language skills, resulting in pressure and stress for those concerned. In Merton's [153] argumentation, five behavioural patterns that individuals adopt as responses to this pressure are to be distinguished and he formulates them as a typology of the types of individual adaptation (Table 5). The so-called *conformist* affirms not only the cultural goals but also the institutionalised means to achieve them. The *Ritualist* downgrades his goals or rejects them altogether but retains the legal means. Both types are not of criminological importance. Another type identified by Merton is the *innovator* who, while affirming cultural goals, tries to achieve them by illegal means and thus shows criminal behaviour. The *apathist, on* the other hand, rejects both the cultural goals and the institutionalized means, which is reflected, for example, in a flight into illusory worlds opened by alcohol, drugs or sects. Ultimately, Merton identifies the *rebel who* fights the cultural goals and institutionalised means in the form of e.g. politically motivated crime or terrorism for the purpose of changing the existing social structure [2][31].

Table 5: Types of adaption

Types of adaptation	Cultural goals	Institutionalised resources
1. conformity	+	+

[82] Translated by the author from German

2. innovation	+	-
3. ritualism	-	+
4. apathy (retreat)	-	-
5. rebellion	(+/-)	(+/-)

+ = approval, - = rejection; +/- = rejection of dominant values and substitution with new values

Against this background, Schweer critically notes that Merton does not explicitly distinguish between legal and legitimate means [2]. He explains that although certain behaviours are considered illegal by law, they may be accepted by the majority of the population and thus gain legitimacy. He also points out that cultural objectives can be both criminal and legitimate. Against this background, Schweer states that it is particularly important for criminologists to find out "to what extent illegal options for action are regarded as legitimate, since the social dissemination of a pattern of behaviour is less oriented to whether an action is legal or illegal, or whether it is legitimised by people's morality" [2][83]. Thus, state morality, which shows what can be considered legal within a society (by legal definition), and people's morality, which reflects the prevailing opinion in large parts of the population about what is considered legitimate, are two different variables (Figure 13).

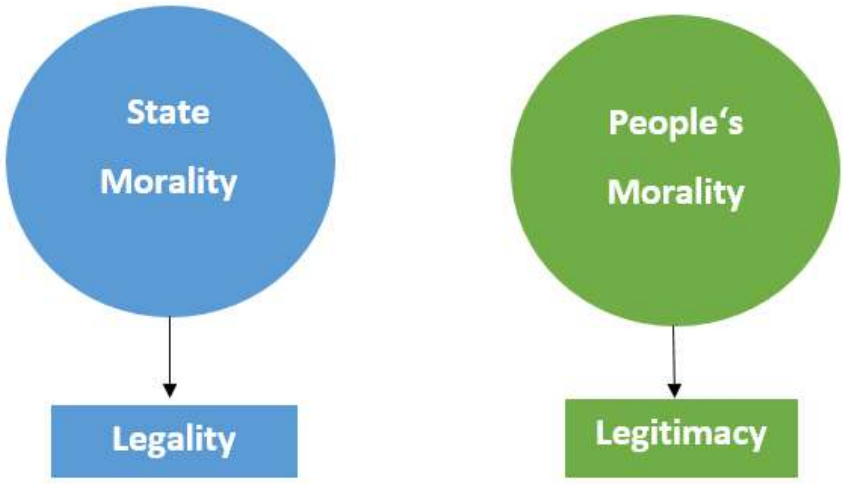

Figure 13: State-Morality and People's-Morality

If state and people's morals are congruent, it can be assumed that there is no serious social problem with regard to crime and that crime is the exception rather than the rule [2]. In contrast, the further state and

[83] Translated by the author from German

people's morals distance themselves from each other, the more likely criminality becomes as the "result of *a cultural lag between applicable law and everyday culture*"[2][84].

Thus, according to Schweer, it can be assumed that the means used to satisfy individual needs and personal goals can be both legal and legitimized by the population or can be in conflict with each other [2]. Based on this, Schweer identifies four types in reference to Merton (Table 6):

"On the one hand, Compliance with the law, which, in order to achieve cultural objectives, makes use of means that are both legitimate and legal to achieve cultural goals. To be distinguished from this is the social outsider, who uses means to achieve cultural goals that are legal but illegitimate. Furthermore, the conformist should be mentioned who behaves legitimately in the sense of popular morality in the 74egitimized of cultural goals, but criminally in the sense of state morality, as well as the actual criminal who violates both popular morality and state morality. It should be borne in mind that, in the wealth of options for action in a society, every social actor can assume the role of law-abiding, social outsider, conformist and criminal, depending on the type of action involved and the social context in which he carries it out" [2][85].

Table 6: Typology of types of individual adaption [2]

	State Morality	People's Morality
Compliance with the law	+	+
The Social Outsider	+	-
The Conformist	-	+
The Criminal	-	-

+ = affirmation; - = rejection

In this context, however, there is the problem of 74egitimized when an illegal pattern of behaviour is 74egitimized by popular morality. To this end, different types can again be distinguished: the *Law-Abider*, the *Deregulator*, the *Punisher* and the *Innovator* (Table 7):

"The punisher legitimises the respective criminal behaviour, but still demands a ban or punishment. [...] Like the punisher, the innovator also legitimises the respective criminal behaviour pattern, but, in contrast to the punisher, advocates its legalisation. [...] Although the deregulator cannot personally endorse the criminal behaviour pattern in question, he can classify the individual right [...] higher than the penal law

[84] Translated by the author from German
[85] Translated by the author from German

[...], while the law-abiding attitude continues to demand punishment or prohibition for what he considers to be not only illegitimate but also illegal behaviour" [2][86].

Table 7: Types of behaviour under conditions of social change [2]

	Assessment of illegal conduct	Demand for legalisation
The Law-Abider	-	-
The Deregulator	-	+
The Punisher	+	-
The Innovator	+	+

+ = affirmation; - = rejection

At this point, the question arises what empirical added value the theoretical findings discussed above have and to what extent they can be used for predictive purposes.

The quantitative identification of socially predominant attitudes towards illegal behaviour and their punishment or prohibition is of particular relevance in view of the fact that attitudes are considered as determinants of behaviour. On the basis of the empirical depiction of attitudes, it is possible to draw conclusions about future predominant behaviour patterns and thus about possible future social problems in terms of deviant and criminal behaviour. This insight can be used to establish a monitoring model.

In order to determine whether and to what extent deviant behaviour will spread in the future and develop into a problem relevant to society as a whole, the identification of the spread of punishers and innovators is of particular interest, since these types legitimise criminal behaviour and the individual willingness to criminal action is primarily determined by the legitimacy of a pattern of behaviour [2]. If one follows this logic, persons who, for example, consider the use of violence against fugitives or persons with a migration background or the exercise of violence to achieve political goals to be "not bad" are more likely to assume that they will show such behaviour in the future or at least tolerate it.

For concrete implementation, data must be used that depict attitudes to criminal behaviour and punitivity attitudes. In this context, it would be conceivable, for example, to use batteries of items to determine attitudes to various illegal behaviour patterns, such as

"How bad do you think the following actions are?

- Consumption of illegal hashish, cocaine or heroin.
- Exercise of violence against ethnic minorities.
- Exercise of force for the purpose of achieving important policy objectives

[86] Translated by the author from German

- Etc."

A Likert scale could be used to determine whether a behaviour is considered "very bad", "quite bad", "less bad" or "not bad at all". A similar approach could be taken with regard to the detection of punitive attitudes.

Persons who consider a certain behaviour to be bad, such as the consumption of hashish, and who advocate its punishment or a ban on hashish, represent the type of law-abiding behaviour. The statement that hash consumption is considered bad but should not be punished makes a respondent a deregulator. If people do not find an illegal behaviour pattern bad, but demand a punishment, these people are to be classified as punishers, while a legitimation of illegal behaviour and the demand for legalisation is typical for an innovator (see Table 8).

Table 8: Characteristics of behaviour types and social change [2]

Assessment of illegal conduct	Behaviour should be forbidden/punished	Behaviour should not be forbidden/punished
Very bad/seemingly bad	The Law-Abider	The Deregulator-
Less/not bad at all	The Punisher	The Innovator

The aim is to create a picture of society in order to draw conclusions about future crime problems. If the proportion of innovators within a society is to be classified as (very) high for certain areas of crime, then it can be assumed, as already mentioned, that this phenomenon will gain relevance in the future.

A number of modifications are required in order to transfer such a monitoring model to the field of extremism. Similar to the procedure described above, the measurement of attitudes is also relevant for the monitoring of extremism, whereby the collection of punitive attitudes for this area can be neglected. In order to assess whether the potential for extremist excesses prevails within a (democratic) society, the identification of those persons who are willing to participate illegally in a political system is also particularly important, as is the identification of prevailing extremist attitudes. The willingness to participate illegally in politics reflects whether individuals are considering rejecting the socially institutionalized means of political participation (e.g. participation in approved demonstrations, voter turnout, etc.) and instead resorting to illegal means such as the use of force to achieve political goals.

A person who has both an extremist attitude and a willingness to participate illegally in politics can be seen as a *violent extremist.* A person is considered a *political extremist if he or she has an* extremist attitude but is not prepared to resort to illegal means for political participation. If a person does not have an extremist attitude at the moment but would in principle be willing (in the course of social changes/ upheavals) to achieve their political goals, for example by using violence, then this person is a *potential extremist*. A person who is neither extremist nor considering the use of illegal means for political participation is a *systemic Conformist* (see Table 9).

Table 9: Measuring the extremist potential of society

		Readiness for illegal political participation	
		will	**No willingness**
Current extremist attitude	**Extremist attitude**	*Violent extremist*	*Political extremist*
	No extremist attitude	*Potential Extremist*	*Systemic Conformist*

Empirically, extremism monitoring can be implemented as follows:

In order to measure extremist attitudes and the willingness to participate illegally in politics, it is possible to resort to items used, for example, in studies conducted by the Konrad Adenauer Foundation between 1997 and 2007 [154]. Items such as "We should make sure that we keep the German in and that we prevent the mixing of peoples" or "Foreigners and asylum seekers are the ruin of Germany" [154][87] are examples of instruments for measuring right-wing extremist attitudes. The degree of agreement with these statements is usually measured on multi-level scales from "fully agree" to "disagree at all". By dichotomising these variable characteristics, you can clearly determine whether a person is extremist or not. If a whole battery of items is used to measure attitudes, it makes sense to carry out a factor analysis, as this makes it possible to check whether the items which, for example, are assumed to measure the construct "right-wing extremism" from a content point of view can be combined into a single factor.

The readiness for illegal political participation can be measured, for example, by items such as "In every democratic society there are conflicts that must be resolved by force" or "Those who do not act radically cannot realize the true ideals in politics" [154][88]. These items can be used in the same way as described above.

Descriptive analyses can be used to determine the proportion of violent extremists, political extremists, potential extremists and systemic conformists within a society. For the identification of societal risk potentials in relation to extremism, the consideration of the willingness to participate illegally in politics within a society is of great relevance. For it is true that the greater the proportion of violent extremists in a society, the more likely it is that there will be a future problem of extremism in this society. In addition to the extremists who are willing to use violence, the potential extremists also represent a problem group, since they would also be prepared to participate illegally in politics (if social changes were to take place).

Overall, such an anomie monitoring model could be used to make statements about how the opinion within a society on certain crime phenomena is shaped and whether the potential of societal problems with regard to crime exists in the future. Such an image of the societal mood would make it possible to

[87] Translated by the Author from German
[88] Translated by the author from German

draw conclusions about potential future developments with regard to crime and to plan and initiate measures against problematic predicted social developments at an early stage. The operational bonus also lies in being able to react to such outgrowths by adjusting or amending laws or by increasing the number of investigators in certain areas.

5.2.2.3 *Media Coverage and Terror*

The connection between media and terrorism has already been investigated many times in criminological and media research. Among the central questions are the extent to which public opinion on terrorism is influenced by media coverage of this crime phenomenon or the impact of terrorist attacks on media coverage. On the other hand, it is much less frequently examined whether and to what extent such media coverage increasingly entails follow-up acts.

The thesis that increased media coverage of terrorist attacks and terrorism leads to an increased number of terrorist attacks can be empirically tested. With the help of qualitative and quantitative content analyses, media content can be analysed in a first step. On this basis, it is possible to investigate correlations between media content and both public opinion and social events and phenomena by means of correlation or regression analyses. Some studies can be cited as examples which have already empirically proven this thesis.

Jetter [155] has, for example, investigated the effect of US media coverage on terrorist attacks by the al-Qaida terrorist network and has been able to confirm its hypothesis that the number of terrorist attacks is related to intensive media coverage of this topic. Specifically, he found that "[e]ach minute of Al-Qaeda coverage in a 30-minute news program encourages approximately one additional attack in the next seven days, on average" [155]. Jetter also confirms this hypothesis with his 2014 study, in which Jetter examined media coverage of terrorist attacks - in particular the New York Times - between 1998 and 2012: "The results suggest that media attention does indeed predict future terrorist activities" [156].

Beckmann et al. also found evidence that there is a connection between media coverage of terrorist attacks and their occurrence [157]. However, the results indicate that this mechanism differs in the short and medium term. In the short term (two months), media coverage has an influence on the quality of terrorist attacks, but not on quantity, which is plausible in view of the time required to plan terrorist attacks. In the medium term, however, an increasing number of terrorist attacks could be recorded [157].

Against this background it can be assumed: The more the media reports on terrorist attacks, the greater the risk of future terrorist attacks. This knowledge can be used for forecasting purposes. If there is an increased tendency in the media to report on terrorist attacks, the probability of subsequent acts increases considerably.

According to Rohner and Frey [158], the thesis that increased media coverage of terrorist attacks and terrorism leads to an increase in terrorist attacks can be explained by the fact that terrorist organisations schedule attacks in a way to generate maximum media attention and Jetter [155] adds that terrorist groups exploit an already existing media attention for this purpose. The so-called Werther effect, which originally goes back to Philips [159] and refers to imitative acts as a result of real and fictitious suicides, also provides explanatory power for the thesis mentioned. The Werther effect is based on the recognition

that the suicide described in Goethe's novel "The Sorrows of Young Werther" triggered a series of further suicides in Europe [160]. Philips [159] looked at the mimicry of coverage of suicide in daily newspapers in the UK and USA in the period 1947-1968 as part of a scientific investigation and found an increase in suicides among the general population as a result of media coverage of suicides of well-known personalities [160]. This finding can also be applied to the observed relationship between media coverage and terrorist attacks. For example, intensive reporting on terrorist attacks motivates and encourages potential assassins to carry out attacks as well.

5.2.2.4 *Network Analyses based on Social Media*

The Internet in general and social media in particular have developed in recent years into a dynamic form of interpersonal communication. Social networks such as Facebook, Twitter, Tumblr, Instagram, YouTube, etc. not only enable the user to communicate in real time, but also offer a continuous exchange of information. Due to the high reach and popularity of these platforms, their easy accessibility and anonymity, they are also used by criminals and radical, extremist and terrorist groups for their purposes such as spreading ideologies, promoting radicalisation and recruiting members [161].

Above all (closed) forums and chat rooms offer the opportunity to exchange ideas with like-minded people and to discuss ideologically charged topics, whereby the anonymity felt in these digital spaces can strengthen ideology and suggest a reduced feeling of danger before prosecution [162]:

"This also and especially applies to social networks and video sharing platforms such as YouTube, Facebook, Twitter, Instagram, WhatsApp, SnapChat etc., where information and entertainment formats mix with ideologically colored content and which are actively used by extremist movements to address (especially young) people worldwide" [162][89].

Platforms such as Facebook offer a variety of communication options, such as chat functions, open and closed groups as well as fan pages on various topics. Links, videos and photos can be posted in real time and by clicking the "Like" button it is possible to quickly and easily identify potential buyers [163].

An associated problem is the algorithm-based selection of displayed content, which is related to the content consumed by the user and is called a filter bubble. Users are increasingly being shown content that matches their individual online behaviour [162]. The danger of moving superficially in so-called echo chambers, in which one-sided contents are shared and disseminated by like-minded people [164], is increased, which has "both an *enabling* and an *accelerating* effect in connection with radicalisation processes" [162][90].

However, as already indicated, the communication of criminal groups and/or ideologically motivated extremists takes place not only in closed virtual spaces, but also on openly accessible sites and in public forums. This is of particular relevance for law enforcement agencies, as it allows to reconstruct who communicates with whom, when, where and how often, or communicated in the past. The evaluation of these contents represents an important added value not only for criminal prosecution, but also for

[89] Translated by the author from German
[90] Translated by the author from German

preventive purposes. The problem, however, is that this network-based analysis approach (see Figure 14) produces a large amount of data, whose evaluation is extremely time-consuming, which is why it only makes sense to analyse the metadata and topology and not the concrete content. For this type of analysis, it should be critically considered that personal data are also included.

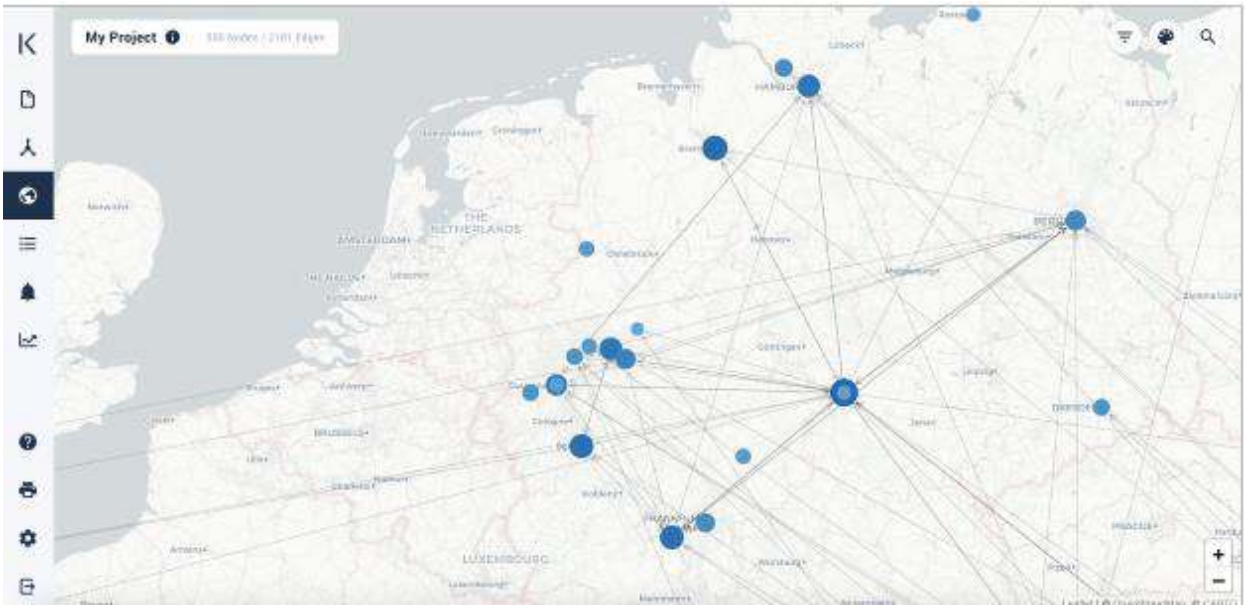

Figure 14: Network analysis91

On the basis of metadata, conclusions can be drawn about relationships between people. By identifying social networks made up of actors known as nodes and their relationships to each other, the so-called edges, it becomes possible to track down people who belong to an extremist network, or who participate in or plan extremist actions, but have not yet been on the police radar[92]. Given that Facebook alone had around 2.45 billion active users worldwide in the third quarter of 2019 [165] and that the Internet and social networks such as Facebook are regarded as an integral part of the communication structures of radical organisations [162], it can be assumed that the analysis of the communication of people on such platforms can make a promising contribution to the fight against terrorism. However, the fact that several hundred million people perform social activities in the social media every day also poses great challenges to law enforcement agencies worldwide:

„However, due to the dynamic nature of social media platforms, identifying […] content, locating users and predicting events by keyword-based search is overwhelmingly impractical. The volume of content being posted on social media platforms makes it challenging for security analysts to discover such content manually" [161].

Social media monitoring tools or network analysis tools can help in this regard. Systems such as KIVU (see Figure 14) can be used to identify people who, for example, follow radical or extremist groups or people

[91] KIVU
[92] But here it can also happen that innocent people are targeted by the police.

within a social network such as Facebook or Twitter and/or share or link their content. While such information does not provide any indication of the reason why a person follows another person or group (e.g. for journalistic reasons, sympathy or personal identification with the shared content or the people posting it), it does at least provide an opportunity to identify relevant persons of whom the law enforcement authorities have had no knowledge to date. In this context it should be noted that personal data (at least in Germany) may not be stored for preventive purposes without concrete grounds for suspicion. Social media monitoring tools and network analysis tools would therefore have to query data in real time (and without storage) when used. Information about systemically identified networks could thus be retrieved on a daily basis and changes such as the addition of new members or the withdrawal of previously active members of the network could be identified. The latter could, for example, be an indication of increased radicalisation and/or concrete planning of an attack. It is important that a system can simultaneously analyse several or different sources in order to gain a comprehensive overview of an actor's activities on the Internet.

The system PREDATA developed in the USA by the former CIA employee James Shinn also works with Open Source Intelligence. Every day, 10,000 selected Wikipedia pages, 50,000 You-Tube videos and 1,000 Twitter feeds are evaluated. With the help of scraper programs, historical events such as terrorist attacks are linked to Internet activities and patterns are searched. One pattern could be that before a terrorist attack the intensity of communication or the number of hits on certain pages increases significantly. If this is the case, "peaks" may indicate an imminent stop. PREDATA is able to calculate the probability of terrorism for each country. The system is a kind of seismograph for real-time events. However, it cannot predict the exact time or location of the crime. Against this background, the question arises what the operational benefit of the software ultimately is.

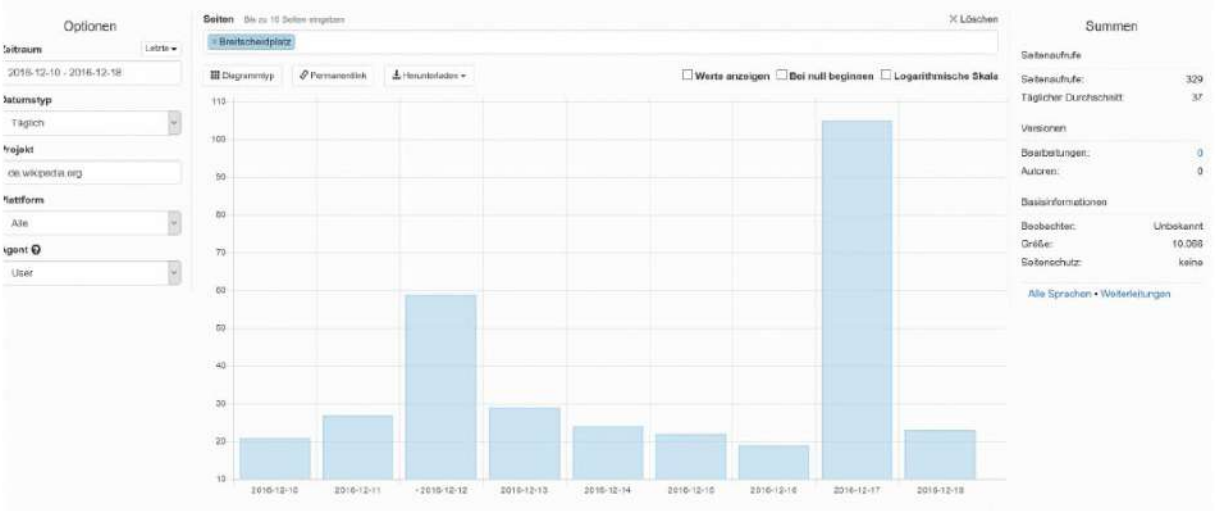

Figure 15: Example of the web activity on Wikipedia for the article "Breitscheidplatz" before the terror attack in Berlin on December 19th, 2016

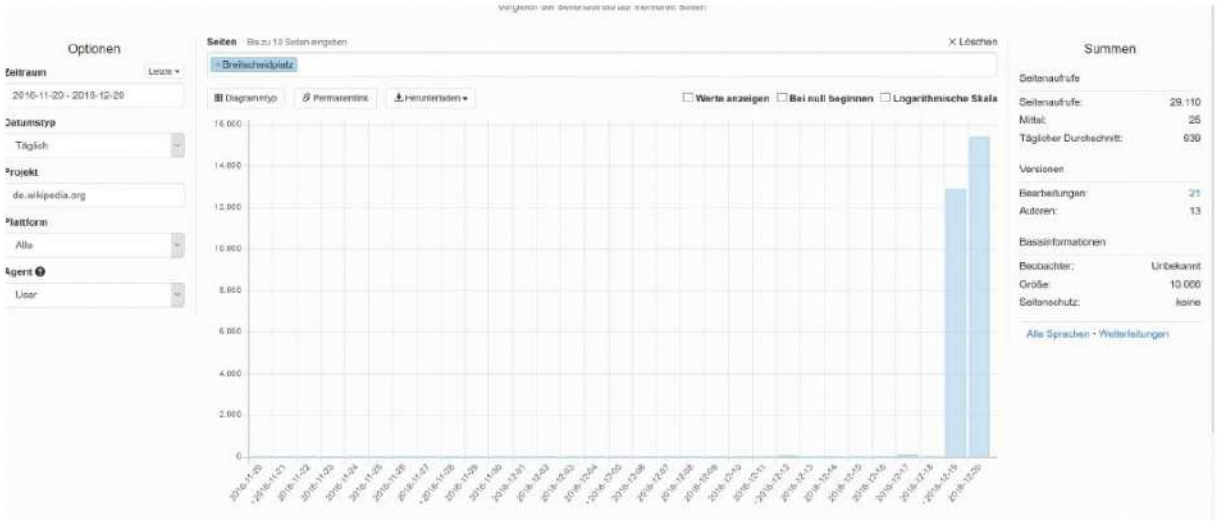

Figure 16: Example of the web activity on Wikipedia for the article "Breitscheidplatz" after the terrorist attack on December, 19th, 2016

The method will be illustrated briefly using the example of the attack at Breitscheidplatz on 19th December 2016 (see Figure 15 and Figure 16). For this the German Wikipedia page "Breitscheidplatz" was chosen. On 17th December 2016, two days before the attack, there was a clear increase in calls ("peak"). If such rashes were now registered on pages selected for daily analysis, it would be one of several indicators of a potential terrorist attack. On 19th December (day of the attack) and 20th December (one day after the attack) the number of appeals rose rapidly due to the topicality of the attack, which is explained by the national and international interest in the attack.

The work of Stefan Wuchty, Professor of Computer Science at the University of Miami, goes in a similar direction. He evaluates the behaviour of radical groups in freely accessible social networks. His "escalation parameter" measures the number of new sympathizer groups on the internet. He suspects that relevant political events are to be expected at the peak of such a development - either an attack or the outbreak of social unrest.

According to Wuchty, the problem is that platforms such as Facebook and Twitter are deleting radical content at an even faster rate, which makes analysis and thus the prediction or verification of his theses considerably more difficult [166].

5.2.2.5 *Trendanalysis*

A trend is a systematic increase or systematic decrease in a time series that also shows fluctuation or periodic fluctuations. A trend in a short time series can be fundamental or a temporary trend.

Trend analyses are used to obtain a view as realistic as possible of the future with regard to certain factors (e.g. offences) and thus to identify a trend. The regular and early assessment of the development of individual offences or phenomena enables deviations (e.g. increase or decrease of offences) to be

recognized very early and allows for timely action. In addition, this results in approaches for the analysis of possible reasons for significant increases or decreases.

Trends exist wherever a reference value can change and a direction of development emerges from this change. Especially natural sciences, technology and economics deal with trends in the form of time series. Trends are intended to provide the analyst with information about developments of a reference value within a certain time period and/or location in order to gain insights into certain processes. The starting point is first of all a trend free observation within a time period/location. Then the mean value and variance of a time series remain constant over an entire observation period, this is called stationarity. Only non-stationary time series are subject to a trend development and therefore do not have a fixed mean value [1]. Here, a distinction is made between trend stationary time series with deterministic trend and differential stationary time series with purely random stochastic trends (Wikipedia).

In PREVISION primarily trends are worked out in the context of text analyses. This is especially done in the context of UC 2 (Identification of Radicalisation and Terrorist Propaganda). Available and self-created texts from various sources are used as data basis.

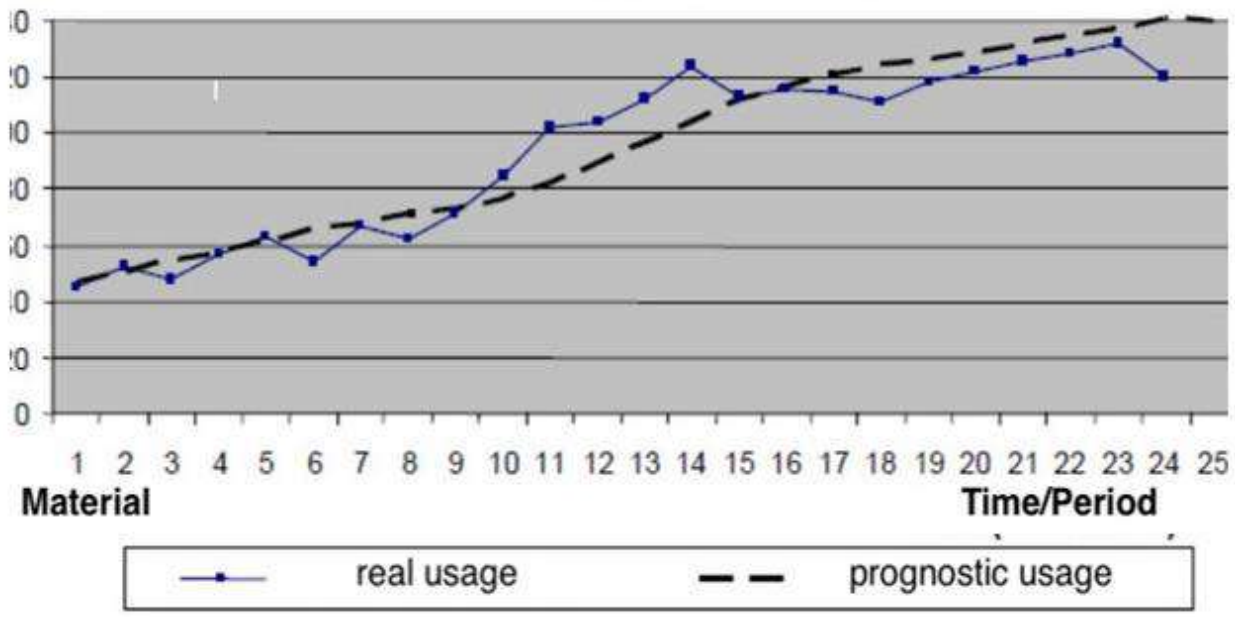

Figure 17: Example of a trend visualization - graph

Relevant methods are

- Monitoring (directed observation of certain early warning indicators)
- Scanning (undirected search for indications of influential developments)
- Scenario technique (The scenario technique is a procedure, in order to project several conceivable developments for a certain fixed question and its environment into the future. All known possible influencing variables and their interrelationships are taken into account. The result of the considerations is the description of many possible situations and the representation of the development and the way

to it. The developed scenario can then form the basis for the development of a strategy or existing strategies can be reviewed with regard to the scenario (Handbuch der Polizeilichen Auswertung, BKA 2007).

However, trend analyses can also be very helpful in the field of organized criminality/artifical theft (UC 5).

Short description of a possible approach to the phenomenon of art theft:

Terrorist groups such as the IS finance themselves to a not inconsiderable extent through the sale of antique art treasures.

The terrorist militia earns millions with robbery excavations, especially in Syria and Iraq, and with the sale of antiques on the international art market.

Experts assume that ¾ of the antiquities offered on online campaigns come from robbery excavations in Syria and Iraq.

It is a billion-dollar business. There are experts who classify the illegal art trade as the third most lucrative business after drugs and weapons. Others assume an annual turnover of 6-8 billion dollars. There are hardly any statistics on the extent of the trade.

• What are the reasons:

Although there is an export ban on such antiques, a state must officially assert its property rights. For states that are in a state of war, this is virtually impossible. Moreover, neither the law enforcement agencies nor politicians, nor dealers, auction houses and buyers have any interest in systematic criminal prosecution.

Germany is a relevant reloading point for looted art. Munich is a center for looted art. There are therefore only estimates of how many looted art objects are currently in circulation (dark field cannot be quantified).

Actually, traders would need a proof of origin or an export license. An export certificate is also planned. As a rule, these documents are not available. Law enforcement is very negligent, even if the art objects can be clearly identified as looted art.

• Scenario:

Predators sell the antiquities for small money to local fences.

Middlemen collect the pieces and sell them to dealers abroad. There they are stored safely. Via action houses/antique dealers/online auctions they go to private owners. The sellers often pretend that the offered pieces come from private collections.

Example for trade: From Iraq via Turkey via the free port of Dubai (where the antiques get fake papers) to Germany.

• Thesis:

With the increase in warlike conflicts in countries with relevant art treasures, the trade in looted art is also on the rise.

Which numbers can be relevant:

- Number of confiscations
- Number of determinations
- Number of criminal proceedings

Another factor is the number of areas characterized by riots and art treasures. The more such areas there are, the more cases of looted art will be. Similar to drug trafficking, looted art is a victimless crime (affected states = abstract victim = do not report; make no claims); the proactive action of law enforcement agencies is a major factor in clearing the dark field.

• Target:

- The goal is to combat looting and trafficking of cultural heritage as a means of financing terrorism.
- Accelerating the discovery of artifacts and helping to reduce the number of looted archaeological sites.
- Detect robbery artifacts in a shorter time with greater accuracy.
- Crowdsourcing system (different experts contribute their expertise to the system)

• Content of the application/software solution:

- Images of antiquities from the red list are added to the database. The images can be used for crawling in the WWW, social networks and darknet.
- Images can be georeferenced, i.e. the place/country of origin can be displayed.
- Trade routes can be entered / visualized
- Creation of a database for legislation

6. Concepts of Predictive Policing Tools

6.1 Person-related Predictive Policing System

In the PREVISION project, various use cases and related functionalities were described by the participating authorities (LEAs). After a detailed analysis of the use cases it turned out that there are only a few requirements related to the field of "Predictive Policing". Mainly, functionalities from the areas "Investigation and search support" are concerned. In particular, to meet the requirements by the LEAs regarding the detection, prediction and fight against radicalisation and terrorism formulated in use case 2 "Radicalisation detection & terrorist threat prevention", the use of Predictive Policing is beneficial.

Therefore, IfmPt developed solutions and applications referring to the area of "Recognition/Detection and Prediction of Radicalisation Processes" in the digital world. Specifically, IfmPt provides the concepts of a software solution with the aim of enabling LEAs to recognise radicalisation processes and to assess the radicalisation level and risk potential of persons, who are already known as endangerers to security authorities. Thus, it is a person-related predictive policing system.

The risk assessment should be based on the evaluation of various sources. On the one hand, information originating from investigations or provided by official authorities are taken into account, and on the other hand, information about the relevant persons, that are available online, including their Internet activity on social media (especially the linguistic communication), are included. Thus, an approach of forensic linguistics is pursued here. This is because a linguistic approach can and should play a central role in the assessment of the risk potential of groups and also individuals [175].

"[T]he importance of radicalisation in social media is growing, as the Internet offers extremist groups a (wide) range of platforms for the exchange of information and the expression of opinions. It also facilitates the dissemination of (online) hate speech and extremist propaganda" [176][93]. In this context, however, it should be noted that, "[n]ot everyone who shares an ideology or idea on the net is willing to go down the path of radicalisation to the use of violence. However, the supposed anonymity of the Net often leads to linguistic brutalization and to a lack of respect for fellow human beings. Language is used to share ideas and ideologies and even to call for the use of violence, for example against immigrants, people of other faiths or other minorities" [176][94].

Even if hate speech is mostly outside the justiciable range, hate statements are nevertheless problematic, "because they can radicalize people or groups for example with wrong facts" [176][95]. With the help of tools of linguistic IT forensics and machine learning, an automated recognition and containment of hate speech and the radicalisation that builds up is possible before violence is used. In this context, research has shown that not only a distinction must be made between neutral postings and hate postings, but also that algorithms used must be able to recognize the difference between "only" offensive speech and hate speech [176].

[93] Translated by the author from German
[94] Translated by the author from German
[95] Translated by the author from German

With the help of the person-related predictive policing system it should be possible to (automatically) find problematic communication of endangerers on social media and to evaluate it.

Besides information about the social media activity of endangerers, further information that is relevant for the assessment of the degree of radicalisation of those persons should be found on the Internet and should also be taken into account in the evaluation of their radicalisation level.

Radicalisations are known from different motives and ideologies. In the PREVISION project we focused on the detection and prediction of radicalisation processes in the context of Islamism. This is also in direct relation to use case 2[96]. In terms of language and terminology, there is a concentration on “English”, as this is also the project language. The software solution presented in the following is to be understood as an example of an implementation of requirements of the LEAs. The presented methods and functionalities can be adapted to other ideologies (e.g. right-wing and left-wing extremism) and languages (e.g. Arabic).

Various data are necessary both for the conceptual design of the planned software solution and its implementation. For the identification of indicators that point to problematic radicalisation processes and thus can be used to assess the risk of individuals, data on biographies of endangerers, extremists and terrorists is needed. As a result of non-existent or unavailable data, which were originally intended to be provided by the LEAs and which unavailability is also due to ethical EU regulations and restrictions, the necessary data had to be collected and datasets had to be created by IfmPt with great effort. Therefore, biographical data were collected from known extremists, radicals and terrorists using public sources in order – as already mentioned – to derive indicators for the assessment of radicalisation processes on the basis of these personagrams (see attachment1_Biographies example).[97] A further essential step was the creation of taxonomies (. The taxonomies are the basis for the detection of radical content and phrases in texts. It was intended to use taxonomies of a similar project (TENSOR). For security and administrative reasons, the taxonomies created in the scope of TENSOR and used in relation to the detection of radicalisation processes on the net could not be used in PREVISION. As a result new ones had to be created. For more details, see Task 4.2 in WP 4 in connection with the Task Force "Predictive Policing and Radicalization".

In order to realise the aforementioned social media monitoring, relevant data of social media accounts and postings is needed to configurate appropriate algorithms. As a result of the applicable data protection regulations, it was not possible to use real accounts. Hence, synthetic or pseudonymised accounts were used to demonstrate the mode of operation.

Functionality of the person-related predictive policing system

Basically, the following goals are pursued with the software solution:

[96] Furthermore, relevant data and necessary resources on other ideologies, such as right-wing or left-wing extremism, were not available and an additional elaboration of these was an unmanageable workload.

[97] Since, as mentioned in the previous chapters, socio-demographic characteristics of a person alone are not very meaningful and do not provide information about the risk he or she poses to society, variables that indicate concrete actions of persons were also taken into account.

1. Gaining knowledge about radicalisation processes of known endangerers and its evaluation.
2. Gaining knowledge about possible radicals/terrorists that are not yet on the radar of police authorities.

In order to achieve these goals, various functionalities should be ensured. These are shown in the following visualized workflow.

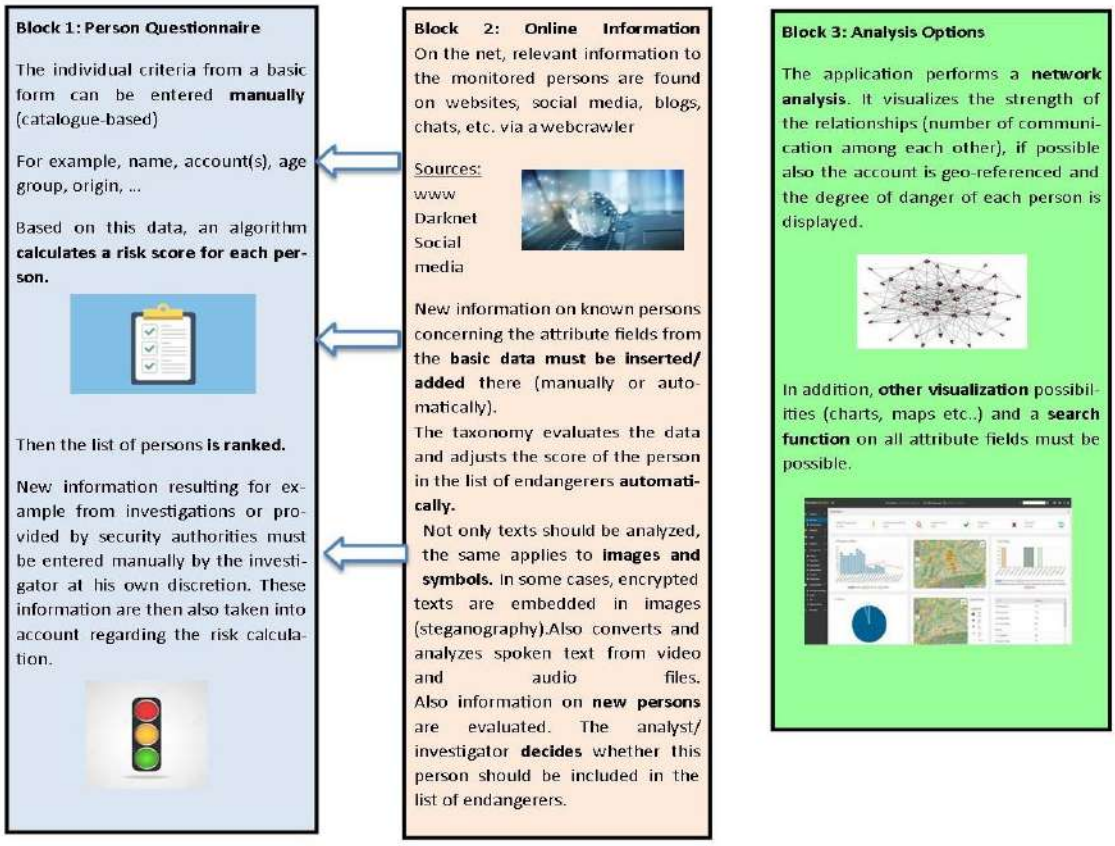

Figure 18: person-related predictive policing system

First Block: Person Questionnaire

The so-called "lists of endangerers" available to security authorities is a basis for this functionality. These are persons who are already under investigation by the police and who are already subject to a certain monitoring. At present, however, this is largely done manually and involves a great deal of effort.

It is intended that in the operational use of the system, basic information on the personal characteristics of the endangerers and information from previous investigations etc. are recorded in the system by the investigator. For this purpose a “Person Questionnaire” was designed.

In this “Person Questionnaire”, information on predefined risk factors (e.g. criminal records, military training, psychological abnormalities etc.), which are e.g. available from investigations, will be entered in individual attribute fields, which on the one hand allows an easy recording and on the other hand ensures

standardization. This guarantees that each person is recorded according to the same rules and terms, which in turn is indispensable for later analyses. Each attribute field (and the possible entry options) is linked to a specific weighting value. An algorithm calculates a risk score on the basis of those values and the person is classified in terms of his or her radicalisation level. As a result, the end user receives a ranked hit list on which persons are sorted in descending order with regards to their estimated risk.

This so-called basic data must always be updated. If, for example, the investigator obtains new information from investigations or information from other authorities, this information must be stored in the questionnaire.

Second Block: Online Information

A further functionality of the system is intended to ensure an extensive knowledge acquisition from all available sources. This functionality is that the system scans various online sources (www, social media platforms, chats, blogs, darknet etc.) for relevant information on the endangerers. This is done with Web Crawlers that search for keywords, phrases etc.

The results are provided according to defined output formats and then analysed using software solutions. The acquired data is "decomposed" in terms of content, i.e. groups are formed (extraction of entities):

- Texts
- Accounts
- E-mail addresses
- Phone numbers
- IP addresses
- Geographical indications
- Metadata
- Pictures, symbols
- Etc.

The texts are analysed according to the aforementioned predefined risk factors, by checking whether the risk factors – indicating radicality – are fulfilled. Here, the created taxonomies are used. And also, a morphological analysis must be applied. Also converts and analyses spoken text from video and audio files.

Images and symbols should also be included in the analysis. These can also give an indication of radicalisation processes. A special feature here is steganography, where texts are embedded in images and thus corresponding messages are conveyed.

All information found are assigned to the specific person (see block 1) and are evaluated by an algorithm. The risk score of the person is adjusted accordingly.

In addition to gaining knowledge about known endangerers, this strategy can also be used to find information about people or accounts, that investigators had not on their radar. It is at the discretion of the investigator whether these persons are included in the list (block 1) or not.

Persons are assessed on the basis of the following risk factors:

Table 10: Risk factors - Person-related Predictive Policing System

Risk factor	Description	Weighting
Concrete announcement of violence	The person has announced a concrete exercise of violence.	
Letter of confession/confessor video	There is a confessional letter or confessional video in which the exercise of an act by the person is announced.	
Directly communicated threat	The person has communicated concrete threats against other persons, groups, buildings etc.	
Direct contact with violent extremists	The person has contact (virtual or physical) with extremists.	
Travel abroad for non-governmental training and fighting	The person has already started or is planning tris abroad for non-governmental training and fighting.	
Setting up a manifest	The person has created and distributed an manifest.	
Glorification of extremist acts of violence	The person glorifies extremist acts of violence, e.g. as part of his or her online communication.	
Concern with assassin(s)	The person is concerned with the biographies and actions of assassin(s).	
Military or paramilitary education or training	The person has participated in military or paramilitary education.	
User of extremist websites	The person uses extremist and/or radical websites.	
Signs of suicidal tendencies	The person shows signs of suicidal tendencies, e.g. via verbal or written statements.	
Access to weapons	The person has access to weapons or has built him-/herself weapons.	

Previous conviction for politically motivated acts of violence	The person has a criminal record of politically motivated acts of violence.	
Support through (virtual) community	The person is supported in his or her views by a (virtual) community.	
Sex	Sex of the person.	
Age	Age of the person.	
Use of hate speech	The person uses in his or her written or spoken communication hate speech.	
Attachment to ideology that justifies violence	The person shows a personal attachment to an ideology that justifies and legitimises the use of violence.	
Rejecting violence to achieve political goals	The person rejects the use of violence to achieve political goals.	
Person disappeared/ stay unknown	The person has disappeared/ His or her whereabouts are unknown.	
Own postings of extremist content	The person posts extremist content on social media channels, blogs, chats etc.	
Sharing of extremist content	The person shares extremist content from other sources on social media channels, blogs, chats etc.	
Liking of extremist content	The person likes extremist content from other sources.	
Situational alienation	The person shows signs of situational alienation.	
Biographical availability	The person shows a biographical availability, i.e. he/she lives no longer with his/her parents, but has not yet started a family of his/her own.	

Third Block: Analysis Options

The third area contains functionalities for statistical analysis, evaluation, search and visualization. Various statistical evaluation options (mainly descriptive statistics) can be used by the investigators, for example, to find out to which age group people who are considered to be risky mainly belong or whether there are similarities in socio-demographic characteristics. Network analyses can also be performed, but these are mainly concerned with the visualization of communication networks, showing who communicates how often with whom.

It must be possible to produce charts and statistics, and a geographical visualization is also required, for example to show spatial information (whereabouts, geodata of IPs, etc.).

Note:

An essential feature of the software solution is that the results are transparent and comprehensible for the investigator. This is particularly important with regard to subsequent police measures, but also with regard to the acceptance of such "prediction systems".

6.2 Web-Monitoring System

In addition to the person-related monitoring system, which is described in the previous chapter, IfmPt has also developed a concept for identifying and monitoring radical and extremist websites. As it emanates from (especially) use case 2, the identification of radicalization and terrorist propaganda online is a crucial aim of PREVISION. However, the system presented here is not only aimed to identify websites with radical content but also to classify them according to their level of radicalisation and extremism. In order to achieve these goals, the basic functionality of the web-monitoring system is similar to the functionality of the person-related predictive policing system described above. But as this system is not about assessing the risk potential of a person, but about detecting extremist propaganda on websites and assessing their level of radicalisation, no persons are used as a basis. Rather, known websites already classified as extremist or radical are used as starting points for the detection. With the identification of radical or extremist websites and a possible resulting dissociation of these, it can be achieved that people cannot radicalise themselves by using these websites.

A WebCrawler is used to search for extremist and radical websites. The aim is to find websites with radical content that are not yet on the radar of security authorities. For this procedure the WebCrawler requires starting points. Therefore IfmPt has developed a list of URLs of websites on the world wide web and on social media. These are websites that are classified as extremist by official security agencies or that are identified by own research. Furthermore, these websites are in English language and are active and openly accessible to users.

The further procedure is that crawled websites are analysed in order to determine whether specific risk factors apply to the websites. Each website is therefore assessed by means of a catalogue of risk factors that are weighted differently. Based on these factors, a risk score is then calculated, which indicates how radical or extremist the website is to be classified.

The workflow of the web-monitoring system can be visualized as follows:

Figure 19: Workflow - Web-Monitoring System

The following risk factors are used to classify the websites and to determine their level of extremism:

Table 11: Risk Factors - Web-Monitoring System

Risk factor	Description	Weighting
Website of a prohibited group/organisation	It is a website of a prohibited group/organization	
Calls for violence	The websites calls for violence against ethnic minorities and marginalised social groups.	
Glorification of terrorist actions or politically motivated acts of violence	The websites glorifies terrorist actions or politically motivated acts of violence.	
Anticonstitutional characteristics	The website shows anticonstitutional characteristics.	
Call for departure to battle zone	The websites calls for a departure to battle zones.	
Website denies holocaust	The websites deny the holocaust.	

Website is linked with websites of prohibited groups/antidemocratic content	The website is linked to other websites of prohibited groups or antidemocratic content.	

By using the system, the end-user receives a ranked hitlist of websites, sorted in descending order of their potential for extremism. For websites for which immediate action by security agencies is required (e.g. detaining the operators, shutting down the page, etc.), an alert is issued.

This scoring system can be used by the end-users to monitor the activity on websites already known to them, to monitor (new) websites that were previously not on their radar and to be able to identify any relevant actors communicating on these websites. With the daily updated information provided by this system it is possible to shut down websites and/or stop relevant actors. Persons who are identified in this way can also be evaluated and observed with the described person-related assistance system.

6.3 Network Analysis

With the assistance of network analysis, relationships between individuals, groups and institutions can be identified and analysed. In the context of Prevision, the analysis is aimed primarily at actors out of the extremist environment and the field of organized crime. Often actors from these two phenomena interact with each other. For example, goods such as drugs, oil or looted art are offered by extremist groups on the illegal market. Organized crime groups then resell these goods. Terrorist organizations use the money they make to finance their armed fights, among other things. But the path also goes the other way round. Weapons are not sold by organized crime groups to terrorist groups. Organized Crime (OC) groups also support terrorist organizations in, among other things, smuggling sympathizers into combat zones.

Social network analysis has become a standard tool of police analysis. "SNA is typically employed by Law Enforcement Agencies (LEAs) to analyse criminal networks, investigate the relations among criminals, and evaluate the effectiveness of law enforcement interventions aimed at disrupting criminal networks.

When dealing with criminal networks, a distinction must be made between virtual and real networks. In the modern world, individuals exchange information via both i.e. real (face to face) and virtual networks (e.g. WhatsApp, Telegram, Facebook, Twitter). But there are also networks whose members communicate exclusively via social media. Extremist groups in particular use the diverse opportunities offered by the digital world to exchange information across borders. For example, other people are usually involved in the run-up to the acts of so-called "lone wolves"; only the act is carried out by a single person. In the modern world, physical contact is no longer necessarily required to form a criminal network. Behind every "lone wolf" there is an ideological pack.

As already mentioned, the WWW, the Dark Net and social media play an increasingly important role in the fight against terrorism and organized crime. In the field of terrorism, this is particularly true with regard to recruitment, radicalization and crime planning; in the field of organized crime, it is true with regard to money laundering and cybercrime and in the trade in illegal goods and services.

What operational added value does network analysis have for law enforcement authorities? People are social beings. They need and seek contact with others. Consequently, all people move in social networks. Criminals are no exception in this respect. A social network can be defined as a limited number of individuals who maintain social relationships with each other. "Social networks are graphically represented by dots and lines; the dots are the people, the lines are the social relationships.

Granovetter distinguishes between "strong ties" and "weak ties". Strong ties are strong relationships, e.g. friendships, whereas weak ties are rather weak relationships, e.g. loose acquaintances. "Absent ties" denote missing relationships. According to Granovetter, one can assume the following premise: If A has a strong relationship to B and C, then the probability is very high that B and C also have a strong relationship to each other, even if this relationship is not yet recognizable or proven. He calls such a constellation "forbidden triad". Networks with strong ties cultivate an intensive relationship among each other, which, for criminological analysis, allows the conclusion that they act and think similarly.

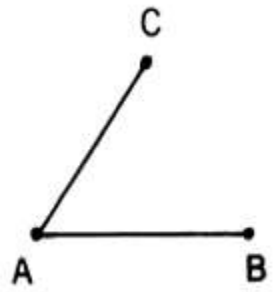

Figure 20: Forbidden Triad (Granovetter 1973, S. 1363) [177]

But how do you find criminal networks in the digital world? One way can be to use crawlers to search for relevant content (prohibited symbols, images, language, etc.) and thus identify incriminated chats. Once such a network has been disclosed, information can be skimmed off, providing clues about individual actors and the size and structure of the network.

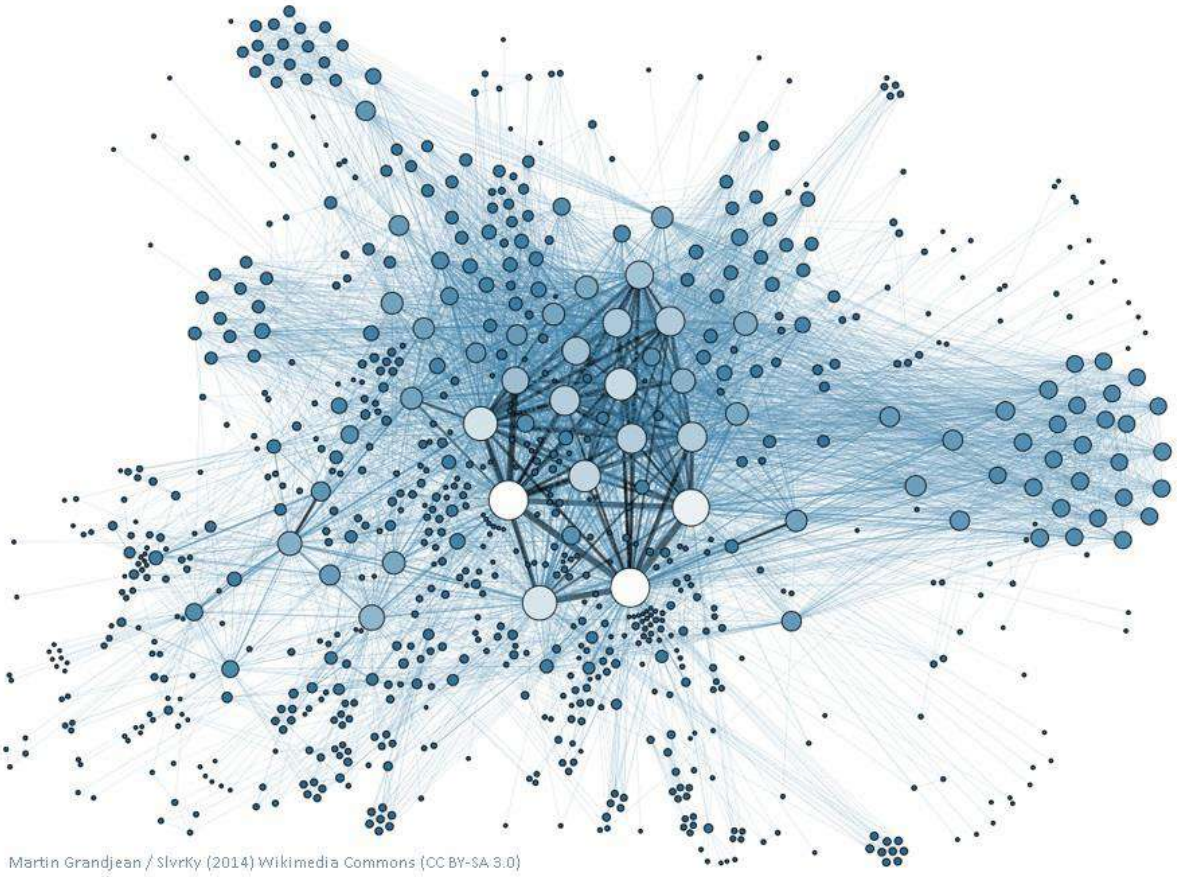

Figure 19: Visualization of an analysis of social networks - Ferguson 2018 [178]

Another approach is the ego-centred network analysis. Starting from a concrete person ("ego"), relationships to other people ("alter") can be established. In a further step, an "alter" can also function as an "ego"; and thus, the analysis of a network can be continuously expanded.

In order to evade police measures, criminal gangs increasingly rely on modern encryption technology to conceal their activities from the police. One example of this was the short message service Encrochat. This service was used almost exclusively for criminal activities. If law enforcement agencies succeed in penetrating these services, not only a variety of crimes but also criminal network structures can be uncovered.

What is the added value of network analysis for the LEAs involved in Prevision. The primary goal should be to identify extremist/criminal networks. Furthermore, the most active and prominent actors are to be named, and the size and scope of the network is to be analysed. It is of utmost importance to identify actors that are not yet in the focus of law enforcement agencies.

The density of a network says a lot about the influence on or control of the network on individual actors. The higher the density, the greater the influence and control. In addition, scoring could be used to determine the risk potential of a network, especially with regards to active threat situations (calls for violence, confessional videos, etc.)

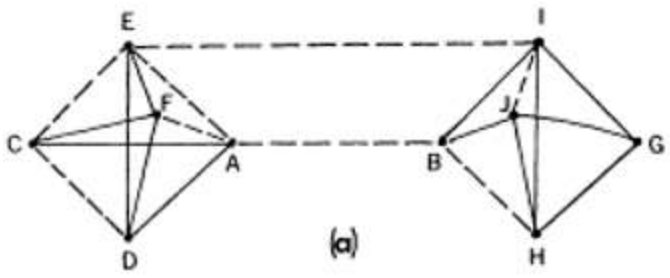

Figure 20: Local bridges (Granovetter 1973, S. 1365) [177]

Of particular interest in this context are the so-called "bridge builders", i.e. people who establish connections between two networks. In general, not all persons have the same influence on the functionality of a network in terms of their human and social capital. When breaking up extremist/criminal networks, the primary goal should be to identify and eliminate the main actors. Criminals rely on short lines of communication. If this flow of information can be disrupted in the long term, the network's ability to act is massively reduced. The goal must therefore be to find the actors who are responsible for most internal communication (intermediate centrality). If the five percent of actors with the highest intermediate centrality are eliminated, up to 70 percent of communication is paralyzed. The network is therefore virtually incapable to operate.

„Our SNA results can be directly translated onto law enforcement actions, considering that we are now able to efficiently identify the top 5% most trusted affiliates (i.e., the ones typically employed as intermediaries between bosses and the other members). In turn, we can virtually neutralize the clans' internal communication infrastructure by getting the trusted affiliates in custody. Intuitively, whenever arrests can be made in block (raids), that would further impair the ability of the criminal communication network to be re-established. "[179]

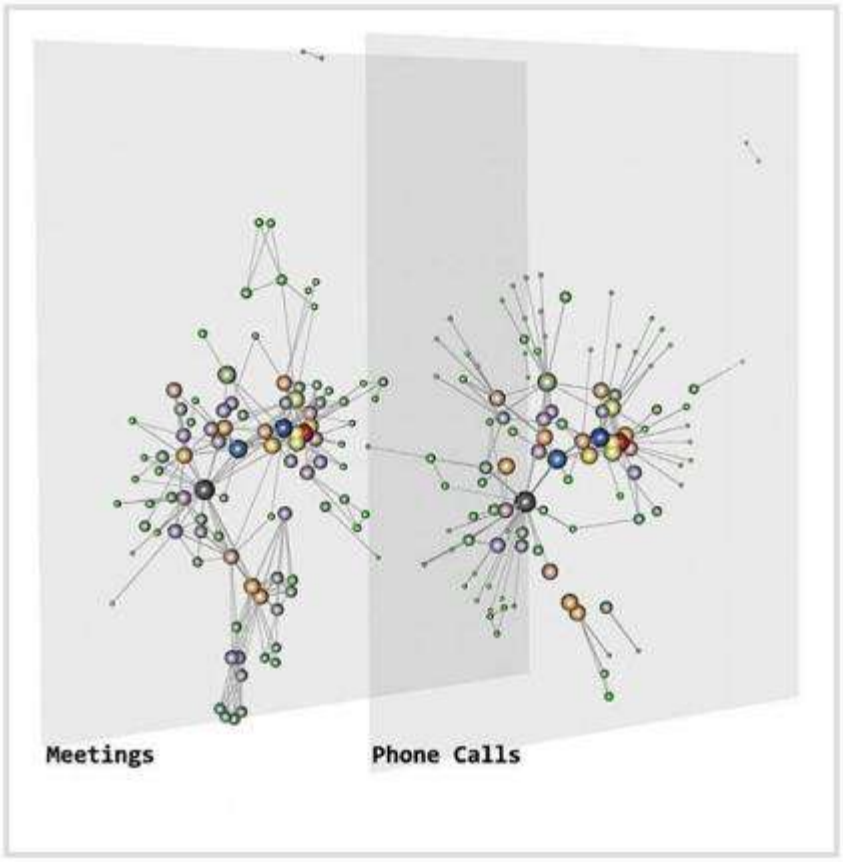

Figure 21: Personal meetings and telephone calls of Cosa Nostra members Klaubert 2020 [180]

The network-based analysis approach is therefore about who communicates with whom, when, where, how and how often. In this way, important insights can be gained about (potential) crimes and offenders. The more different data sources are integrated, the higher the quality of the analysis results.

7. Ethical and Data Protection Aspects of Predictive Policing

Working with predictive policing software is often associated with prejudices. Their use is always accompanied by the consideration of moral and ethical aspects, which are referred to below.

With the use of spatial predictive policing models, there is a risk that people who temporarily stay in or live in a space declared by the software as risk area have to fear being stigmatized across the board as potential criminals. This is mainly due to the increased control by the police. Such an approach can lead to a consolidation of prejudice and discrimination: If the police patrols more frequently in a risk area, more crime is registered there. This in turn would be more strongly weighted in future forecasts.

In addition, police control practices are selective. It is not unusual for (individual and institutional) stereotypes to be reproduced in this way. In this context, criticism is voiced that these stereotypes are reflected in police data and can ultimately be incorporated into the algorithms used to predict crime. To make matters worse, when using AI and ML, a point can be reached where the developers or analysts can no longer understand the results of the forecasting software. In this context, critics point out that police measures are then taken on the basis of a "black box". In addition, the collection of large amounts of data (keyword: BIG DATA) from different data sources increases the danger of spurious correlations, i.e. statistical correlations that are technically unfounded.

The use of personal predictive policing approaches is accompanied by the consideration of various ethical and moral aspects, whereby criticism often refers to the classification of persons as extremists or "endangerers". According to critics, this can lead to serious invasions of the privacy of those concerned (monitoring of chat histories, observation, etc.), because the probability that all predictions are correct is almost unrealistic. Even a success rate of 95 percent would result in five percent of those affected being wrongly suspected. In monitoring the social media of suspects or people classified as "dangerous", innocent people can always be included. Here the disproportionality is criticized or the danger is seen that people are falsely accused by the security authorities. There are also concerns that collected data is not promptly or completely deleted and thus also innocent persons remain permanently in the system.

When personal data is collected, citizens can be put on a so-called "heat list" simply because they are an acquaintance of a person classified as dangerous, but have never been convicted of any criminal offence themselves. Critics see this as criminalizing innocent people, whose stigmatization could also have an impact on other areas of their life.

A comprehensive surveillance of social media using crawlers and forensic linguistics would be a form of surveillance without cause. Although a message would only appear once a suspicious chat or communication was identified, critics reject the use of such software for reasons of proportionality.

Furthermore, the terms "extremist" and "terrorist" are used in an inflationary way. Autocracies and dictatorships instrumentalize these terms in order to discredit political dissenters (this can be seen in examples such as Turkey or Hong Kong).

In addition, critics point out that it has not been sufficiently clarified which (parliamentary) supervisory bodies monitor the use of predictive policing software. In this context, it is also a matter of debate whether

comprehensive security justifies the "transparent man". Critics argue that "freedom" and "security" should always be in a reasonable relationship to each other. After all, the benefits of predictive policing in protecting citizens from crime can also serve as a pretext for "socially disciplining" people, which can even result in social exclusion, as in China, for example.

In addition, voices of data protectionists are being raised in the field of predictive policing. They fear that the amount of data collected by the security authorities could fall into unauthorized hands. It has already happened in the past that authorities have been victims of hacker attacks, which makes it particularly important to protect such sensitive data.

Despite the criticism mentioned above, the use of predictive policing also has advantages for security authorities and thus ultimately for citizens. Predictive Policing serves to reduce complexity. It enables people to analyse large amounts of data in a timely manner and identify patterns contained within it, which would be virtually impossible without the use of such technology. In addition, AI and ML can be used to find patterns and identify relationships that would not have been discovered manually. Likewise, algorithms do not know prejudices and stereotypes, they are not racist or discriminatory. Thus, the more racism and discrimination are suppressed from cop culture, the less these aspects play a role in the prognosis by algorithms. Predictive policing also considerably shortens the action time. Data and analysis results are available more quickly, so that decisions can be made more quickly and measures implemented more quickly. Finally, scientific research has proven that software solutions are more effective than humans in creating forecasts.

As a result of the sensitivity of the data required for the development of software solutions, different data sources and types were used.

<u>These are divided into:</u>

- Publicly available resources
    - Many technical partners have these and use them for training and evaluation of various (statistic-based) models (e.g. resources from LDC or ELRA)
- Data collected from open sources
    - Data from social media available through public APIs (e.g. Twitter’s streaming API, Facebook Graph-API)
- Data from other (research) projects
    - Resources which have been created by other (research) projects and which are available to partners
- Resources created and held by individual technical partners
    - Data with technical partners which they have created themselves, e.g. when working on a language where no data is available from UC 1) (or too expensive)
    - These can be shared between project partners or be “private” to individual partners and not shared
- Simulated data

- Data simulated by (technical) partners using input from LEAs and experts in order to be able to develop, evaluate, improve algorithms and methods
- Expertise for simulation would come from LEAs and experts and enable technical partners to simulate things in a realistic manner

• Resources from LEAs from cold cases

- Data from cold cases, anonymized and in a state which allows LEAs to pass them on to (technical) project partners. These data are not only realistic, but they are the closest type to the “real thing” for non-LEA members of the consortium

8. Summary and conclusions

In today's police work of investigators and analysts, more and more holistic IT evaluation and query solutions are demanded. These can be subsumed under the term "platform technology". This represents a system reversal, because the data is no longer kept in oversized databases but remains in its previous source systems. Above this lies a level of software solutions that recognize and show connections under consideration of access and authorisation concepts. This can also be coupled with alarm functions that immediately indicate new findings. In addition, a variety of search options and visualisations up to the integration of “other” software are possible. This ensures that the knowledge gained here can also be compared with the existing information in the LEA’s own databases.

It must also be possible to trigger this knowledge acquisition according to fixed or freely definable times (e.g. once a day, every 2 hours, for a specific reason).

This makes it possible, for example, to make a statement about the radicalization process on the basis of the knowledge gained and the methods/algorithms used and the associated software solutions. This also serves as a basis for further police measures.

The aim of this paper was to elaborate the value of predictive policing in the fight against crime - primarily in the areas of cybercrime, organised crime and terrorism - and to present possible applications of different predictive models to the use cases formulated within the framework of PREVISION. Predictive policing is the consistent further development of police strategies for the prevention of crime, not only in the area of mass crime, but also in the fight against cybercrime, organised crime and terrorist threats. The EU-funded project PREVISION picks up on this development by developing innovative software solutions to support police forces in identifying and combating future threats at an early stage. In the context of the present elaboration, the value of social science and criminological theories was addressed in addition to empirical findings and already existing methods and software solutions.

When developing predictive policing software, it should be ensured that it is theory-driven rather than purely data-driven, because theory-driven approaches promise higher quality output. Without sociological, psychological and criminological theses and theories, meaningful predictive policing is hardly conceivable. In this respect, a detailed theoretical discussion of the topic is also indispensable in this project. Furthermore, the methodologies used should be transparent and comprehensible for the end users, otherwise the necessary acceptance by the users might be lacking. At this point, the use cases formulated by the end users will be discussed in detail.

It is noticeable that the LEAs involved often outline technical solutions in the use cases they describe, which are primarily investigative support technologies or investigative tools. In particular, there is a growing demand for video surveillance with face recognition and real-time data comparison, especially at neuralgic locations such as airports, train stations or football stadiums. One example is the use case 1 "Soft targets protection - Attempted terrorist attack at stadium", in which terrorists plan an attack with explosives and vehicles on visitors to a football match. One of the aims here is to prevent perpetrators from bringing explosives into the stadium unnoticed. It is also aimed to identify suspicious persons and vehicles in real time using modern video surveillance and face recognition. In the event of an attack,

existing data material must be evaluated quickly, for example in order to be able to initiate search measures quickly.

Such technical solutions are currently being worked on throughout the world, including in the European Union. For instance, the contactless identification of body-worn explosives is the objective of the POLINEX project (portal with a cost-effective IMS network for the contactless detection of body-worn explosives). Within the scope of detection methods, explosives, e.g. in the form of explosive belts or explosive cases, are to be detected even in moving persons. This can be realized with the help of portals equipped with sensors, e.g. in the form of passage tunnels at airports [167].

The German-Austrian cooperation project FLORIDA is concerned with the evaluation of video material. This is a system for visual and auditory analysis of image and video mass data in order to reconstruct the course of events more quickly and to identify suspects more quickly [168]. The importance of video surveillance also emerges from the Use Case 2 "Radicalisation & terrorist threat prevention". Fraunhofer IOSB also recognized the great importance of video surveillance for public safety and developed the NEST, DigLT and ivisX systems. In this context, the "Video Surveillance Mannheim Project" is worth mentioning. Since 2018, intelligent, algorithm-based video surveillance has been used in Mannheim in public areas with the aim of detecting police-relevant movements such as violent assaults [169]. In Berlin, biometric face recognition was also successfully tested as a supporting tool for police searches at the Berlin Südkreuz station as part of the "Biometric Face Recognition" project of the Federal Police Headquarters in Potsdam as part of the testing of systems for intelligent video analysis [170].

In addition to video surveillance and face recognition, the importance of analysing social networks and Internet communication is also addressed in the use cases "Soft target protection - Attempted terrorist attack at stadium", "Cyber-enabled crime - CNP fraud as terrorist act facilitator" and "Radicalisation & terrorist threat prevention". The fact that this field has enormous potential for fighting crime and promoting public safety is evident in software solutions such as KIVU. KIVU conducts network analyses and uses and analyses open source data for this purpose. Also, the mentioned algorithm LEA (see Chapter 5.2.2.1) represents a kind of social media monitoring and is able to identify and filter radical and extremist content from comments and contributions on social media platforms.

Network analyses are also used in the area of financial crime, which is covered in the use case 3 “Financial crime investigation - Detection of fraudulent companies”, which deals with the detection of criminal activities and other violations of law. At present, systems such as kantwert are already used to identify network structures in the area of financial crime, making use of public registers and entries such as company registers. Concrete transactions and activities on the financial market are also already systematically monitored and conspicuous transactions identified on the basis of algorithms. However, such systems often operate on an extremely coarse mesh, as the majority of the transactions identified as conspicuous ultimately turn out to be irrelevant. Thus, such systems produce outputs to a considerable extent that are not relevant for the fight against financial crime. Rather, this results in an enormous expenditure of resources, because if a transaction is classified as conspicuous, this must be verified by humans. This means that previous systems need to be modified and expanded. For this reason, IfmPt is

already working with a partner to improve the algorithms used so far in order to generate a more fine-meshed output.

Data-mining and data-science tools, such as those formulated in the Use Case 5 "Illicit markets investigation - Police and archaeology against looting and trafficking of cultural goods", which deals with the trade of cultural heritage to finance terrorism, are already in operational use, for example in predictive policing solutions, which underlines their importance in the fight against crime. Knowledge databases are also established techniques within law enforcement.

In the Use Case “Soft targets protection - Attempted attack at stadium”, the technology of georeferencing is also shown for the identification of endangered districts or districts to be protected. Georeferencing is a central component of spatial predictive policing and it is implemented in a number of existing software solutions. As already mentioned, however, the use cases mainly outline investigation-supporting technologies and investigative tools. As underlined by the existence of numerous projects and software solutions, these are of great importance in the fight against cybercrime, organized crime and terrorism. However, technical solutions that fall within the area of “predictive policing” are less addressed in the requirements of the LEA, especially with regard to spatially based predictive policing. Spatial predictive policing solutions such as PRECOBS or SKALA are particularly relevant in the fight against mass crime. As already mentioned, spatial predictive policing is, however, only taken up by LEAS in the use case “Soft target protection - Attempted terrorist attack at stadium”, whereas the situation is different for person-related predictive policing. In particular, the descriptions of the Use Case “Radicalisation & terrorist threat prevention” show the significant relevance of models that can recognise and/or predict radicalisation processes of individual persons or groups. Intensive research and development of new technologies is already made in this area.

In Germany, several projects are currently being carried out on the subject of “Radicalisation and the Internet”. The project “X-Sonar” (“Analyse extremist efforts in social networks”) is working on the development of a software-supported analysis and evaluation tool. The aim is to “investigate the development of radicalisation processes in online networks, blogs and Internet forums. Among other things, inhuman discourses as well as criminally relevant behaviour patterns will be analysed in order to identify patterns of radicalisation and to develop indicators for the early detection of radical tendencies. In dialogue with the state criminal investigation offices and authorities involved, an instrument for the recognition of extremist network structures and for the assessment of individual and collective immunization processes is also being developed” [171]. The project “RadigZ” (Radicalization in the digital age) is also dedicated to this topic. It aims to prevent radicalisation processes and to immunise people against radical ideologies on the Internet. The central concern is the development of target group-specific protection measures. Target groups are young people and teachers as well as members of the police and judiciary. The developed materials are made available to all interested parties on an internet platform [172].

PANDORA is the abbreviation for "propaganda, mobilization and radicalization to violence in the virtual and real world". PANDORA serves, among other things, the early detection of processes of radicalisation by examining "which extremist ideas and symbolisms are used on the Internet and social media and how

they contribute to radicalisation". The attempt to document connections between Internet propaganda and real events is interesting. "In the process, current violent events and the associated discussions in the social media are mapped and assigned to the respective extremist milieu" [173]. The software solutions RADAR-iTE, VERA-2R, ERG22+, TRAP-18, SAVE and Screener Islamism, which have already been discussed, are further examples of already established personal predictive policing instruments.

Perhaps there is still a lack of knowledge among LEAs about the possibilities that predictive policing already offers for everyday operational use. In this context, it seems to make sense to hold a workshop with the LEAs in order to present the possibilities of predictive policing in a concrete way and to specify the requirements on this basis. For example, a not inconsiderable proportion of mass crime is gang or organised crime (burglary, theft from motor vehicles, theft of vehicles), which can be effectively combated with predictive policing solutions.

Overall, it is clear that the LEAs cover a large part of the relevant areas for combating cybercrime, organised crime and terrorism and for maintaining and promoting internal security with the requirements formulated in the use cases. The fact that solutions e.g. in the form of software applications are already on the market for some of the scenarios described in the use cases underlines their relevance. Nevertheless, it remains to be stated that, precisely because of the existence of already established methods or software tools, the solutions planned within the framework of the PREVISION project should have unique selling points. Otherwise, public authorities are probably not willing to replace tools that have just been introduced, e.g. in the field of predictive policing, with new ones, as the introduction of new technical instruments into the cop culture is an extremely complex process.

9. References

[1] Lee, C., Kriminalität der Mächtigen: Gegenstandsbestimmung, Erscheinungsformen und ein Versuch der Erklärung. Soziale Probleme, 6/1: 24-61, 1995, at: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-247420 [last accessed: 31.08.2005].

[2] Schweer, T., Der Kunde ist König. Organisierte Kriminalität in Deutschland. Frankfurt am Main u. a.: Peter Lang, 2003.

[3] Lampe , K. von, Organisierte Kriminalität. Vortrag vor der Arbeitsgemeinschaft sozialdemokratischer Juristinnen und Juristen, Landesverband Berlin, 5. Dezember 2000. Unter: http://www.organized-crime.de/organisiertekriminalitaet.htm [last accessed: 31.08.2005].

[4] Hobbs, D., Organisierte Kriminalität und Gewalt, in: W. Heitmeyer & J. Hagan (Hrsg.): Internationales Handbuch der Gewaltforschung. Wiesbaden: Westdeutscher Verlag. Wiesbaden, 2002.

[5] Kelly, R. J., Organized Crime: A Global Perspective, Totowan/NJ: Rowman and Littlefield. 1986.

[6] Bourdieu, P., Die feinen Unterschiede. Kritik der gesellschaftlichen Urteilfähigkeit. Suhrkamp: Frankfurt am Main, 2008.

[7] Kinzig, J., Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität. Berlin: Dunker & Humblot, 2004.

[8] Arlacchi, P., Mafiose Ethik und der Geist des Kapitalismus: Die unternehmerische Mafia, Frankfurt am Main: Cooperative-Verlag, 1989.

[9] Neumahr, A., Organisierte Kriminalität. Konzeption und ihr Realitätsbezug. Eine kritische Analyse aufgrund einer Auswertung des bisherigen Forschungsstandes der USA. Tübingen: MVK, Medienverlag Köhler, 1999.

[10] Besozzi, C., Organisierte Kriminalität und empirische Forschung Zürich: Verlag: Rüegger, 1997.

[11] Longrigg, C., Patinnen: die Frauen der Mafia. München: Blessing, 1998.

[12] Raith, W., Nachwort, in M. Pino: Im Dienst der „Familie“. Weibliche Drogenkuriere der Mafia. Frankfurt a.M.: Fischer Taschenbuch Verlag, 134-143, 1996.

[13] Kreisky, E., Vorlesung „Mafia, Staat und Männlichkeit“, Institut für Politikwissenschaft, Universität Wien, 2003, at: https://docplayer.org/44329484-Vorlesung-sose-mafia-staat-und-maennlichkeit-prof-eva-kreisky-zur-rolle-und-funktion-von-frauen-in-der-italienischen-mafia.html [last accessed: 09.12.2019].

[14] Mermelstein, M., Der Mann mit dem Schnee: Ein Insider des Drogenkartells packt aus. Köln: Kiepenheuer & Witsch, 1991.

[15] Adler, P. A. & P. Adler, Großdealer und -schmuggler in Kalifornien: Karrieren zwischen Abweichung und Konformität. In: Paul, B. u. H. Schmidt-Semisch (Hrsg.): Drogendealer: Ansichten eines verrufenen Gewerbes, Freiburg i.Brsg.: Lambertus: 148-166, 1998.

[16] Bourgois, P., Crackdealer in East Harlem. Widerstand und Selbstzerstörung unter amerikanischer Apartheid. In: Paul B. u. H. Schmidt-Semisch (Hrsg.): Drogendealer. Ansichten eines verrufenen Gewerbes. Freiburg i.: Lambertus: 167-182, 1998.

[17] Gernert, J., Er wird, er wird nicht, er wird …Ein Soziologe sagt, sein Computerprogramm könne vor der Geburt eines Menschen herausfinden, ob der straffällig wird. Aber will man das? 2016, at: https://taz.de/Algorithmen-und-Kriminalitaet/!5243783/ [last accessed: 01.12.2019].

[18]Reinares, F., Terrorismus. in: W. Heitmeyer & J. Hagan (Hrsg.): Internationales Handbuch der Gewaltforschung. Westdeutscher Verlag: Wiesbaden: 390-405, 2002.

[19]"9/11 – Die Welt danach". arte Dokumentation. At: https://www.youtube.com/watch?v=i0Sh0jK3fIY&t= 1658s [last accessed: 27.11.2019].

[20]Harari, Y. N., 21. Lektionen für das 21. Jahrhundert. München: C.H.Beck, 2018.

[21]Hess, H., Terrorismus: Quo vadis?. Kurzfristige Prognosen und mittelfristige Orientierungen, In: Kemmesies. U. (Hrsg.), Terrorismus und Extremismus – der Zukunft auf der Spur: Beiträge zur Entwicklungsdynamik von Terrorismus und Extremismus - Möglichkeiten und Grenzen einer prognostischen Empirie. München: Wolters Kluwer Deutschland: 105-150, 2006.

[22]Hoffman, B., Terrorismus – Der unerklärte Krieg: Neue Gefahren politischer Gewalt. Frankfurt am Main: Fischer Taschenbuch Verlag, 2002.

[23]Schneckener, U., Globaler Terrorismus. Bundeszentrale für politische Bildung, 2006, at: http://www.bpb.de/publikationen/7N2DFT.tml [last accessed: 01.12.2006].

[24]Wietlisbach, O., Die vergessenen Jahre des Terrors: In den 70ern und 80ern zogen Terroristen eine Blutspur durch Europa, 2016, at: https://www.watson.ch/wissen/schweiz/982459207-terror-in-europa-und-der-schweiz-seit-1970-diese-fakten-sollte-man-kennen [last accessed: 05.12.2019].

[25]Brandt, M., Zwischen RAF und IS, 2016, at: https://de.statista.com/infografik/5378/terrorattacken-in-westeuropa/ [last accessed: 05.12.2019].

[26]Kahneman, D., Schnelles Denken, langsames Denken. München: Siedler Verlag. 2011.

[27]Zangl, B. & M. Zürn, Die Auswirkungen der Globalisierung auf die Sicherheit in der OECD-Welt, in: Lippert, E. et al. (Hrsg.), Sicherheit in einer unsicheren Gesellschaft, Opladen: Springer:157-187, 1997.

[28]Kutscha, M., Trennungsgebot, in: Lange, H.-J. (Hrsg.), Wörterbuch zur Inneren Sicherheit, Wiesbaden: Springer: 337-340, 2006.

[29]Pelzer, R. & S. Scheerer, Terrorismus-Prognosen: Fehlerquellen und Rechtsstaatlichkeit, in: U. E. Kemmesies (Hrsg.): Terrorismus und Extremismus – der Zukunft auf der Spur: Beiträge zur Entwicklungsdynamik von Terrorismus und Extremismus – Möglichkeiten und Grenzen einer prognostischen Empirie, München: Luchterhand: 199-216, 2006.

[30]Stodt, B. A., Internetnutzungskompetenz als Determinante funktionaler und dysfunktionaler Facetten der Internetnutzung. Universität Duisburg-Essen, 2018, at: https://duepublico2.uni-due.de/servlets/MCRFileNodeServlet/duepublico_derivate_00046830/Diss_Stodt.pdf [last accessed: 05.12.2019].

[31]Schwind, H.-D., Kriminologie und Kriminalpolitik. Eine praxisorientierte Einführung mit Beispielen. 23., neubearbeitete und erweiterte Auflage. Heidelberg: Kriminalistik, 2016.

[32]BKA – Bundeskriminalamt, Internetkriminalität/Cybercrime, 2019b, at: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html [last accessed: 15.11.2019].

[33]Brockhaus Enzyklopädie, 21. Auflage, Band 18. Leipzig, 2002.

[34]Schnell, R., P. B. Hill & E. Esser, Methoden der empirischen Sozialforschung. München, Wien: Oldenbourg, 1989.

[35]Dahle, K.-P., Psychologische Kriminalprognose. Wege zu einer integrativen Methodik für die Beurteilung der Rückfallwahrscheinlichkeit bei Strafgefangenen. Freiburg: Centaurus, 2010.

[36]Bliesener, T., Psychologische Instrumente für Kriminalprognose und Risikomanagement. Praxis der Rechtspsychologie 17/2: 323-344, 2007.

[37]Bergmann, B., Expertise in der Prognose von Kriminalität. Eine Untersuchung am Beispiel der polizeilichen Einschätzung zukünftigen Verhaltens junger Straftäter. Kiel: Christian-Albrechts-Universität, 2018.

[38]Dahle, K.-P., Kriminal(rückfall)prognose, in: R. Volbert & M. Steller (Hrsg.): Handbuch der Rechtspyschologie. Göttigen: Hogrefe: 444-452, 2008.

[39]Görgen, T., H. van den Brink, A. Taefi & B. Kraus, JuKrim2020. Mögliche Entwicklungen der Jugend(gewalt)kriminalität in Deutschland. Szenarien, Trends, Prognosen 2010-2020. Abschlussbericht zur Herbstkonferenz 2010 der Ständigen Konferenz der Innenminister und –senatoren der Länder. Münster: Deutsche Hochschule der Polizei, 2010.

[40]Grime, M. M. & G. Wright, Delphi Method. Statistics Reference Online: 1-6, 2016.

[41]Anders, K., A. Prochnow, R. Schlauderer & G. Wiegleb, Die Szenario-Methode als Instrument der Naturschutzplanung im Offenland, in: K. Anders, J. Mrzljak, D. Wallschläger & G. Wiegleb (Hrsg.): Handbuch Offenlandmanagement am Beispiel ehemaliger und in Nutzung befindlicher Truppenübungsplätze. Berlin, Heidelberg: Springer: 97-104, 2004.

[42]Vogel, J., Prognose von zeitreihen. Eine Einführung für Wirtschaftswissenschaftler. Wiesbaden: Springer Gabler, 2015.

[43]Clarke, R. & M. Felson, Routine Activity and Rational Choice. NJ: Transaction, 1993.

[44]Lamnek, S., Theorien abweichenden Verhaltens. München: Fink, 1988.

[45]Sutherland, E. H., Principles of criminology. Chicago, Philadelphia: Lippincott, 1939.

[46]Cloward, R. A., & Ohlin, L. E., Delinquency and Opportunity: A theory of delinquent gangs. New York: Free Press, 1960.

[47]Burgess, R. L., R. L. Akers, A Differential Association Reinforcement Theory of Criminal Behavior. Social Problems 14/2: 128-147, 1966.

[48]Cohen, L. E. & M. Felson, Social Change and Crime Rate Trends: A Routine ActivityApproach. American Sociological Review 44/4: 588-608, 1979.

[49]Siegel, R., Criminology. Belmont: Wadsworth Publ. Comp, 2000.

[50]Brandt, D., Wirkungen situativer Kriminalprävention – eine Evaluationsstudie zur Videoüberwachung in der Bundesrepublik Deutschland. Diplomarbeit Universität Bielefeld, 2004, at: https://pub.uni-bielefeld.de/download/2306207/2306210 [last accessed: 05.12.2019].

[51]Felson, M. & R. V. Clarke, Opportunity Makes the Thief. Practical theory for crime prevention. Police Research Series Paper 98. London: Home, 1998, at: https://pdfs.semanticscholar.org/09db/dbce90b22357d58671c41a50c8c2f5dc1cf0.pdf [last accessed: 05.12.2019].

[52]Felson, M., Crime and Everyday Life. Thousand Oaks: Pine Forge Press, 1998.

[53]Durkheim, E., Le suicide: Étude de sociologie. Paris: Félix Alcan, 1987.

[54]Thrasher, F. M., The Gang. A Study of 1.313 Gangs in Chicago. Chicago: New Chicago School Press, 2000.

[55]Whyte, W. F., Die Street Corner Society (Erstausgabe 1943), Berlin/New York: de Gruyter, 1996.

[56]Burgess, E. W. & R. E. Park; Introduction to Science of the Sociology, 1921.

[57]Park, R. E., E. W. Burgess & R. D. McKenzie; The City. University of Chicago Press, 1925.

[58]Hoyt, H., The Structure and Growth of Residential Neighborhoods in American Cities. Washington D.C.: Federal Housing Administration, 1939.

[59]Harris, C. D. & E. L. Ullman, The Nature of Cities. The Annals of the American Academy of Political and Social Science 242: 7-17, 1945.

[60]Shaw, C. R. & H. D. Mc Kay, Juvenile Delinquency and Urban Areas: A Study of Delinquency in Relation to Differential Characteristics of Local Communities in American Cities, Chicago, 1942.

[61]Lamnek, S., Theorien abweichenden Verhaltens, München: Fink, 1993.

[62]Bourekba, M., Countering Violent Extremism in the MENA Region: Time to Rethink Approaches and Strategies EuroMesco Policy Brief Nº63, 2016: Retrieved from: http://www.iai.it/sites/default/files/euromescobrief_63.pdf.

[63]Schmid, A. P., "Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review", The International Centre for Counter-Terrorism – The Hague 4, no. 2, 2013.

[64]Dzehkova, R., et.al., 2016. Understanding Radicalization: Review of Literature, CSD, ISBN: 978-954-477-261-1.

[65]Bötticher, A. (2017). Towards Academic Consensus Definitions of Radicalism and Extremism. Perspectives on Terrorism, 11(4), 73-77. Retrieved from: www.jstor.org/stable/26297896.

[66]Steven Hutchinson & Pat O'malley (2007) A Crime–Terror Nexus? Thinking on Some of the Links between Terrorism and Criminality, Studies in Conflict & Terrorism, 30:12, 1095-1107, DOI: 10.1080/10576100701670870

[67]Arun Kundnani, 'Radicalisation: the journey of a concept', Race & Class, Vol. 54, No. 2 (Oct.-Dec. 2012), p. 3.

[68]Costanza, W (2012). An interdisciplinary framework to assess the radicalization of youth towards violent extremism across cultures, Georgetown University, p. 26

[69]Jeffrey Monaghan & Adam Molnar (2016): Radicalisation theories, policing practices, and "the future of terrorism?", Critical Studies on Terrorism, DOI: 10.1080/17539153.2016.1178485

[70]Horgan, J., (2008). From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism, The Annals of the American Academy of Political and Social Science, 618 (10), pp. 80-94.

[71]Gunning, J. (2009). Social movement theory and the study of terrorism," in R. Jackson, M. B. Smyth, & J. Gunning (eds.) Critical terrorism studies: A new research agenda. New York: Routledge.

[72]Zald M., and McCarthy, J., 1987. Social movements in an organizational society. New Brunswick, NJ: Transaction Books.

[73]Merton, R.K., 1938.Social Structure and Anomie. American Sociological Review Vol. 3, No. 5, pp. 672-682.

[74]https://www.files.ethz.ch/isn/48325/WP082.pdf

[75]Dalgaard-Nielsen, A., (2008). Studying Violent Radicalization in Europe I: The potential contribution of Social Movement Theory. DIIS Working paper no.2008/2 [pdf] Available at: https://www.files.ethz.ch/isn/48325/WP082.pdf

[76]Allport, G.W. (1985). The historical background of social psychology," in G. Lindzey and E. Aronson (eds.), Handbook of social psychology New York: McGraw Hill.

[77]Rambo, L.R., 1993. Understanding religious conversions. New Haven: Yale university.

[78]McCauley, C., and S. Moskalenko, S. (2008). Mechanisms of political radicalization: Pathways toward terrorism. Terrorism and Political Violence vol. 416.

[79]Wright, S., (2007). The dynamics of movement membership: Joining and leaving new religious movements," in D. G. Bromley (ed.), Teaching new religious movements, Oxford: Oxford University Press.

[80]Dawson, LL., 2010. The Study of New Religious Movements and the Radicalization of Home-Grown Terrorists: Opening a Dialogue," Terrorism and Political Violence 22:1, pp. 1–21.

[81]Crossett, Ch., and Spitaletta, J.A., (2010). Radicalization: relevant psychological and sociological concepts. The John Hopkins University, Applied Physics Laboratory: U.S. Army Asymmetric Warfare Group.

[82]Christmann, K. (2012). Preventing Religious Radicalisation and Violent Extremism: A Systematic Review of the Research Evidence [pdf] Available at: https://www.safecampuscommunities.ac.uk/uploads/files/2016/08/yjb_preventing_violent_extremism_systematic_review_requires_uploading.pdf

[83]Campelo, N., Oppetit, A., Neau, F., Cohen, D., & Bronsard, G. (2018). Who are the European youths willing to engage in radicalisation? A multidisciplinary review of their psychological and social profiles. European Psychiatry, 52, 1-14. doi:10.1016/j.eurpsy.2018.03.001

[84]Moghaddam, F. (2005) The Staircase to Terrorism. A Psychological Exploration. American Psychologist, 60(2), 161-9.

[85]F.M. Moghadam, 'De-radicalisation and the Staircase from Terrorism', in David Canter (Ed.), The Faces of Terrorism: Multidisciplinary Perspective (New York: John Wiley, 2009), pp. 278-79.

[86]Sageman, M., (2008). Leaderless Jihad: Terror Networks in the Twenty-First Century, Philadelphia: University of Pennsylvania Press.

[87]Joshua Sinai, 'Radicalisation into Extremism and Terrorism: A Conceptual Model', The Intelligencer, Vol. 19, No. 2 (Summer/Fall 2012), pp. 22-3.

[88]https://www.fbi.gov/cve508/teen-website/why-do-people-become-violent-extremists

[89]Cole, J., Alison, E., Cole, B., & Alison, L. (2010). Guidance for identifying people vulnerable to recruitment into violent extremism. In S. o. Psychology (Ed.): University of Liverpool.

[90]Böckler, N., Leuschner, V., Roth, V., Zick, A., & Scheithauer, H. (2018). Blurred Boundaries of Lone-Actor Targeted Violence: Similarities in the Genesis and Performance of Terrorist Attacks and School Shootings. Violence and Gender, 5(2), 70-80. doi:10.1089/vio.2018.0002

[91]Lankford, A., & Hakim, N. (2011). From Columbine to Palestine: A comparative analysis of rampage shooters in the United States and volunteer suicide bombers in the Middle East. Aggression and Violent Behavior, 16(2), 98-107.

[92]Böckler, N., Leuschner, V., Zick, A., & Scheithauer, H. (2018). Same but different? Developmental pathways to demonstrative targeted attacks – qualitative case analyses of adolescent and young adult perpetrators of targeted school attacks and jihadi terrorist attacks in Germany. International Journal of Developmental Science,12, 5-24.

[93]Meleagrou-Hitchens, A., and Kaderbhai, N., (2017). Research perspectives on online Radicalisation: A literature review 2006-2016. [pdf] Available at: https://www.voxpol.eu/download/vox-pol_publication/Research_Perspectives_Lit_Review.pdf

[94]https://www.voxpol.eu/download/vox-pol_publication/Online-Behaviours_FINAL.pdf

[95]von Behr, I., et.al., (2013). Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism. [pdf] Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

[96]Gill, P., Horgan, J. and Deckert., P. (2014). Bombing alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists. Journal of Forensic Sciences, 59: 425– 435.

[97]https://www.e-ir.info/2017/07/19/an-analysis-of-online-terrorist-recruiting-and-propaganda-strategies/#_ftn2

[98]Idag, O., Leiser, A and Boehnke, K., 2019. Reviewing the role of the Internet in Radicalisation Processes. Journal for deradicalization, 21, pp. 261-300. https://journals.sfu.ca/jd/index.php/jd/article/view/289/197

[99]Liebermann, V., (2017). Terrorism, the internet and Propaganda: a deadly combination. Journal of National Security law & Policy, 9, pp. 95-124.

[100] Gill P., et.al., (2017). Terrorist use of internet by the numbers. Criminology and Public Policy, 16 (1). https://doi.org/10.1111/1745-9133.12249

[101] Hassan, G., et.al. (2018). Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence. International journal of developmental science, 12(1-2), 71-88.

[102] BKA – Bundeskriminalamt, Gesichtserkennung, 2019a:, at: https://www.bka.de/DE/UnsereAufgaben/ Ermittlungsunterstuetzung/Kriminaltechnik/Biometrie/ Gesichtserkennung/gesichtserkennung_node.html [last accessed: 04.12.2019].

[103] BLKA – Bayerisches Landeskriminalamt, Informationen über die dritte Dimension des Erkennungs-dienstes. Gesichtserkennung. Informationsflyer. München: Bayerisches Landeskriminalamt, 2019.

[104] Würtz, R. P., Technik und Leistungsfähigkeit automatischer Gesichtserkennung, FlfF-Kommunikation 19/1, 2002, at: https://www.ini.rub.de/upload/file/ 1470692857_a5e984290737c0fc3074/rolf-fiff2002.pdf [last accessed: 04.12.2019].

[105] Wolfangel, E., Auf der falschen Spur. Süddeutsche Zeitung Nr. 80., 2018.

[106] Töpfer, E., Videoüberwachung in Europa: Entwicklung, Perspektiven und Probleme, in: H.-J. Kreowski (Hrsg.): Informatik und Gesellschaft: Verflechtungen und Perspektiven. Berlin, Münster: LIT Verlag: 61-82, 2008.

[107] Feltes, T. & A. Ruch, Stellungnahme zur öffentlichen Anhörung am Montag, 06.03.2017 im Innenausschuss des Deutschen Bundestages, 2017, at: https://www.bundestag.de/resource/blob/495434/95e763508e5400acbad1bc0b71386d98/18-4-785-c-data.pdf [last accessed: 03.12.2019].

[108] Knobloch, T., Vor die Lage kommen: Predictive Policing in Deutschland. Chancen und Gefahren datenanalytischer Prognosetechnik und Empfehlungen für den Einsatz in der Polizeiarbeit. Stiftung Neue Verantwortung. Bertelsmann Stiftung, 2018, at: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/predictive.policing.pdf [last accessed: 30.09.2019].

[109] Egbert, S. & S. Krasmann, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis. Projektabschlussbericht. Hamburg: Universität Hamburg, 2019.

[110] Buttkus, M. & R. Eberenz, Big Data in der Konsumgüterindustrie: Kunden verstehen, Produkte entwickeln, Marketing steuern, in: Buttkus, M. & R. Eberenz (Hrsg.), Controlling in der Konsumgüterindustrie: Innovative Ansätze und Praxisbeispiele. Wiesbaden: Springer, S. 69-90, 2014.

[111] Leese, M., Predictive Policing in der Schweiz: Chancen, Herausforderungen, Risiken. Bulletin 2018 zur schweizerischen Sicherheitspolitik. Zürich: Center for Security Studies, 2018.

[112] Dern, H., R. Frönd, U. Straub, J. Vick & R. Witt, Geografisches Verhalten fremder Täter bei sexuellen Gewaltdelikten. Bundeskriminalamt Wiesbaden, 2004.

[113] Hill, B. & R. Paynich, Fundamentals of Crime Mapping. Burlington: Jones & Bartlett Learning, 2014.

[114] Balogh, D., Untersuchung des Phänomens der sogenannten Near-Repeat-Wohnungseinbruchsdelikte am Beispiel der Stadt Zürich. Möglichkeiten und Grenzen des Prospective Crime Mappings. Masterarbeit. Universität Bern / SCIP (School of Criminology, International Criminal Law and Psychology Law)., 2013.

[115] Townsley, M., R. Homel & J. Chaseling, Infectious Burglaries. A Test of the Near Repeat Hypothesis. British Journal of Criminology 43: 615-633, 2003.

[116] Stockrahm, S., Mit Mathematik Verbrechen bekämpfen. Die Zeit 22.Februar 2010, 2010, at: http://www.zeit.de/wissen/2010-02/mathematik-kriminalitaetsmodell [last accessed: 06.05.2013].

[117] Knox, E. G., Epidemiology of Childhood Leukaemia in Northumberland and Durham. British Journal of Preventive and Social Medicine. 18/1964: 18-24, 1964.

[118] Gluba, A., Der Modus Operandi bei Fällen der Near Repeat-Victimisation. Ergebnisse einer empirischen Studie. Kriminalistik 6/2017: 369-375, 2017.

[119] Farrell, G., Progress and Prospects in the Prevention of Repeat Victimisation, in: N. Tilley (Hrsg.): Handbook of Crime Prevention and Community Safety. Portland: Willan Publishing: 143-170, 2005.

[120] LKA NRW – Landeskriminalamt NRW, Abschlussbericht Projekt SKALA, 2018, at: https://polizei.nrw/sites/default/files/2018-07/180628_Abschlussbericht_SKALA.PDF [last accessed: 30.09.2019].

[121] Pease, K., Repeat Victimisation: Taking Stock. Crime detection and prevention Series, Paper 90. London: Home Office, 1998.

[122] Chainey S. P. & B. F. A. da Silva, Examining the extent of repeat and near repeat victimisation of domestic burglaries in Belo Horizonte, Brazil. Crime Science 5: 1-10, 2016.

[123] Morgan, F., Repeat Burglary in a Perth Suburb: Indicator of Short-Termin or Long-Term Risk, in G. Farrell & K. Pease (Hrsg.): Repeat Victimisation: Crime Prevention Studies 12:83-118, 2000.

[124] Hindelang, M. J., Gottfredson, M. R. & Garofalo, J., Victims of personal crime: An empiricalfoundation for a theory of personal victimization. Cambridge, MA: Ballinger, 1978.

[125] Fielding, M. & V. Jones, "Repeat Victimisation – Road to Reduction". Disrupting the Optimal Forager. Submission Goldstein Award 2012, 2012, at: https://popcenter.asu.edu/sites/default/files/12-08f_manchester_trafford.pdf [last accessed: 27.12.2019].

[126] Caplan, J. M. & L. W. Kennedy, Risk Terrain Modeling Overview, in: J. M. Caplan & L. W. Kennedy (Hrsg.): Risk terrain Modeling Compendium. Newark, NJ: Rutgers Center on Public Security: 11-13, 2011.

[127] Kennedy, L. W., J. M. Caplan, E. L. Piza & H. Buccine-Schraeder, Vulnerability and Exposure to Crime: Applying Risk Terrain Modeling to the Study of Assault in Chicago. Applied Spatial Analysis and Policy 9/4: 529-548, 2015.

[128] Collados, M. C., Statistical Analysis of spatio-temporal crime patterns. Optimization of patrolling strategies. Universidad de Granada, Tesis Doctorales, 2016.

[129] Grundies,V., Gibt es typische kriminelle Karrieren?, in: D. Dölling & J.-M. Jehle (Hrsg.), 2013: Täter – Taten – Opfer. Mönchengladbach: Forum Verlag Godesberg: 36-52, 2013.

[130] Artz, K., Max-Plank-Institut sucht typische Kriminelle. RP Online 12. Mai 2012, 2012, at: https://rp-online.de/panorama/wissen/max-planck-institut-sucht-typische-kriminelle_aid-8952465 [last accessed: 10.12.2019].

[131] Anonymus, Mein Leben für die Mafia. Der Lebensbericht eines ehrbaren anonymen Sizilianers. Reinbek bei Hamburg: Rowohlt, 1989.

[132] Arlacchi, P., Mafia von innen. Das Leben des Don Antonio Calderone. Frankfurt a.M.: Fischer Taschenbuch Verlag, 1995.

[133] Schneider, H. J., Kriminologie. Berlin: de Gruyter, 1987.

[134] Lamnek, S., Neue Theorien abweichenden Verhaltens. München: Fink, 1997.

[135] Brendler, M., Gesucht: Ein Profil zur Terroristenfrüherkennung. Interview mit dem Psychiater Norbert Leygraf, 2015, at: https://www.faz.net/aktuell/wissen/leben-gene/gesucht-ein-profil-zur-terroristenfrueherkennung-13949944.html?printPagedArticle=true#pageIndex_3 [last accessed: 27.12.2019].

[136] Lützinger, S., Die Sicht der Anderen. Eine qualitative Studie zu Biographien von Extremisten und Terroristen. Reihe Polizei + Forschung, Bd. 40. Köln: Luchterhand, 2010.

[137] Neumann, P., Die neuen Dschihadisten. IS, Europa und die nächste Welle des Terrors. Berlin: Ullstein, 2015.

[138] Logvinov, M., Risikobewertung extremistischer Gewalt. Verfahren – Instrumente – Kritik. Wiesbaden: Springer VS, 2019.

[139] Borum, R., Assessing risk for terrorism involvement. Journal of Threat Assessment and Management 2/2: 63-87, 2015.

[140] Pfahl-Traughber, A., Von den „Aktivisten“ über die „Kommunikation“ bis zur „Wirkung“. Das AGIKOSUW-Schema zur Analyse terroristischer Bestrebungen, in: A. Pfahl-Traughber (Hrsg.): Jahrbuch für Extremismus- und Terrorismusforschung 2014 (II). Schriften zur Extremismus- und Terrorismusforschung.167-188. Brühl: Hochschule des Bundes für öffentliche Verwaltung, 2014, at: https://www.hsbund.de/SharedDocs/Downloads/2_Zentralbereich/20_Referat_W/50_Publikationen/20_Schriften_Extremismus_Terrorismusforschung/band_09.pdf?__blob=publicationFile&v=3 [last accessed: 06.12.2019].

[141] Urban, J., Die Bekämpfung des Internationalen Islamistischen Terrorismus. Wiesbaden. VS Verlag für Sozialwissenschaften, 2006.

[142] Rettenberger, M., Intuitive, klinisch-idiographische und statistische Kriminalprognosen im Vergleich – die Überlegenheit wissenschaftlich strukturierten Vorgehens. Forensische Psychiatrie, Psychologie, Kriminologie 12/1: 28-36, 2018.

[143] Berg, A. von, Risk Assessment im Phänomenbereich gewaltbereiter Extremismus – State of the Art. Interventionen – Zeitschrift für Verantwortungspädagogik. Schwerpunkt Risiko 13: 4-15, 2019.

[144] Bröckling, M., Wie die bayerische Polizei das Predictive Policing nach Deutschland brachte. Interview mit dem Soziologen Simon Egbert, 2019, at: https://netzpolitik.org/2019/wie-die-bayerische-polizei-das-predictive-policing-nach-deutschland-brachte/#spendenleiste [last accessed: 09.12.2019].

[145] BKA – Bundeskriminalamt, Neues Instrument zur Risikobewertung von potentiellen Gewaltstraftätern. Presseinformation des Bundeskriminalamtes. BKA Pressestelle, 2017.

[146] Bundesregierung, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Martina Renner, Kersten Steinke und der Fraktion DIE LINKE. – Drucksache 18/13301 – Instrument des Bundeskriminalamtes zur Risikobewertung potentieller islamistischer Gewalttäter, 2017, at: http://dip21.bundestag.de/dip21/btd/18/134/1813422.pdf [last accessed: 22.11.2019].

[147] Böckler, N., M. Allwinn, J. Hoffmann & A. Zick, Früherkennung von islamistisch motivierter Radikalisierung. Vorstellung und empirische Validierung eines verhaltensbasierten Instrumentes zum Fallscreening. Kriminalistik 8-9, 2017.

[148] Haverkamp, R., Die Prognose von terroristischen Anschlägen: Grenzen wissenschaftlicher Erkenntnisse und der Versuch zur Entwicklung eines Präventionsmodells, ZStW 123 Heft 1, p. 92-109. 2011.

[149] Peteranderl, S., Predictive Policing: Dem Verbrechen der Zukunft auf der Spur, 2019, at: https://netzpolitik.org/2019/predictive-policing-dem-verbrechen-der-zukunft-auf-der-spur/#spendenleiste [last accessed: 27.12.2019].

[150] Meyer-Schilf, K., Raus aus der Filterblase. taz 13. Februar 2018, 2018, at: https://taz.de/Extremismus-Ueberwachung-im-Internet/!5481327/ [last accessed: 06.12.2019].

[151] Beratungs-Netzwerk Hessen, Monitoring-Berichte, 2019, at: http://beratungsnetzwerk-hessen.de/monitoring-berichte [last accessed: 06.12.2019].

[152] BMFSFJ – Bundesministerium für Familie, Senioren, Frauen und Jugend, Strategie der Bundesregierung zur Extremismusprävention und Demokratieförderung. 1. Auflage, 2016, at: https://www.bmfsfj.de/blob/109002/5278d578ff8c59a19d4bef9fe4c034d8/strategie-der-bundesregierung-zur-extremismuspraevention-und-demokratiefoerderung-data.pdf [last accessed: 06.12.2019].

[153] Merton, R. K., Sozialstruktur und Anomie, in: F. Sack & R. König (Hrsg.): Kriminalsoziologie. Frankfurt am Main: Akademische Verlagsgesellschaft: 283-313, 1968.

[154] Neu, V., Rechts- und Linksextremismus in Deutschland. Wahlverhalten und Einstellungen. Zukunftsforum Politik. Sankt Augustin, Berlin: Konrad-Adenauer-Stiftung, 2009.

[155] Jetter, M., Terrorism and the Media: The Effect of US Television Coverage on Al-Qaeda Attacks. IZA Discussion Paper No. 10708. Institute of Labor Economics (IZA), 2017.

[156] Jetter, M., Terrorism and the Media. IZA Discussion Paper No. 8497. Institute of the Study of Labor, 2014.

[157] Beckmann, K., R. Dewenter & T. Thomas, Can News Draw Blood? The Impact of Media Coverage on the Number and Severity of Terror Attacks. Discussion Paper. Düsseldorf Institute for Competition Economics. Düsseldorf University Press, 2016.

[158] Rohner, D. & B. S. Frey, Blood and ink! The common-interest-game between terrorists and the media. Public Choice 133/1-2: 129-145, 2007.

[159] Philips, D. P., The influence of suggestion on suicide: substantive and theoretical implications of the Werther effect. American Sociological Review 39/3: 340-354, 1974.

[160] Brosius, H.-B. & W. Ziegler, Massenmedien und Suizid: Praktische Konsequenzen aus dem Werther-Effekt. Communicatio Socialis 34/1: 9-29, 2001.

[161] Argawal, S., Applying Social Media Intelligence for Predicting and Identifying online Radicalization and Civil Unrest Oriented Threats, 2015, at: https://arxiv.org/pdf/1511.06858.pdf [last accessed: 02.12.2019].

[162] Knipping-Sorokin, R. & T. Stumpf, Radikal Online - Das Internet und die Radikalisierung von Jugendlichen. Eine Metanalyse zum Forschungsfeld, in: B. Frischling & M. Näser-Lather (Hrsg.): (H)acktivismus und Partizipation? Zur politischen Dimension des Digitalen. Sonderausgabe von kommunikation@gesellschaft 19/14: 1-29, 2018.

[163] DIVSI - Deutsches Institut für Vertrauen und Sicherheit im Internet, Radicalisation of young people via the Internet? A literature review, 2016, at: https://www.divsi.de/wp-content/uploads/2016/11/Radikalisierung-Jugendlicher-ueber-das-Internet.pdf [last accessed: 02.12.2019].

[164] Busch, A., Informationsinflation: Herausforderungen an die politische Willensbildung in der digitalen Gesellschaft, in: H. Gapski, M. Oberle & W. Staufer (Hrsg..): Medienkompetenz. Herausforderung für die Politik, politische Bildung und Medienbildung. Bundeszentrale für politische Bildung (bpb), Schriftenreihe Band 10111: 53-62, 2017.

[165] Statista, Anzahl der monatlich aktiven Facebook Nutzer weltweit vom 1. Quartal 2009 bis zum 3. Quartal 2019, 2019, at: https://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/ [last accessed: 23.12.2019].

[166] Bischoff, M. & K. Schmitz, Digitale Terror-Prognose. Spektrum 22. August 2017, 2017, at: https://www.spektrum.de/news/wie-kann-man-anschlaege-verhindern/1485569 [last accessed: 27.12.2019].

[167] Bundesministerium für Bildung und Forschung, o.J.a: Portal mit kostengünstigem IMS Netzwerk zum berührungslosen Nachweis am Körper getragener Explosivstoffe (POLINEX), at: https://www.sifo.de/files/Projektumriss_POLINEX.pdf [last accessed: 06.01.2020].

[168] Bundesministerium für Bildung und Forschung, o.J.b: Flexibles, teilautomatisiertes Analysesystem zur Auswertung von Videomassendaten (FLORIDA), at: https://www.sifo.de/files/Projektumriss_FLORIDA.pdf [last accessed: 06.01.2020].

[169] Fraunhofer Gesellschaft e.V., Gemeinsam für öffentliche Sicherheit, 2016, at: https://www.iosb.fraunhofer.de/servlet/is/93474/Broschuere_Oeffentliche_Sicherheit.pdf [last accessed: 06.01.2020].

[170] Bundespolizeipräsidium Potsdam, Teilprojekt 1 „Biometrische Gesichterkennung“ des Bundespolizeipräsidiums im Rahmen der Erprobung von systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz im Zeitraum vom 01.08.2017 – 31.07.2018, 2018, at: https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=E4DF12B50147BEEB445A074F9A980618.1_cid324?__blob=publicationFile&v=1 [last accessed 06.01.2020].

[171] Bundesministerium für Bildung und Forschung, o.J.c: Analyse extremistischer Bestrebungen in sozialen Netzwerken (X-Sonar), at: https://www.sifo.de/files/Projektumriss_X-SONAR.pdf [last accessed: 06.01.2020].

[172] Bundesministerium für Bildung und Forschung, o.J.d: Radikalisierung im digitalen Zeitalter (RadigZ), at: https://www.sifo.de/files/Projektumriss_RadigZ.pdf [last accessed: 06.01.2020].

[173] Bundesministerium für Bildung und Forschung, o.J.e: Propaganda, Mobilisierung und Radikalisierung zur Gewalt in der virtuellen und realen Welt (PANDORA), at: https://www.sifo.de/files/Projektumriss_PANDORA.pdf [last accessed: 06.01.2020].

[174] Peuckert, R., Abweichendes Verhalten und soziale Kontrolle, in H. Korte & B. Schäfers (Hrsg.): Einführung in die Hauptbegriffe der soziologie. 6. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften: 105-125, 2006.

[175] Beckers, K., J. Reissen-Kosch & F. Schilden, Sprachstratgeien der rechten szene im Netz – Wörter, Werte und ihre semantischen Transformationen, Glottotheory 4/2: 87-114, 2014.

[176] Vogel, I., R. Regev & M. Steinebach, Automatisierte Analyse Radikaler Inhalte im Internet, in: K. David, K. Geihs, M. Lange & G. Stumme (Hrsg.), INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft. Bonn: Gesellschaft für Informatik e.V.: 233-245, 2019.

[177] Forbidden Triad (Granovetter 1973, S. 1363)

[178] Visualization of an analysis of social networks (Ferguson 2018)

[179] Cavallaro, L., Disrupting resilient criminal networks through data analysis: The case of Sicilian Mafia. PLOS ONE, at: https://doi.org/10.1371/journal.pone.0236476 August 5, 2020, S. 17, [last accessed: 02.09.2020].

[180] Personal meetings and telephone calls of Cosa Nostra members Klaubert 2020