



HOOGHIEMSTRA
&
PARTNERS
strategisch en juridisch advies

pro facta

Summary comparative legal study
System for protective security



Colophon

Hooghiemstra & Partners
Bezuidenhoutseweg 161

2594AG Den Haag

www.hooghiemstra-en-partners.nl

info@hooghiemstra-en-partners.nl

This study - commissioned by Wetenschappelijk Onderzoek- en Datacentrum - was conducted by Hooghiemstra & Partners, a strategic and legal consultancy firm specialized in data (protection) and law and Pro Facto, a bureau for administrative and legal research.

Researchers: Thijs Drouen, Anna Keuning, Lieve Smeets (Hooghiemstra & Partners)
Heinrich Winter, Christian Boxum, Stan Roggeveen (Pro Facto)

Publisher: Wetenschappelijk Onderzoek- en Datacentrum (WODC)

Date: 18 December 2025

Guidance commission:

Prof. dr. mr. G.K. Sluiter (Chairman, UvA)

Dr. I.W.J. van der Vegt (UU)

Dr. E. de Busser (UvA)

Drs. P.S.M. Rademakers, followed up by mw. C.E. Stokhof (MinJenV)

Mr. W.M de Jongste (WODC)

Foto credit cover page:

Bosco Yun via [Unsplash](https://unsplash.com/)

The researchers are responsible for the content of the report and this summary. Contributing (as an employee of an organisation or as a member of the guidance committee) does not automatically mean that the person concerned agrees with the entire content of the report and this summary. This also applies to the Ministry of Justice and Security and its minister.

©2025 Hooghiemstra & Partners. Copyrights reserved.

Summary

Introduction

This study examined the protective security frameworks in a number of European countries. The objective of the study is to inform and support the further development of the Dutch protective security framework. Particular attention was given to the manner in which the collection, assessment and sharing of information are organised in the countries examined, in order to enable the protection of individuals facing serious threats.

On the basis of the findings from the countries studied, a conceptual framework was developed outlining the key characteristics of an effective protective security framework. This framework incorporates various elements drawn from the arrangements in the countries examined. It should be noted, however, that these elements cannot be considered in isolation from the institutional, legal and operational context from which they originate.

The study may serve as a source of inspiration for the Netherlands with regard to the organisation of coordinating responsibilities within the protective security framework, the structure and functioning of case-based coordination mechanisms, and the statutory basis governing the use of investigatory powers.

Background

In recent years, the Netherlands has been shaken by several serious violent incidents targeting individuals. These attacks have had a profound impact on the democratic rule of law and on the perceived sense of safety and freedom within society. Through the national system for protective security, the government fulfils its duty of care to protect citizens against serious and life-threatening harm. The system is under increasing pressure as the volume and complexity of threats continue to rise. In recent years, several studies have been conducted into the functioning of the Dutch system for protective security. The findings of these studies led to a revision of the system in 2023. A particularly important issue in this context concerns the legal basis for the system and the associated challenges relating to the collection and exchange of information in protective security situations. The Research and Data Centre of the Ministry of Justice and Security (WODC) commissioned a comparative legal study into the protective security of individuals in a number of European countries.

The Dutch system for protective security

The Dutch system for protective security is a cooperative framework involving the National Coordinator for Security and Counterterrorism (NCTV), the Public Prosecution Service, the police, the Royal Netherlands Marechaussee (KMar), the General Intelligence and Security Service (AIVD), the Military Intelligence and Security Service (MIVD) and mayors. Although there is no specific statutory basis for this cooperative framework as such, procedures and responsibilities are laid down in the Circular on Protective Security. The system determines how threat and risk information is translated into protective measures and which authorities are responsible for implementing those measures, with the Minister of Justice and Security bearing overall responsibility.

Safety is regarded as a shared responsibility of government, citizens and employers, with government intervention occurring only where others are unable to provide sufficient protection. Decentralized authority plays a central role, while the central government has a special responsibility for designated persons, objects and services. Threat assessments are prepared by the AIVD, MIVD and the police, while the police and the KMar implement protective measures under the direction of the Minister, coordinated through the NCTV.

There is no statutory basis in the Netherlands for the cooperative framework on which the system for protective security is founded. The tasks arising from the system are assigned by law to the Minister of Justice and Security and to the police. Tasks carried out by the police (and the KMar) are laid down in the Police Act. Powers exercised in the context of protective security are limited to the general task of the police and may involve no more than a limited interference with the right to privacy. As a result of these limitations, the police are unable to conduct in-depth investigations, and threats may persist without coming to the attention of investigative authorities. Where criminal procedural powers or special statutory regimes are not applicable, information can be gathered only on the basis of the general police task.

This leads to difficulties both when information must be collected from the perspective of the threat actor (an individual or group) in order to identify a concrete threat and its modus operandi, and when information must be collected from the perspective of the threatened individual in order to detect and analyse (potential) threats. In addition, the various partners involved in the system appear to operate in overly siloed ways, which undermines the preparation of adequate risk assessments and the adoption of appropriate protective measures.

Research questions

This report addresses the following central research questions (summarised):

1. How is the protective security of individuals organisationally structured in a number of EU Member States?
2. What is the legal framework in the selected countries for the collection and sharing of information relating to the protective security of individuals?
3. How is external oversight organised?
4. Has academic or policy-oriented research been conducted in the selected countries into the practical application of the relevant powers?
5. What lessons can be learned from practice in the selected countries regarding the collection and sharing of information?
6. Which elements from the countries studied could serve as inspiration for the Dutch system for protective security?

Research design

The study focuses primarily on individuals threatened by terrorism and organised crime, as these threats proved during the research period to be the most decisive for the functioning of the various systems and therefore yielded the most useful insights. Consequently, less attention is paid to the protection of (crown) witnesses and VIPs. Threats arising in a familial or relational context fall outside the scope of this study.

- A number of conditions guided the selection of countries for inclusion:

- The country falls within the jurisdiction of the European Convention on Human Rights (ECHR);
- A legal framework and some form of authority and oversight are in place;
- The competence to provide protective security to individuals includes at least the (online) collection of data;
- Relevant information can be accessed without disproportionate effort.

In addition, several further criteria were applied to ensure a varied selection of countries. These included:

- The organisation of the security and policing system;
- The nature of the legal system;
- Cultural and societal perceptions of security;
- The presence of international institutions;
- Historical experience with threats;
- The use of technology and innovation.

This resulted in an initial selection of Germany (the federal state of Lower Saxony), Denmark, Belgium, France, Italy, Spain and the United Kingdom. Following desk research, further in-depth analysis focused on France, Belgium, Italy, Denmark and Germany (Lower Saxony). Contacts were established through Dutch embassies to arrange interviews with relevant stakeholders. The amount of information that could be gathered varied by country, largely depending on the willingness of the authorities concerned to provide information. This resulted in a degree of imbalance in the data collected. The most comprehensive information was obtained for Italy, Belgium, Germany (Lower Saxony), France and Denmark.

For each country studied, the analysis addressed, where possible, the following features of the protective security system:

- The division of roles and relationships between organisations;
- Triggers for activating the system;
- Investigatory powers for information collection and threat assessment;
- Information sharing between involved parties;
- The adoption and implementation of measures;
- The evaluation and adjustment of threat assessments and measures;
- The scaling-down of measures;
- Oversight of the system.

Findings

Below, the key findings are presented per feature.

Division of roles and relationships between organisations

In all countries studied, the police are involved in the system for protective security, for example by providing information for threat assessments or by implementing protective measures. Italy is the only country that has established a dedicated organisation (UCIS) specifically to coordinate the system for protective security. UCIS performs several tasks, including assessing risk analyses, evaluating threat situations and deciding on protective measures. Italy does not operate a fully centralised system, as local and regional police forces and prefects—who are responsible for public order in their respective

areas—continue to play an important role. The advantage of a more centralised approach is that, in practice, it has led to improved information sharing and coordination within the system.

In France, a specific organisation (UCLAT) has been established to coordinate cooperation in response to terrorist threats. In Belgium, an organisation has been created with the specific task of coordinating threat assessments for security issues, including those relating to threatened individuals. Belgium is the only country in which the national crisis centre plays a role in the system that is comparable to the role of UCIS in Italy.

Denmark is the only country with a fully centralised system. In Denmark, the security and intelligence service is primarily responsible for the protective security of individuals. This service can be compared to a combination of the Dutch AIVD, the Royal and Diplomatic Protection Service (DKDB) and the NCTV. The Danish intelligence service collects intelligence, prepares threat assessments, determines which measures are required and subsequently implements the physical protection itself. As a result, Denmark has limited need to organise cooperation between multiple parties in this domain. This is noteworthy, as all other countries examined rely on cooperation between at least several actors within the system. In Germany, a distinction is made between federal-level and state-level tasks. At federal level, the Federal Criminal Police Office (Bundeskriminalamt) is responsible for the protection of a limited and specific group of individuals, while other tasks are assigned to the federal states.

Triggers for activating the system

The process of protective security can be initiated for various reasons. The study shows that, in all countries examined, the filing of a police report may serve as a trigger for activating the system. In Belgium and Italy, signals from other involved organisations may also initiate the process. In Italy, for example, signals may originate from local police forces. In Belgium, signals from the public prosecutor or information arising from consultations held by the national crisis centre may constitute a trigger. In Belgium, Italy and Denmark, it is important that the individual concerned files a police report, as this provides the legal basis for deploying criminal-law investigatory powers and for collecting information on the threat picture. Notably, in Belgium, signals from the media may also be taken into account.

Investigatory powers for the collection of information

France has established a separate legal regime governing the use of investigatory powers for the collection of information in the context of the protective security of individuals. In France, both the intelligence services and the police fall within the scope of the Intelligence Act, which grants them investigatory powers to collect information where there is a terrorist threat. These powers include the adoption of preventive measures and security zones, surveillance and monitoring, the interception of communications, and the use of emergency powers. In Belgium, the legislation explicitly provides that the intelligence services may deploy investigatory powers for the purpose of carrying out a protective security assignment for an individual. Such powers may be exercised only where ordinary methods are insufficient and where the use of investigatory powers is proportionate in light of the seriousness of the threat.

In Italy and Belgium, the police rely on their ‘traditional’ powers under criminal law. Information cannot be collected through investigatory powers solely for the purpose of ensuring an individual’s safety, but only within the framework of ongoing criminal investigations. When an individual files a police report, the police may initiate a criminal investigation, after which such powers may be deployed. Although

Danish legislation explicitly links intelligence-gathering by the intelligence service to the protection of individuals, the use of investigatory powers in Denmark likewise requires the existence of a criminal investigation. The most significant difference compared with other countries is that, in the context of the protection of individuals, only the intelligence service—and not the police—may exercise these investigatory powers.

In Lower Saxony, Department 25 of the State Criminal Police Office (Landeskriminalamt) has statutory powers to collect information for the purpose of preparing risk assessments. In none of the countries studied were organisations other than the police and intelligence services found to possess investigatory powers.

Information collection and sharing via other organisations

No explicit statutory provisions were identified in the countries studied that specifically regulate the collection of information from open sources. Instead, reliance is placed on more general statutory provisions granting organisations the competence to collect information. By contrast, various statutory provisions exist governing the collection and sharing of information with or through other organisations. No specific legislation was identified that relates exclusively to the collection and sharing of information in the context of the protective security of individuals.

Threat assessments

In all countries for which information was available, threat assessments are conducted using multiple threat levels. With respect to terrorist threats, it is notable that Italy, Belgium and France each operate a specific organisation responsible for coordinating threat assessments. These organisations serve as focal points where information collected by the various involved parties is brought together. The precise role of these organisations, and the manner in which information is shared with them, differs by country.

In Belgium (OCAD and DJO: a special department of the police) and France (UCLAT), threat assessments are partly conducted by these coordinating bodies themselves, on the basis of confidential information provided by the police and intelligence services. In Italy, by contrast, the coordinating organisation (UCIS) merely assesses the threat analysis prepared by the police for the purpose of determining protective measures. In Belgium, the National Crisis Centre (NCCN) subsequently carries out a comparable assessment of the threat analysis that has been partly prepared and coordinated by OCAD/DJO. Owing to the separation between the preparation and the assessment of the threat analysis, it is not necessary in Italy to share in writing the confidential underlying information on which the threat analysis is based.

In Lower Saxony, no separate organisation has been established for coordination and implementation. Instead, these tasks are assigned to a specific department within the State Criminal Police Office, which prepares threat assessments and adopts measures on the basis of police information. In Denmark, coordination takes a different form due to the centralised nature of the system. Because the collection of information, the preparation of threat assessments and their assessment for the purpose of implementing protective measures are all vested in the intelligence service, there is less need to organise cooperation and information sharing with other involved parties.

With regard to the preparation of threat assessments, Italy stands out in that the police also take the lead in preparing threat assessments for individuals threatened by terrorism. In Belgium, France and Denmark, this responsibility lies primarily with the intelligence services and/or the coordinating organisations. In Italy, the intelligence service mainly provides information at the level of phenomena, such as the nature of a particular terrorist group.

In cases involving organised crime, Italy relies on the same coordinating organisation as for terrorist threats. In France, such coordination is absent in the field of organised crime, and threat assessments are prepared by the police. Denmark differs most markedly in this respect, as the intelligence service also prepares threat assessments relating to organised crime, rather than the police.

Adoption, evaluation and scaling-down of measures

The study shows that the authority to decide whether protective measures are to be deployed for threatened individuals differs between countries. This is distinct from the question of who determines the content of those measures. It also varies whether this competence is vested in a single organisation or shared among several. In all countries examined, the threat assessment forms the basis for the measures to be adopted, although the manner in which it translates into concrete measures differs.

In Italy, both the specially established coordinating organisation (UCIS) and the prefect decide whether measures are to be deployed. Although standard packages of measures exist, the extent to which measures are predetermined or require a case-by-case assessment depends on the threat level. A notable feature of the Italian system is that it allows room for tailored solutions and is not strictly bound to fixed combinations of threat levels and measures.

In France, the Minister of the Interior decides whether protective measures are to be deployed. It is not known whether France uses standardised packages or tailor-made measures for each protected individual. The Minister decides on the basis of threat assessments and receives advice from a committee when determining the content of the measures.

In Belgium, the National Crisis Centre is competent to decide on the deployment of measures. The NCCN prepares a threat evaluation based on information received from OCAD and a specialised police department. On the basis of the threat level—ranging from level 1 to level 4—it is determined which measures are appropriate in a given situation.

In Denmark, the Danish Security and Intelligence Service (PET), as the organisation responsible within the national system for protective security, decides on the deployment of measures.

In all countries examined, protective measures and threat assessments are evaluated, at least when new information becomes available. The same applies to decisions on scaling down measures.

Oversight

Oversight of the system for protective security is organised in different ways across the countries studied. France has established an advisory body as an independent oversight mechanism. This body may issue non-binding advice in advance on the powers of the intelligence services and may also exercise ex post oversight. Denmark has a parliamentary committee tasked with overseeing the intelligence services, which advises the government orally or in writing. In Belgium, two standing committees are responsible for overseeing the parties participating in the system for protective

security, including with regard to the protection of personal data. In Germany, external control is organised through parliamentary oversight.

Italy is the only country examined that does not have a formal oversight body in the form of committees or authorities. In Italy, oversight takes the form of ministerial responsibility, with the Minister of the Interior bearing ultimate responsibility.

Inspiration for the (draft) legislative proposal on investigatory powers

This study was conducted to provide inspiration for a (draft) legislative proposal aimed at creating autonomous powers for tasks in the field of protective security in the Netherlands. Because the systems for protective security in the countries studied all operate within their own societal and legal contexts, it is not possible to transfer those systems, or even specific elements thereof, directly to the Dutch situation. For this reason, a reference model for a system for protective security was developed, consisting of benchmark criteria derived from the findings of the study. These benchmarks were elaborated using practical examples from the countries studied. The benchmarks are as follows:

- Access to the system is adequate;
- Coordination between parties is adequate and roles are clearly defined;
- There is a clear legal basis for collecting and sharing information;
- There is a clear legal basis for the use of investigatory powers;
- Threat assessments are adequate and usable;
- The evaluation of measures is effective;
- Oversight is coherent and effective.

The following sections describe these benchmark criteria of the reference model and provide examples of how they are implemented in several of the countries studied, which may serve as inspiration.

Adequate access to the system

When designing access to the system, a key dilemma arises. From an efficiency perspective, it is not desirable for the threshold for access to be too low; at the same time, threatened individuals must be able to find their way to the system. Belgium offers a compelling approach in this respect. When an individual files a police report, it is forwarded to the National Crisis Centre (NCCN). The NCCN assesses the report on the basis of a threat analysis and estimates the protective measures to be taken. The NCCN may also initiate the protective security process on the basis of other signals.

Adequate coordination between parties and a clear division of roles

Effective and efficient coordination requires that the number of organisations involved are limited. At the same time, important information and expertise relevant to protective security tasks may be dispersed across many different organisations. In Belgium, Italy and Germany (Lower Saxony), a single body has been designated to perform the coordinating role. In our view, this provides the necessary degree of decisiveness without sacrificing access to knowledge and expertise.

A clear legal basis for collecting and sharing information

When collecting information, it is essential on the one hand to be able to gather and share sufficient relevant information, while on the other hand avoiding disproportionate infringements of the right to privacy. In Denmark, the Danish Security and Intelligence Service (PET) has the authority to collect all

relevant information itself. In addition, the PET may request information from, for example, local police forces. This process is surrounded by appropriate safeguards.

A clear legal basis for the use of investigatory powers

Investigatory powers may be necessary to collect crucial information, but they must be exercised in a manner that is necessary and proportionate. In France, the investigatory powers that may be deployed are clearly regulated in the Intelligence Act, which also specifies the requirements applicable to automated data processing and the manner in which information may be collected via other organisations.

Adequate and usable threat assessments

Protective measures must be proportionate to the actual level of threat. An excess of measures is inefficient, while insufficient measures entail security risks for the individual concerned. For this reason, an adequate threat assessment is essential. In Denmark, this task is assigned to a single organisation, which conducts assessments on the basis of current and comprehensive information, resulting in a high degree of accuracy. In Belgium, a dedicated organisation has been established to coordinate threat assessments and prepare threat evaluations, ensuring that information from the various involved parties—each with its own expertise, such as organised crime and terrorism—is brought together in one place.

Effective evaluation of measures

Periodic evaluations of protective measures are important to ensure that the package of measures remains aligned with the changing circumstances of the threatened individual. At the same time, it is important to avoid both over-evaluation and under-evaluation. In Belgium and Italy, measures are evaluated at least when new information becomes available that is relevant to an individual's security situation, for example when a suspect is arrested. In addition, cases involving threatened individuals are discussed periodically—every three months in Belgium and Italy, and every six months in Italy.

Coherent and effective oversight

Effective oversight is crucial to the proper functioning of the system for protective security. The central dilemma is that effective oversight requires transparency, while the nature of certain information may limit openness. France and Belgium have addressed this challenge clearly. In France, an oversight body has been designated to supervise the system as a whole. In addition, an independent committee has been established to advise on privacy-related issues concerning the use of intelligence-gathering instruments. This committee may issue non-binding advice in advance and may also exercise ex post oversight. Belgium has chosen to entrust oversight of the parties participating in the system for protective security to two standing committees.

HOOGHIEMSTRA & PARTNERS
strategisch en juridisch advies



Bezuidenhoutseweg 161, 2594 AG Den Haag • **T** +31 (0) 6 39 27 85 33
E info@hooghiemstra-en-partners.nl • www.hooghiemstra-en-partners.nl
ING Bank NL49INGB0008938076 • **KvK** 73390356 • **BTW** 8595.06.447.B01