EX POST PAPER

Triple P: Coordination and collaboration between police, prison and probation services in dealing with violent extremist and terrorist offenders

Introduction

The cooperation between police, prison and probation services around (violent) extremist and terrorist offenders[1] is of great importance with regard to managing security and promoting resocialisation. It is a key triangle in the larger multi-agency cooperation that also encompasses other stakeholders such as prosecution, local municipalities and social work.

At their joint meeting in September 2018, the RAN Working Groups on Police and Law Enforcement (RAN POL) and on Prison and Probation (RAN P&P) zoomed in on the challenges and opportunities for police, prison and probation (Triple P) collaboration with regard to this specific group of suspects and offenders. Practitioners discussed information sharing, working with risk assessment tools and contributing to a rehabilitation process. They observed that information sharing lies at the heart of the collaboration and coordination of Triple P and noted that the legislative framework — which forms the cornerstone of these three services — can both help and hinder information sharing. All three sectors perform risk assessments, but while prison and probation services are likely to use similar tools, the police (and intelligence services) often use different tools. This dissimilarity is not necessarily problematic, if the various tools are known and interpreted in the same way. Concerning rehabilitation, the three sectors have a common goal but a different emphasis. More stakeholders outside the criminal justice sector need to be involved.

This paper was written by **Merel Molenkamp and Lieke Wouterse**, RAN Centre of Excellence.
It is based on the information and opinions expressed at the joint meeting of RAN P&P and RAN POL.

[1] When referring to (violent) extremist and terrorist offenders, we mean those charged with or convicted for terrorist (or related) crimes, but also offenders charged with or convicted for other crimes who have shown (violent) behaviour connected to extremism.

Information sharing

To ensure and enable effective information sharing, a legal and policy-making basis is necessary. The legislative framework in the EU, between and within Member States, provides a cornerstone for what information can and cannot be shared, with whom, under which circumstances and for what purpose.

As expressed at the meeting, in an ideal situation all agencies would have access to all data at any time. This vision is unrealistic not only due to legal restrictions, but also for organisational reasons. For each agency to process all information and decide what is relevant for them would be impossible both in operational and financial terms.

A distinction must thus be made as to what information is shared with which agency, under which circumstances, and how this information may be used. However, pinpointing what kind of information is relevant in each case is difficult in the context of preventing and countering violent extremism (P/CVE), because many factors can be of influence. Usually, it is the combining of information that leads to indications of risk or threat. How can this be organised in agreements and protocols?

An example from Germany:

The legal framework for data exchange

In Germany, increased attention and an extended mandate to deal with violent extremist and terrorist offenders went hand in hand with looking into the information sharing opportunities between prisons and security agencies. From a legal point of view, this situation coincided with two developments that influence the sharing of data: changes in the German constitutional framework and modifications of the legal framework at EU level.

Within the German constitutional framework, the possibilities and constraints arising from two judgements of the German federal constitutional court[2] mainly concern four principles that influence information sharing;

- ***Principle of purpose:*** Personal data should be collected and processed for specified and explicit purposes and their subsequent use may only be authorised in accordance with strict conditions. Information cannot be transmitted automatically by one state or authority to another.
- ***Hypothetical re-collection of data:*** Data may be used (and shared) even when the initial purpose has changed — if the new use is of equal weight and if there is a specific occasion in the individual case that calls for the transfer of data.
- ***Blanket monitoring:*** Surveillance that is carried out over an extended period, encompassing almost every movement and expression of the person under surveillance, and that could constitute the basis for a personality profile is incompatible with human dignity. In a prison setting this is quite a problematic principle. Is simply excluding talks with clergymen sufficient to comply with this legislation?
- ***Principle of separation of information****:* Data may generally not be exchanged between intelligence services and the police. Transfers of data between intelligence services and the police for use in potential operational actions

[2] Federal Constitutional Court´s (Bundesverfassungsgericht) judgement of 20 April 2016 (1 BvR 966/09, 1 BvR 1140/09) and judgement of 24 April 2013 (1 BvR 1215/07).

therefore normally have to serve a particularly important public interest.

These principles influence information sharing between security services and prisons. Given the specificities of data collection in prisons and the high risks that could potentially arise from not sharing this data, the information gathered in this setting can in fact be transmitted fairly easily even in line with the new principles — it just cannot be shared automatically. It is therefore important that prison staff be well trained to recognise potentially dangerous behaviour (and not to raise the alarm unnecessarily). One possible easy way to share or check information on potentially dangerous behaviour would be to report the possible danger anonymously — so no personal data is collected.

EU Directive 2016/680 focuses on '*the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*' This directive sets out extensive requirements for transparency, individual rights and individual legal protection, as well as supervisory control of data processing. It will lead to a paradigm shift, as it calls for data exchange with security authorities to be disclosed. In future, the exchange of information will thus be subject to even greater discipline and bound by stricter rules and protocols.

As a response, the German federal states have submitted a model law to the Conference of Ministers of Justice. The model law takes into account the case law of the Federal Constitutional Court, implements the Data Protection Directive and thus provides a legal framework for cooperation between the prison system and the security authorities.

Knowing what information is relevant to share with other agencies requires knowledge about the phenomenon of violent extremism and radicalisation. As with other criminal cases, the single puzzle pieces individual actors may hold can combine into valuable intelligence when viewed together. As the information being shared is sensitive, all agencies must be trained to deal with it.

Discussions in the meeting indicated that security services, by nature, are very adept at handling sensitive information, but that this is not always the case for prison services. Security services monitor and collect information 'from a distance' and are mostly interested in the extent to which someone is engaging in potentially criminal behaviour (who they are in contact with, what they are exchanging, whether there are indicators for plotting an attack in or outside the prison, and so forth).

For prison management and staff, the situation is different. They are in constant contact with the violent extremists / terrorist offenders in their care and consequently need other types of information about these individuals (such as what is their background is, where they are coming from, whether there is a risk of aggression towards the staff, and whether there are particular risk factors and protective factors). In addition, they are tasked with supporting a rehabilitation process. For probation officers, it is very important to know whether their clients — with whom they are not in constant contact — may pose a threat to themselves or others. However, they are quite used to working on a 'need to know' basis.

Clearances and vetting processes are preconditions for a structure in which information can be shared. On the strategic level, agreements and protocols can be made to share detailed, sensitive information. On the operational level, information can be shared on a 'need to know' basis.

For the operational side, this means that, instead of all collected data, only information relevant to the agency or agencies dealing with the offender is shared. Besides a legal framework for information sharing, trust is a very important issue in this respect. Agencies need to be confident in each other's expertise and ability to decide what information is relevant to share. Transparency about the structure of information sharing is helpful too. Instead of receiving all data, agencies would then be aware who has information.

The meeting also explored the risks and responsibilities associated with decisions to share or withhold potentially relevant information. With regard to terrorist suspects and offenders, risk acceptance is typically low, and the profile is high in terms of political and public attention. When an incident or attack occurs, questions are quickly raised about who held what information and who (or which agency) made mistakes in their processes, allowing someone to slip through the net. As a result, the atmosphere surrounding the authorities' work and the sharing of information can be tense. One possible way forward could be to adopt a principle by which the owner of the information holds the risk — which would mean that a person deciding not to share information could be held accountable if something goes wrong. In agreements and protocols, a paragraph should be included about responsibility.

The extent to which information that is being shared can be acted upon or used in decision making is also a relevant aspect in this regard. If sensitive information about a suspect or offender is shared, but using this information is not allowed (e.g. because it could endanger an infiltration attempt in an extremist group in prison), this would mean that the original source of the information is still the owner even though it was shared.

An example from Spain:

Organised information sharing between prison and police

In Spain, prison intelligence is gathered about prisoners through direct control and observation. This information is shared and recorded in the prison computing system, which can be accessed by a coordination group.

This group is composed of Civil Guard members, police officers and translators. It advises the prisons about security plans and the profile of visitors. It can also provide training. Based on the intelligence reports, a risk assessment is performed for individual prisoners. Depending on the severity of the crime, the risk of escape, the individual's connections with other prisoners and so forth, inmates are given a classification.

The classification indicates whether a prisoner should be placed in a closed, ordinary or open regime. For violent extremist offenders (amongst others), there are special prisoner tracking files.

As prisoners in this group pose more risk, they have stricter monitoring and control measures. There are also special monitoring measures to prevent Islamic radicalisation, which are for example used for prisoners vulnerable to this phenomenon.

Most information for the coordination group thus originates from the monitoring of these prisoners. The information is stored within the prison computing system, which the group can compare with the police database. Information from police and prison about violent extremist offenders is thus shared between the prisons and the police.

Risk assessment

As the Member States all have different structures for police, prison and probation, there are different monitoring and risk assessment systems in place, and agencies responsible for these systems also differ.

Examples of structures that can be used to conduct multi-agency monitoring and cross-check outcomes are case conferences, observers in prison or security service units in prisons. With regard to specialised risk assessment tools, VERA2R has now been adopted by many prison and probation services, but it is less commonly used by police and other security agencies.

To use these tools, specific knowledge and training is needed to identify and correctly interpret signs of risk. Risk assessment tools do not replace professional judgement, but they help to ensure that threats are evaluated objectively and that measures taken in response are duly justified. They can substantiate a professional's gut feeling and can be useful when analysing information for decision-making purposes.

In multi-agency cooperation, it is very important to understand each other's tools and the meaning of their outcomes. The outcomes of different tools or monitoring systems can serve as common building blocks and can also be used to cross-check each other's outcomes.

Cooperation is easier if there is a shared language. Awareness of the systems that are in place in other agencies and of the way they are used is a first step towards creating a common language and avoiding duplication. When information is duplicated in different systems, this can lead to false alarms. In Denmark, the prison and probation services were closely involved in the development of the risk assessment tool for the police forces. Although they do not use the exact same tool, the new tools build on the same foundations, and the systems employed by individual agencies are therefore easier to understand for the other services.

An example from Czech Republic:

SAIRO, a risk monitoring system developed by prison and police services

In the Czech Republic, the prison service, the police academy and the National Centre against Organized Crime (NCOZ) joined forces to develop SAIRO.

This web-based programme pulls information together to support early detection of manifestations of radicalisation during imprisonment. In view of national and international developments, the organisations involved recognised the need to work together to detect radicalisation in the prison environment. There was also a need to adapt the tool to the context in the Czech Republic (mostly right- and left-wing extremism).

The prison services lacked sufficient knowledge and capacity to develop an analytical tool. The NCOZ was able to contribute both, and it stood to benefit from more and better information from the prison service. The police academy got involved to help build a solid academic basis and conduct research for the project.

SAIRO was launched in 2017. It contains a collection of measures for obtaining information, which is built on monitoring of inmates during imprisonment (e.g. observation of manifestations and behaviour), then analysing and evaluating this information. To ensure safe sharing of information within the legal framework, some preconditions were put in place: security of data, app access via login, monitoring of the tool by top management of the prison service, different levels of access (user, administrator).

The inmate files are accessible for other prisons in case the prisoners transfer between prisons. This feature ensures continuity in the information available on the prisoner. Upon release of the prisoner, their file is placed in a repository. If the person reoffends, it is transferred back into the analytical tool. SAIRO is now being applied in a pilot version in Czech prisons.

Rehabilitation

For rehabilitation and reintegration, a supporting role for community police or local police can be beneficial to the released offender, both to increase trust in police authorities and to prevent reoffending (by obtaining relevant information from the released offender). This is positive not only for the released offender but also for their direct surroundings.

Contradictory situations can however arise when probation tries to move released offenders away from radicalised networks while these are operating as informants for the police. Informants will attempt to remain in the network to gather information, while a probation officer might be striving to extract the person from this environment. Building trust and sharing information with police (e.g. for a probation officer) can be a delicate balancing act. Transparency about each actor's role and responsibilities can facilitate the process and help to avoid conflicting approaches.

Collaboration with other actors outside the three Ps, such as NGOs, is also of crucial importance for successful rehabilitation. Given police and probation services' constraints in terms of the time to be invested, connecting with the offender's community through NGOs can be a positive cooperation. Vetting NGOs (as to their motives for involvement and their capacity to deal with sensitive cases for instance) is key to ensure they play a constructive role.

An example from Denmark:

A cooperation model involving prison and probation services, the police and other stakeholders

In 1998, a legal framework was established in Denmark to allow for exchange of information about citizens for crime prevention purposes and prison release. Three multi-agency structures were developed:

- KSP: prison & probation, police and social services,
- SSP: police, social services and schools (sometimes accompanied by prison and probation),
- PSP: police, social services and psychiatric services.

In addition, institutions known as 'Infohouses' were developed, in which the aforementioned networks are important partner structures. The overview below, which was provided by the Danish Prison and Probation services, shows how the Danish Intelligence service (PET), the police and the prison and probation services are situated in a larger multi-agency structure to prevent and deal with crime in general. Violent extremism and terrorism have been integrated in this structure.

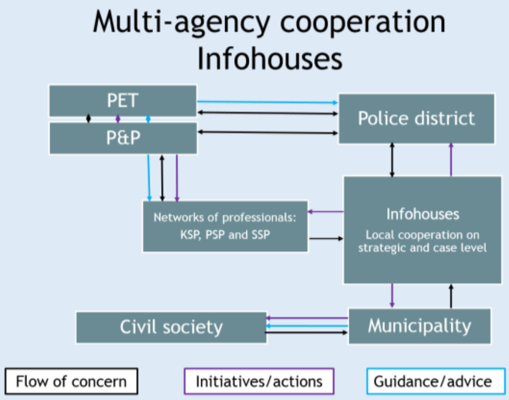

Figure 1: Multi-agency cooperation in Danish Infohouses (Hjørnholm, presentation 20 September 2018)