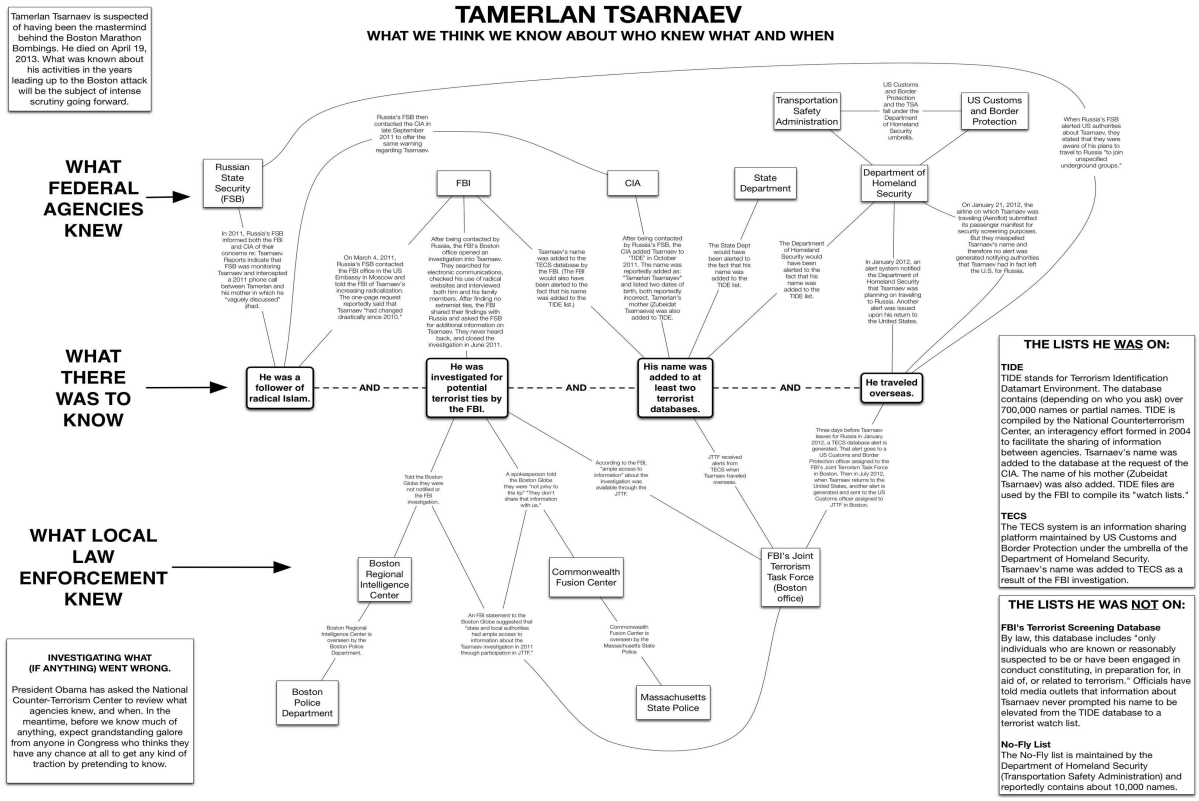
Terrorism, mass surveillance and civil rights

Dr Reinhard Kreissl
Reinhard.kreissl@vicesse.eu
www.vicesse.eu

In the on-going controversy over civil rights and mass surveillance an important aspect of police work to combat terrorism is overlooked. This paper will discuss the question whether more data or better analysis of available intelligence is the key to successful strategies in this area. Based on results from a study of the Austrian situation it will be argued that improving internal organizational structures and providing training for law enforcement experts will yield higher returns for Law enforcement than expanding the data bases used to identify and prevent terrorist acts and offenders. This approach also entails a shift in the operational philosophy of combating terrorism, from a strict prosecution of offenders to a more diagnostic early warning alert. Law enforcement organizations operate on the basis of a cognitive division of labour. A better understanding of the processes of what could be called collective cognition in the domain of law enforcement can help to improve overall performance while at the same time providing for a good protection of citizens' civil rights.

After the events of 9/11 the law enforcement and intelligence community was heavily criticised for having not been able to prevent these attacks. This can be seen as a classical case of hindsight bias. The individuals launching the deadly attacks on the Twin Towers were known to the intelligence agencies, they had been registered on a number of databases and had there been an early intervention, the course of history would have been different.

There are many prominent cases, where in principle intelligence and information about the offenders had been available before an incident but this knowledge was not used. While it is easy in hindsight to link the dots and paint the right picture one might ask whether an uncoordinated collection of information and intelligence by different, often competing institutions at different levels and with different agendas should be seen as the right approach. Often it also unclear whether the information collected is correct, reliable and whether fundamental rights of privacy and data protection can be honoured under such an regime. Below is a graphic representation about the intelligence avalieble – in principle – before the Boston bombings.



A standard reaction for bureaucratic organisations in situations after such an event is to add another layer of information processing or internal supervision to improve the future flow and use of intelligence within the organisation.

In a similar fashion each newly discovered mode of a terrorist attack creates a new mode of control. After the infamous shoe bomber Richard Reid had attempted to bring an improvised explosive device on board a plane, all passengers at U.S. airports had to go through security on their socks, while their shoes were processed through the scanner.
After an attempt to smuggle explosives in a bottle liquids were banned or the volume of liquid to be taken on the plane was restricted.
Since it has been found out recently that planes can be high-jacked by hacking into their computer systems while flying one might expect that Laptops will be banned on board planes as cabin luggage sometime in the future.

What these examples demonstrate is a way of linear thinking. If an established strategy produces a failure, the standard solution is to add more of the same. In most cases there are no stop rules for this more of the same philosophy. And since mass surveillance and data gathering is conceived to be the most promising strategy to combat and identify terrorists, more of the same is added after each event that was not prevented. **PPT 3/1**

In political debates this line of reasoning has produced heated controversies about balancing basic political values of freedom and security. Should civil rights and privacy be sacrificed and traded in for more security? Will more surveillance and more data for the law enforcement agencies significantly increase the level of security in a society?

The idea behind this approach is as simple as it is flawed. More data will put the intelligence and law enforcement agencies into a position to identify potential suspects before they can launch an attack. Keeping an eye on hundreds or even thousands of individuals, identified as potential suspects, will help to prevent future terrorist attacks. Collecting information about violent extremist groups will produce hints about future terrorist events.

While this strategy may look reasonable on paper a closer look at how it is implemented in the day-to-day workings of law enforcement yields a different picture. There are a number of criticisms that have been brought forward against a law enforcement strategy based on increasing mass surveillance, intruding the private sphere of citizens and collecting data from all different sources. After the revelations of Edward Snowdon about the activities of the NSA large segments of the general public in the U.S. and Europe reacted rather sceptical and rejected the idea of mass surveillance pursued by intelligence services.

I will not discuss these issues here. I think they miss the point. Of course it is a legitimate cause to fight for privacy, freedom of speech, and civil rights and to defend a liberal society against massive and intrusive surveillance regimes. The operation of law enforcement agencies has to be governed by legal and constitutional standards. This goes without saying. My staring point is different. I start from the assumption that more data and more surveillance will not help to find the proverbial needle or needles in the haystack. So I am criticising the dominant strategy not on legal and normative grounds of political theory but I think it can be demonstrated that it fails for practical reasons.

The chief of the Swiss national intelligence service in a discussion about legal reform of the Austrian intelligence service rightly suggested, that instead of producing ever-bigger haystacks we should focus on the needle and attempt to get a better picture of these objects of surveillant desire. Of course there are highly sophisticated methods available to process and analyse huge amounts of data from different sources, advanced algorithmic tools can help to identify patterns, pinpoint networks of communication and focus on potential suspects requiring close scrutiny. And of course this can be done on a global level, across jurisdictions and national borders. But this giant global drag-net is not based on a good and complex understanding what and who we are supposed to look for. Risk profiles are notoriously imprecise and tend to produce a substantial number of false positives, leading to an overload of surveillance manpower. Algorithms can help to process and sort huge amounts of date, but their output ends up at the desk of human beings. And – as in most cases, where ICT is involved – the human brain is the bottleneck in the decision process leading from intelligence to practical action.

So what remains at the end of the intelligence and data-processing food chain is the bottleneck of human intelligence and bureaucratic-administrative decision-making. Human actors have to decide what is important. They have to produce written threat assessments informing higher-level policy makers and senior officials. At the end of the day decisions have to be made and someone has to be held accountable for it.

There is this anecdote about the angry reaction of the U.S. intelligence services after 9/11. They were blamed for not informing White House officials in time about the imminent threats of a serious terrorist attack. White House received a daily security brief

summarizing what intelligence agencies had collected the previous day. This briefing paper was a highly condensed and of course highly selective summary of what thousands of analysts around the globe were reporting to their hundreds of superiors who reported to their bosses who then finally drafted the daily briefs for the top-level security advisors at the White House. Unfortunately these briefs did not contain a warning about the events of 9/11. Being criticised for their failure from all sides, the intelligence community angrily suggested delivering the complete volume of data to the White House on a daily basis. Terra bytes of data would then end up on the desks of the senior intelligence advisers of the President to draw their conclusions with regard to the next steps to be taken. Again the needle and the haystack.

I think this anecdote nicely demonstrates an important problematic of mass surveillance and the fight against terrorism in a nutshell. Single events cannot be predicted from mass data. And furthermore identifying potential criminals or terrorists on the basis of theoretical assumptions, what makes an individual a dangerous individual are deemed to fail. Using machine-based algorithmic reasoning for mass data, to create and search so-called data-doubles of individuals and/or groups not only entails the risk of creating huge numbers of false positives but also violates fundamental rights of citizens
.
While there are a small number of success stories of individuals or groups presumably preparing a terrorist attack identified and arrested before they could do any harm, my guess would be that upon closer inspection these cases were heavily relying on what could be called good old police and intelligence work. And all good police and intelligence work is local, based on local knowledge, using local contacts, acting in local contexts. Of course modern terrorism is tied into international networks, spanning the globe. But apprehending potential wrongdoers still is a local achievement on the ground.

Emphasizing the local character of police work of course does not mean to reduce policing to the officer walking the beat and talking to the locals or to go back to the good old days when policing was primarily community policing. Policing and intelligence work are comprised of highly differentiated and complex tasks displaying a high degree of division of labour and professional specialization. And all this involves a lot of technology and data processing. But it should be considered that all this is rooted in ground-level police work involving officers doing their job in the real analogue world. From there information is moving up the hierarchy and is transformed and changed.

Let me give you an example of how the focus on local, low profile and in some respect also low-tech surveillance and data gathering can be combined and integrated with a global approach. I recently stumbled across an investigative feature about the Catholic Church on ARTE, the European TV-channel. In this feature a high level official from a National Security Service from an Eastern European country explained why the Vatican is considered to be one of the most important places for the intelligence community and a hot spot for spies from all nations. The Vatican can be interpreted as the central hub of a global intelligence network, where information from countries all over the world is collected and processed. Local parish priests in remote areas of the globe are important sensors for shifts in public sentiments and as community leaders they also can have an impact on these communities.

Locally collected information flows and is synthesized within a complex layered network of catholic officials at different ranks creating assessments at regional, national

and finally global levels. And while catholic priests have a privileged access to highly private information in the confession box, they can create intelligence without breaching their vow of secrecy or professional confidentiality. You could say they work on the basis of privacy by ethical design. In this feature on ARTE the role of the Vatican under Pope John Paul II for the decline of the former Soviet bloc was reconstructed and it was demonstrated how Rome cooperated with Western intelligence services to foster this process. It became clear how Roman Catholic intelligence became a valuable source for the global intelligence community of the West in managing the decline of the Soviet Empire.

Now don't get me wrong. I am not suggesting theological experts should be hired for the fight against terrorism. Although this is done, as we know, when bringing Imams in to address potential suspects in Western Islamic communities and to inform the Intelligence community about dangerous individual. But what the case of the Vatican demonstrates is a structural and cultural pattern of how to organize and shape the relations of communication in intelligence work. And at the same time one might start to think about operational philosophies, objectives and approaches for good intelligence work based on such a model.

Understanding the fight against terrorism primarily in a framework of thief taking, supported by mass surveillance seems not be a successful strategy. Trying to locate and identify single individuals on the basis of technology supported mass surveillance in order to bring them to court before they commit a terrorist act did not work in a significant number of cases since 9/11. At the same time this approach created massive side effects in terms of public concern and critique. The Snowdon revelations started a worldwide protest movement and created a new awareness for privacy issues leading for example to the development and spread of new encryption technologies making it more difficult for law enforcement to collect data from electronic communication channels. I will return to this problem later. But let me first have a look at what I termed the relations of communication.

In a study we conducted for the Austrian Ministry of Interior on how to address the problem of right-wing extremism in the country, we interviewed members of the national state police to find out how they gathered and processed intelligence about extremist groups and individuals. Austria has a somewhat a-typical system, where the national intelligence service is legally and administratively a part of the national police. This hybrid construction has been criticised for long time by many observers and presently minor reforms are underway. At the same time this hybrid constructions allows for the analysis of different types of police work and the problems emerging at the interface of these two domains of traditional policing and intelligence work.
In our study we tried to understand how the relevant actors in the force identified potential suspects, how they collect, document and process information about right wing extremists in Austria, how the exchange of information and intelligence is organized and how decisions are made about future operations leading to court cases for politically motivated illegal acts from right-wing extremists. We conducted extensive interviews with members of the police at different levels trying to understand their daily work routines and finding an answer to questions like: what does it mean to investigate, identify and observe right wing extremism on ground level, what activities are involved here and how are the observations and findings documented and then processed through the or-

ganisations along the chain of command and communication? How is practical observation transformed into written documents?
How are they transformed, summarized and condensed? How do they impact the performance of the organisation?

What became obvious at an early stage were the problems arising from the hybrid system combining police and intelligence work within one organisation and legal framework. There were a number of mutual misunderstandings and conflicts. The conflicts we identified represented a microcosm of the global situation, where competing intelligence agencies operate with different rationales, creating silos of knowledge not shared on the basis of mutual recognition, trust and understanding.

Members of the police in Austria only had limited capacities to collect intelligence before any reasonable suspicion could be substantiated. The organisation was designed as a standard and traditional thief taking enterprise: locate a suspects, collect evidence and bring him to court. Now locating and identifying right wing extremists requires first of all an understanding of what constitutes an indictable offence in this domain. This was not always easy, given the legal, organisational and operational constraints.

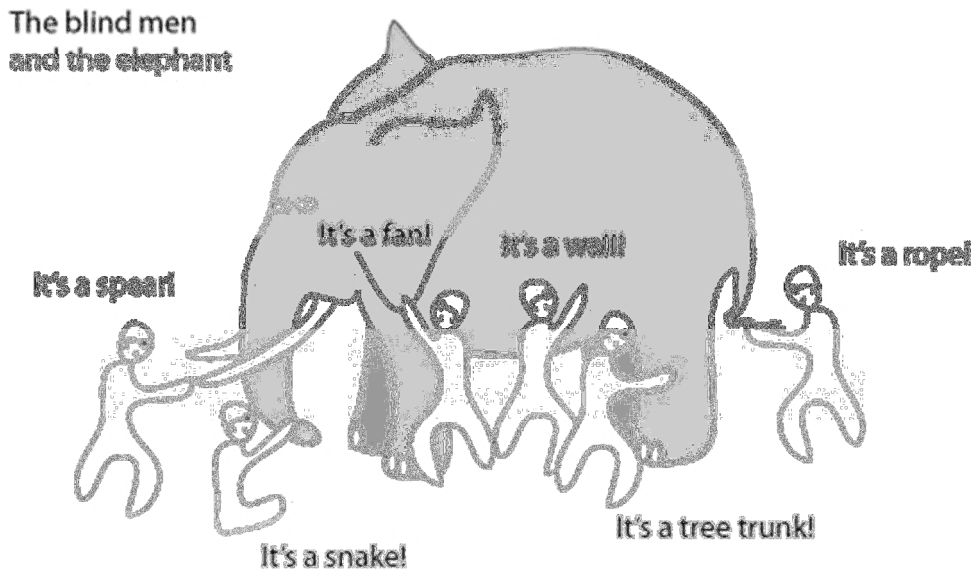
One the one side, from an intelligence perspective it is helpful to identify the larger social context of a single offender trying to find out whether s/he operates within a larger network. From a strict law enforcement perspective it is important to document person-related evidence for the prosecutor and the courts. And this is a different task.
Both tasks have to be performed at ground level before they can be reported to and processed by the higher levels of the organisation. Austria has specially trained police officers located in police departments across the country who have the task to act as "sensors" identifying potential right-wing extremists by simply keeping them under close observation.
The problem these officers face is that they are not integrated into the thief-taking model. It is difficult to determine their effectiveness against standard criteria of performance and internal controlling. Observing informal networks of potential right-wing extremists is a time consuming task and does not lead to immediate results, measured as numbers of arrests within the police logic.

At the same time it is difficult to identify such networks from a police officer's perspective. When is a group of individuals a network? At what level should police intervene and start formal investigations or even make arrests? When you ask police officers such questions, they cannot give you a precise answer. What you get are anecdotes about single cases: "well there was situation XYZ and then we did ABC."

It was also interesting to find out that different local branches of the police had different ideas of how serious the threat from right-wing groups was and what would constitute a situation that required formal intervention or investigation. Not only were there local interpretations of right wing extremism, there were also interesting and very different interpretations about the overall quality of work within the organisation. The top-level management presented the work of the intelligence apparatus quite differently than field operatives at ground level. This can be found out using a methodological approach of asking the mice to learn the truth about the cats. And as we know: the final decisions are made at the top. Somewhere "out there" there was a phenomenon labelled as right-wing extremism, but all individuals involved entertained very different ideas, what this

phenomenon looked like, how it should be addressed and what could be done to prevent its growth. The situation reminded of the tale of the

In conducting this study we acted as trusted outside observers. Members of the organisation at different levels and in different regions presented us their views of their work and also of their view of the overall organisational structure and in the end we had a complex patchwork of different interpretations, that reminded us a bit of the story of the blind men and the elephant.



And of course there were also complaints. Field operatives were complaining about central management because they had to file too many reports and permanently had to respond to requests they did not understand. They never would receive any feedback from their superiors and did not understand the rationale behind the requests they received. Top-level managers on the other hand were complaining about low compliance and a lack of understanding among the field operatives.

Now what can be learnt from this situation for the fight against terrorism and mass surveillance?
First of all we drafted a map of the relations of communication within the organisation: who is talking to whom about what, when, in which format. As it turned out the most important channels of information were informal. This was true for horizontal as well as for hierarchical communication.

Then we suggested a single interface for the regional offices across the country reporting to the central unit. Such a one-stop-shop approach made it easier to communicate across hierarchies and helped to avoid duplications of request for information.

Finally we suggested more regional face-to-face meetings with officers involved in observing right-wing extremism. This could help to increase the communication links, based on personal relations and at the same time provide a platform to exchange intelli-

gence by sharing stories about what had been observed at ground level. Officers were presenting case stories and sharing such stories improved mutual understanding of the overall situation. Representatives from the central management were participating at these regional meetings.

Such an approach helped to produce a shared knowledge base about right-wing extremism in terms of a culturally contextualized understanding of what was going on in the country. Discussing cases among colleagues and sharing information from local activities helped to link the dots to get an overall picture of the situation. It also helped to identify potential hot spots for right wing extremist activities across the country. Locating such hotspots or networks or even individuals it was then possible to start standard police operations, and involve the public prosecutor's office to get search warrants and even make arrests.

What we tried to achieve in our study was a better understanding of different tasks of policing the problems emerging from terrorist or political extremist groups and individuals.
Intelligence work should primarily be understood as an early warning system and that is different from making arrests and bringing potential suspects to court. Each of these tasks requires a different type of knowledge, information or intelligence. Producing huge data sets from mass surveillance is not very helpful for intelligence work. Predicting a terrorist act or preventing it on the basis of individual cases is impossible. What can be achieved is a better understanding of general threats. The situation here is like observing a pot with water where you can say that above a certain temperature it will start to boil and bubbles will appear on the surface, but it is impossible to determine, where exactly the bubbles will appear. When investigating terrorism the situation is similar. You can assess the probability but you cannot determine the precise location or event.

Mass surveillance data taken in isolation are not very helpful here. They produce digital and de-contextualized information that is difficult to link with local events.

Adopting a strategy based on the model of a more analogue, narrative format can help to put all experts involved on the same page and by providing a shared communicative space it helps to sort out misunderstandings and misinterpretations. The intelligence produced here then can inform police to take immediate action and start the standard law enforcement procedures eventually leading to the arrest of potential suspects. Keeping both of these activities apart is helpful to meet the standards of data protection and civil rights and also set a limit on mass surveillance.
As we could see in our study, all intelligence is local and when collecting local knowledge to get an overall picture, there are successful cases of organisations like the Roman Catholic Church and heir global network that have been active in the business of global intelligence over hundreds of years to be studied. They rely on knowledgeable, local trusted informants, integrated in the community they observe and a dense network of exchange and communication within the organisation. Of course we should not take over their objectives and try to establish a society of saints on earth. But good police and intelligence work can help to secure the conditions for an open society where different individuals and groups find their space while at the same time working within the limits of privacy and data-protection laws.