



Time for Openness

A comparison of
public reporting
by security services

The Hague Centre for Strategic Studies N° 03 | 03 | 10



Time for Openness

A comparison of public reporting by security services

The Hague Centre for Strategic Studies

Teun van Dongen, Olof Craenen, Tomas Luinkes, Niek Oude Essink Nijhuis en Daan van Spankeren.

© 2010 The Hague Centre for Strategic Studies. All rights reserved. No part of this report may be reproduced and/or published in any form by print, photo print, microfilm or any other means without previous written permission from the HCSS. All images are subject to the licenses of their respective owners.

Graphic Design *Studio Maartje de Sonnaville, The Hague*

*The Hague Centre
for Strategic Studies*

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
www.hcss.nl

Time for Openness

A comparison of public reporting
by security services

The Hague Centre for Strategic Studies N° 03 | 03 | 10

The Hague Centre for Strategic Studies (HCSS) seeks to advance international security in an era defined by geopolitical, technological and doctrinal transformation and new security risks. HCSS provides strategic analysis and offers concrete policy solutions to decision makers. HCSS serves as a strategic planning partner to governments, international organisations and the business community.



Table of Contents

	Executive Summary	7
	Introduction	9
1	Openness of security services	15
2	Security threats	23
	Conclusion	43
	Sources	47

Executive summary

This report analyses the information that security services publish in their annual reports. First, we examine the differences in openness of the annual reports. Second, we compare the information that is given about security threats. Our analysis of the annual reports shows that security take quite different approaches when it comes to informing the public.

- The Swedish, Czech, Danish and Austrian services shield their information about security threats but are more open about their own activities.
- The German and Swiss services take the opposite approach: they are quite open about security threats, but less open about their own activities.
- The Dutch AIVD takes the broadest approach, as it is relatively open about both security threats and its own activities.

Regarding the security threats, the following observations can be made:

- The threat universe appears to be similar for all services. They identify largely the same threat categories, except organised crime and animal rights extremism, which are not discussed by all services.
- The left-wing extremist movement is generally considered weak and fragmented.
- Although few services see right-wing extremist movement as more than a threat to public order, the movement is generally considered to be on the rise.
- All services emphasise the fragmentation of islamist extremism. Some (Sweden, Switzerland, Norway, the Czech Republic) see their countries as potential targets for attacks by islamist extremists, whereas others (Germany, Denmark and, until recently, the Netherlands) claim that their countries are logistical bases rather than targets.
- The two countries (Switzerland and the Czech Republic) that address organised crime report worrying tendencies of criminal organisations to infiltrate the legal and public sphere.
- China and Russia are considered the main espionage threats. Both countries take a broad approach and are engaged in different kinds of espionage (economic, technological, political, military).

Introduction

Secret services are facing growing demands for accountability, that is, they are increasingly pressured to explain the choices they make and the use they make of the tools and powers they have been granted to counter threats to national security. This accountability takes place within various constellations. For example, there is the possibility for citizens to file complaints against secret services. Citizens may hope that, as a result of such a procedure, a secret service will be ordered to cease a certain practice, for instance approaching potential informers under a false identity.¹ Second, most, if not all, democracies have arrangements for parliamentary oversight. In many such cases, a selected group of parliamentarians has access to secret information to see whether a secret service has violated its mandate. At the request of the Dutch intelligence and security service (AIVD), the mechanisms for parliamentary oversight of six countries were examined in a benchmarking exercise done by CCSS (CCSS 2005).

This report showed that there are fairly elaborate mechanisms to hold the Dutch secret service to account for its actions (Minister of Internal Affairs and Kingdom Relations 2005, p.3). The current report will address a third form of accountability: communication from the services directly to the public at large.

Again, the goal is to compare a group of countries to see how they fulfil their obligations regarding accountability. This report will also look at how the information about security threats differs from country to country. Possibly in response to demands of an increasingly critical public, some services have started releasing publicly available annual reports. It is this type of information that forms the starting point for this report.

1 See for example Nationale Ombudsman, Jaarverslag Nationale Ombudsman 2004 (Tweede Kamer vergaderjaar 2004-2005, 30 030); 429-430. The Ombudsman decided that the AIVD had acted rightly in this case.

This report will first analyse the annual reports of security services of some selected countries to assess the openness of the services. There is an obvious need for secrecy in the work of security services, but the demand for openness is becoming more pressing. This exercise will show the different ways in which security services have struck that balance. Second, our analysis will compare the threat perceptions presented in the reports.



Figure 1. COVER PAGES OF THE ANNUAL REPORTS

Given the availability of the source material, this study focuses on annual reports of services that have a mandate for internal security. Consequently, the section on security threats will only address threats insofar as they manifest themselves on European soil, more specifically northern and central Europe, as the set of surveyed countries consists of Austria, Belgium, the Czech Republic, Denmark, Germany, the Netherlands, Norway, Sweden and Switzerland.

The security services from these countries and their acronyms are the following:

- Austria: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)
- Belgium: Veiligheid van de Staat / Sécurité de l'état (VSSE)²
- Czech Republic: Bezpečnostní informační služba (BIS)
- Denmark: Politiets Efterretningstjeneste (PET)
- Germany: Bundesamt für Verfassungsschutz (BfV)
- The Netherlands: Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
- Norway: Politiets sikkerhetstjeneste (PST)³
- Sweden: Säkerhetspolisen (SÄPO)
- Switzerland: Bundesamt für Polizei (Fedpol)

Most of these security services publish other reports as well, but given the scope of this project, we chose to use the annual reports for three reasons. First, they are similar in nature, which makes them comparable. Second, they provide the most balanced coverage, because they are published once a year by most countries in our sample set. Third, of all types of publications issued by secret services, the annual reports typically address the widest range of threats and activities. This means that examining these sources is the most efficient way to get an impression of the range of threats they monitor and the activities they undertake. Unfortunately, not all countries have released annual reports for all years in the time period we are examining, which explains the gaps in figures 2

2 2008 was the first year about the VSSE published an annual report. Consequently, the Belgian situation will feature only marginally in this report.

3 The publications by the Norwegian PST are somewhat different from the others. Rather than publishing an annual report covering the past year, the PST releases an annual threat assessment, not more than six pages long, describing the threats for the year ahead.

to 4. Table 1 shows the availability of the annual reports per country per year.⁴ The years refer to the years that the reports were about, not to the years in which they were published. For example, the table indicates that the Bfv provided information about 2004. The publication of that report took place in 2005.

	2002	2003	2004	2005	2006	2007	2008
AUSTRIA							
BELGIUM							
CZECH REPUBLIC							
DENMARK							
GERMANY							
THE NETHERLANDS							
NORWAY							
SWEDEN							
SWITZERLAND							

Table 1. AVAILABILITY OF ANNUAL REPORTS

The latest two Danish reports are bi-annual: the report published in 2005 covers the years 2004 and 2005 and the report published in 2007 covers the years 2006 and 2007.

Analysing the openness of the annual reports and the perceptions of security threats presented, our research questions are:

- Which security services provide most information in their annual reports and can be considered the most open?
- What are the similarities and differences between the security services' perceptions of threats to their national security?

4 At the time of writing (2009), not all annual reports for 2008 were released yet. 2008 has therefore been omitted from figures 2, 3 and 4. After they became available, the reports for 2008 have been used for the threat assessments later on.

The first section will address the first research question by looking at the length, level of detail and comprehensiveness of the annual reports. It will conclude by distinguishing the different approaches that the services take when informing the public. The second section will analyse the security threats the services identify. It will outline the main trends and characteristics in extremist movements, espionage and organised crime. The findings will be summed up in the conclusion.

1 Openness of security services

This section of the report will compare the security services on the openness of their annual reports. How much are they willing to share? Which issues are addressed and which are left untouched? How much detail do they provide? The answers to these questions will help us outline different approaches of informing the public about what the services have been doing.

The most obvious variable on which to compare the annual reports would be the length. From figure 2 it is clear that the German reports, on average some 400 pages, are by far the largest, followed by Austria and the Netherlands, with each an average of about 125 pages. The Czech BIS is trailing behind with an average of slightly more than 20 pages. For the period 2002-2007, we had only one threat assessment for Norway (five pages long) without explicit references to people of organisations, so we left it out of the figures 2, 3 and 4.

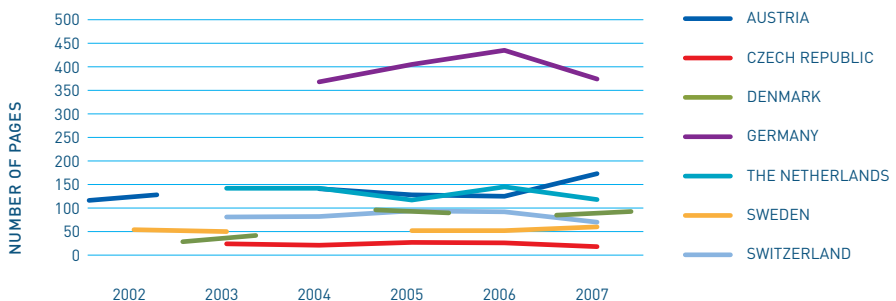


Figure 2. TOTAL LENGTH OF ANNUAL REPORTS

It is true that the length of a report does not necessarily tell us much about its level of openness, as formulations may have been kept deliberately vague or general. In the sections 1.1 and 1.2 we will therefore come up slightly more sophisticated ways of finding out how much substantial information the security services have to offer. As much of the information in the reports is either about security threats or about the activities of the services themselves, we will use these two categories in our analysis below.

Openness about threats

All annual reports have separate sections on left-wing extremism, right-wing extremism, islamist extremism, CBRN proliferation and espionage, using exactly these terms. The only major exceptions are animal rights extremism, only addressed by the Netherlands and Austria, and organised crime, addressed only by Fedpol and the BIS. However, this consensus on the broad contours of the threat universe does not do justice to the variation in the richness of the reports. In order to highlight these differences, we measured the level of detail.

Starting from the assumption that security services that are more willing to divulge the names of the people and organisations that constitute security threats can be considered more open than services that will not do so, we counted in all annual reports the names of people and organisations. Figures 3 and 4 contain the numbers of respectively organisations and individual people that are explicitly named in the reports. The vast majority of the actors that have been counted in this way are organisations and people that are considered threats to national security, i.e. illicit organisations or members of illicit organisation. The references to the very small numbers of people and organisations, e.g. some four or five each year in the German reports, that are not themselves threats to national security, such as money transfer company Western Union, can still be read as willingness to name individuals or organisations that are somehow involved in threats to national security, which is why we included them as well. The results show that the longest annual reports generally contain the most detailed information.

Figure 4 shows that the longer reports (the Netherlands, Switzerland and especially Germany) are also the more detailed ones. The exception is the Austrian BVT, whose reports are generally about as long as the Dutch reports, but which appears to have a policy of not naming more than a handful of concrete people or organisations. The same picture emerges from figure 4,

which, like figure 3, shows that the Netherlands, Switzerland and especially Germany provide information in significantly more detail than Sweden, Austria, Denmark and the Czech Republic.

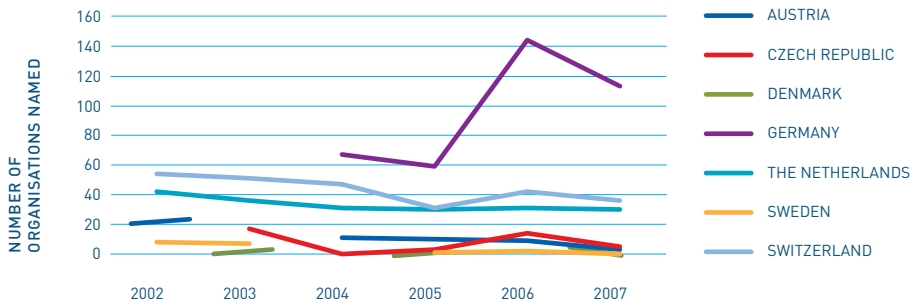


Figure 3. LEVEL OF DETAIL MEASURED BY NUMBERS OF ORGANISATIONS NAMED

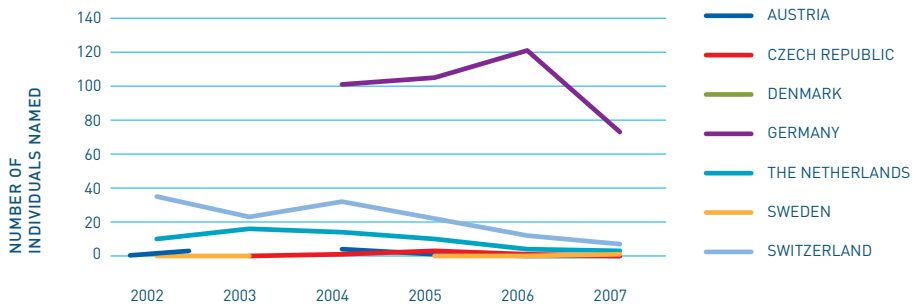


Figure 4. THE LEVEL OF DETAIL MEASURED BY NUMBERS OF EXPLICITLY NAMED INDIVIDUALS

The richest reports, the ones that are the most useful ones for research and analysis, are the German, Dutch and Swiss ones. The German reports are by far the most elaborate ones: it contains extensive background information regarding ideologies and movements and provides tables with numbers of violent incidents and numbers of members of extremist organisations. While still useful, the Dutch and Swiss reports describe trends and developments in subversive movements and other threats to national security in much more general terms, sometimes linking them to the activities of concrete organisations. The Austrian reports describe the general trends and developments, but, as is clear from figures 4 and 5, they are less willing to spell out which people and organisations it concerns.

Openness about activities

Moving away from information about security threats, we also examined how much the sources revealed about the security services themselves. We drew up a list of themes and went over the annual reports to see whether there are sections or paragraphs addressing those themes. The call whether or not a theme was addressed was made on the basis of the table of contents. The list contained the following items:

- *Cooperation (national)*: efforts of the security services together with other governmental bodies of the same country
- *Cooperation (international)*: efforts of the security service together with foreign governmental bodies
- *Internal organisation*: the organisational structure of the security service
- *Legal provisions*: laws and regulations to which the activities of the security service are subjected
- *Outreach*: efforts to present the security service to the public at large
- *International developments*: political trends and events that affect the work of the security service
- *Protective security*: efforts to help guard potential targets against attacks
- *Screenings*: efforts to check the backgrounds of people working in positions where they might compromise national security
- *Oversight*: the role of parliament to see to the legality of the actions of the security service

Table 2 below shows which countries address which themes over the years. A blue cell means that that theme was addressed by all countries in all annual reports. The purple cell indicates that it was addressed in some years, but not in others. A white cell indicates that a theme was not addressed at all.

	AUSTRIA	CZECH REPUBLIC	DENMARK	GERMANY	NETHERLANDS	SWEDEN	SWITZERLAND
COOPERATION (NATIONAL)							
COOPERATION (INTERNATIONAL)							
ORGANISATIONAL STRUCTURE							
LEGAL PROVISIONS							
OUTREACH							
INTERNATIONAL DEVELOPMENTS							
PROTECTIVE SECURITY							
SCREENINGS							
OVERSIGHT							

Table 2. OPENNESS ABOUT ACTIVITIES IN THE ANNUAL REPORTS

It is striking that all security services address the same themes over the years, with the exception of Sweden and Denmark, which display a tendency to address a theme in one year and drop it the next. On this variable, the Dutch AIVD appears to be the most open service, as it addresses all items on the list, except 'international developments'. The German BfV, by far the most open service in the previous section, is significantly less forthcoming when it comes to its own activities. Similarly, the Swiss Fedpol is quite open about what it knows about its enemies, but has next to nothing to say about itself.

Different approaches to informing the public

Since we have two variables on which we compared the annual reports, it is possible to give an overview of the overall results in one figure. Figure 5 shows how the services score on the two variables. The more detail is provided, the more a country will be placed to the left, and the more issues regarding its own activities are discussed, the closer a country will be to the top of the figure.

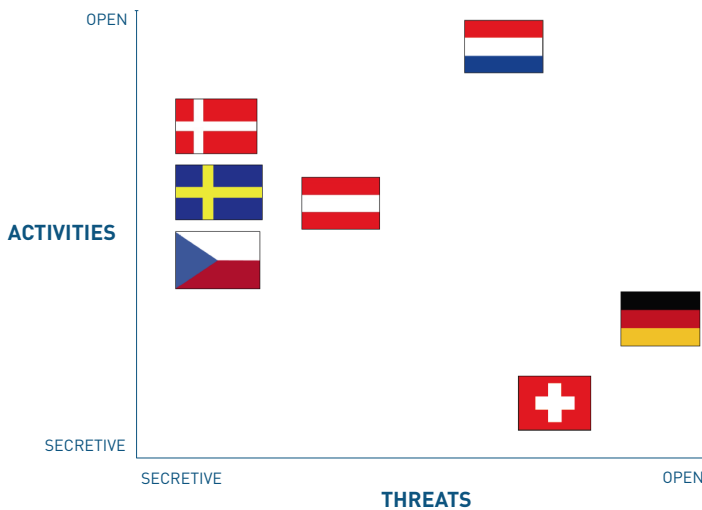


Figure 5. OPENNESS OF SECURITY SERVICES

As is clear from figure 5, the information gaps are generally in different places and the surveyed countries have very different perceptions about what it means to inform the public. There are three ‘information strategies’ that can be discerned from our results. The four countries on the left (Denmark, Sweden, Austria and the Czech Republic) prefer to be more open about their own organisation than about what they know about security threats. Germany and Switzerland take the opposite approach. They are quite detailed and specific about the security threats they are countering, but are less willing to provide information about themselves. The one country that is open across the board is the Netherlands. The AIVD scores quite high on both variables and can thus be

said to take the broadest approach in informing the public. We can only guess about the explanations for these differences. The BIS, PET, SÄPO and BVT may be more risk averse and may want to avoid any risk of losing their sources. Another possibility is that they may be less willing to make themselves vulnerable for criticism. The latter may be the case after a high-impact incident or attack perpetrated by a threat that was reported as being weak and marginalised. The German, Dutch and Swiss services appear to have decidedly less qualms in this regard than their Czech, Danish, Swedish and Austrian counterparts.

2 Security threats

This section will focus more on the contents of the reports. Does the information about security threats differ from service to service or is there consensus about the size and nature of the threats? For a clear understanding of how this section came about, it is important to take note of the irregular nature of the reporting. Typically, only major organisations like al Qaida, the Tamil Tigers, Hizb ut-Tahrir, the GSPC and the PKK and some major local organisations are mentioned in more than three reports of the same country. The reporting appears to be rather erratic, with some organisations or people being mentioned as part of an extremist movement in one year and disregarded in the next. Also, especially in the Czech and Swedish reports, there is a tendency to focus on manifestations of threats that have already drawn a lot of media attention. They contain lengthy descriptions of incidents or arrests that can be assumed to be already widely-known among the public at large.⁵ This unstructured and incident-driven focus of these reports makes it difficult to track the development of a certain organisation and thus stands in the way of a bottom-up analysis of a threat category, i.e. the use of information about its separate components to build a picture of the threat category. For example, by collecting information about all right-wing extremist groups, one could discover patterns and make an assessment of the right-wing extremist movement as a whole. Given the nature of the annual reports, this is not an option. Instead, as all reports discuss roughly the same threat categories in at least general terms, we decided to focus this section of the report on the general characteristics of the threat categories and compare those across years and countries, using the more detailed reports to give examples and illustrations.

5 Compare e.g. SÄPO 2008, 24, 29 and 34 to respectively <http://www.dn.se/ekonomi/saabspion-far-fyra-ars-fanhelse-1.464191>, <http://www.dn.se/nyheter/sverige/svenskens-identitet-bekraftas-av-irakiska-myndigheter-1.673414> and http://www.upi.com/Top_News/2008/03/12/Swedish-police-find-neoNazi-arms-cache/UPI-47361205297897/.

The focus of the analysis in this section on security threats will be on three major themes: extremist movements (movements that are considered a threat to the democratic order, e.g. left-wing extremism), espionage and organised crime.

Extremist movements

For all types of extremism (left-wing, right-wing, islamist and animal rights) we examined the annual reports on the following characteristics to get an idea of the way these movements function.

- *Within movement cohesion*: is the movement well-organised or fractured?
- *International cooperation*: are there many contacts between elements of the movement and their counterparts abroad?
- *Violence*: is the movement physically aggressive?
- *Popular appeal*: does the movement have significant support outside of its own members, i.e. among the general public?
- *Membership*: how many people can be considered part of the movement?
- *Fanaticism*: does the movement display deep ideological commitment?
- *Strength*: how do the security services assess the overall strength of the movement?

These were the questions that guided our examinations of the annual reports and consequently the analyses below.

Left-wing extremism

The extreme-left movement is a category that encompasses many different strands of radical thought. It includes anarchist groups, the so-called autonomous blocks and the more Marxist-Leninist oriented organisations. Left-wing radicalism has a long and rich history of ideological infighting and discord. The current time-frame does not appear to be an exception in this regard. Several countries report on splits in the left-wing extremist movements (BIS 2003, p.11; BIS 2004, p.10; BIS 2005, p.11; SÄPO 2003, p.39; PET 2003, p.39; PET 2004, p.51). Germany and Switzerland are the only countries where there appears to be a significant level of cooperation between left-wing extremist groups ((BfV 2004, pp.132-134; BfV 2007, p.171; Fedpol 2002, p.10 and 26; Fedpol 2006, p.25; Fedpol 2007, p.41).

Left-wing extremism can traditionally count on its fair share of attention from intelligence services. However, the left wing extremist movement appears weak in most of the analysed countries. An interesting deviation is Switzerland. In

almost all years, the Fedpol assessed that the movement was a significant threat, albeit not to national security, but rather on the local level (Fedpol 2002, pp.24-25; Fedpol 2003, p.22; Fedpol 2004, pp.20-21 and 27-38; Fedpol 2005, p.10 and 26; Fedpol 2006, p.27; Fedpol 2007, pp.7, 11, 41 and 67; Fedpol 2008, p.46). The scattered clues provided by the reports for the other countries suggest that, although there appears to be a slight increase in the strength of left-wing extremism in Switzerland and Germany, left-wing extremism is not a significant threat and remained at roughly the same threat level throughout the period 2002-2008 (SÄPO 2007, p.23; BIS 2004, p.10; BIS 2005, p.11; BIS 2006, p.10; BIS 2008, p.8; AIVD 2004, pp.43-44; BVT 2004, p.18 and 52; BVT 2005, p.41; BVT 2006, p.53; PST 2007, p.3).

Since 2002, membership of left-wing extremist movements increased only in Switzerland. Only Fedpol reports growing numbers of members of the left-wing extremist movement (Fedpol 2002, pp.24-25; Fedpol 2003, p.22; Fedpol 2004, p.22). The available annual reports for the other countries do not provide enough data to make claims considering membership, but they do allow for the conclusion that although the movement is seriously trying to appeal to youth, e.g. by the flyering during concerts and organizing manifestations, it remains largely isolated and its popular appeal is generally low (BIS 2003, p.11; BIS 2005, p.11; BIS 2006, pp.10-11; BIS 2007, p.7; PET 2003, p.39). The ability of the extreme-left to gain popular support is limited. Even in Switzerland, where the movement appears more vibrant and active than in other countries, the picture in this regard is bleak, as it is claimed that the extreme-left attracts criminals and people that are simply looking for riots and is unable to generate popular support for its anti-globalist agenda (Fedpol 2002, p.24 and 26; Fedpol 2003, pp.11, 21 and 81; Fedpol 2004, p.22).

Notwithstanding the weakness in many regards, several services report serious levels of international cooperation and communication between left wing extremist groups (BfV 2004, pp.150-156; BfV 2006, pp.167, 177 and 181; Fedpol 2002, p.10 and 26; Fedpol 2007, pp.11 and 40-41; BIS 2005, p.11; BIS 2007, pp.6-7; PET 2003, p.51). This increase in international contacts is largely driven by the increasing intensity of the use of the internet. The internet has become the major interface through which international communication between extremist left wing groups takes place, as it facilitates mobilisation and promotion for events like the so-called Social Fora (BfV 2005, p.190). These manifestations, which are also attended by more moderate left-wing groups, are organised in a different European country every year and have, as a result of the dissemination of the

internet, grown significantly in scope and size over the last ten years. It should be noted that the activities of the extreme-left in the countries under consideration are generally limited to protest demonstrations and manifestations like the Social Forum. The movement uses relatively little violence, although the Bfv and Fedpol report willingness on the part of left-wing extremist groups to use violence (Fedpol 2004, p.11; Fedpol 2005, pp.23-24 and 84; Fedpol 2006, pp.23-26 and 75). The violence that does occur is often directed at members of the right-wing extremist movement. A trend that stands out in almost all countries is the increasing focus of the extreme-left movement on the extreme-right. Left-wing extremist movements throughout Europe increasingly tend to engage in ‘anti-fascist’ activities, meaning disturbing right-wing rallies, which often end in street fights. The violence against right-wing extremists makes up the lion’s share of violence on the part of the left-wing extremist movement (Fedpol 2004, p.11; AIVD 2006, p.21; AIVD 2007, p.49; AIVD 2008, p.43). The findings on left-wing extremism are summed up in table 3.

CHARACTERISTIC	STRENGTH/WEAKNESS	EXPLANATION
WITHIN-MOVEMENT COHESION	Weakness	The movement is characterised by many ideological debates and rivalry between the different strands of the radical left.
INTERNATIONAL COOPERATION	Strength	Left-wing extremist groups regularly get in touch with their foreign counterparts to organise demonstrations and manifestations.
VIOLENCE	Weakness	Left-wing extremist groups mostly rely on non-violent means of protest, except when confronting right-wing extremist groups.
POPULAR APPEAL	Weakness	In spite of attempts to gain support (flyering campaigns and manifestations) the movement remains isolated.
MEMBERSHIP	Weakness	With the exception of Switzerland, left-wing extremist movement has been getting smaller.
FANATICISM	Unknown	The reports provide little information on the ideological commitment of the members of left-wing extremist groups.
OVERALL STRENGTH	Weakness	Left-wing extremism is considered at most a threat to public order, but most services consider it to be quite weak.

Table 3. OVERVIEW STRENGTHS AND WEAKNESSES LEFT-WING EXTREMISM

Right-wing extremism

Generally speaking, the views of most right-wing extremist have two things in common: racism and authoritarianism (BfV 2007, p.46). The right-wing extremist movement is permeated with a sense of embattlement of its cultural identity, be it by the influx of immigrants or by the growing influence of the European Union, and sees strong leadership as a necessary condition to counter these threats. It should immediately be noted that these views are not always articulated well and that membership of a right-wing extremist movement is often as much a matter of identifying with a certain group of individuals as it is of assenting to a set of political views. There are different levels of politicization of right-wing groups. Although they all subscribe to the ideas just outlined, some organisations aim to change the system through participation in mainstream politics, whereas others rather incite riots and use gang-like violence without any clear sense of political direction. Especially the so-called 'skinheads' are prone to use extreme violence against immigrants, the government and people they associate with the political left. Skinheads are generally quite young, as the older right-wing supporters tend to leave these groups to join a more politically oriented group or abandon right-wing extremism altogether (Fedpol 2004, pp.10-11 and 19-20). This distinction is outlined by, for instance, the Austrian BVT and the Belgian VSSE, both of which identify the more politically oriented strand of the extreme-right, where attempts are being made to participate in democratic politics, and the skinhead scene, which is less organized, more aggressive and is not acting according to a clear political agenda ((BVT 2005, pp.30-31; VSSE 2008, p.26). The AIVD even argues that these latter groups should not be considered part of the right-wing extremist movement (AIVD 2008, p.38). Examples of politically more articulate movements that are also attempting to gain access to mainstream politics can be observed in the Czech Republic, Austria, Germany and Switzerland (BfV 2007, pp.49-50; Fedpol 2003, p.11 and 20; Fedpol 2008, p.42; BIS 2008, pp.7-8). The Norwegian PST also mentions some attempts on the part of right-wing extremist groups to gain a foothold in mainstream politics (PST 2008, p.2).

Overall, the right-wing extremist movement does not seem to differ essentially from country to country. The observations below can thus be read as applying to right-wing extremism in Northern and Central Europe, although, unfortunately, the Swedish reports say too little about right-wing extremism to make general statements about the nature of the right-wing extremist movements in these countries.

Going by the information provided in the reports, we can say that the perceptions of the size of the threat of right-wing extremism differs. The reports of the German, Swiss, Austrian, Czech and Danish services all treat right-wing extremism as a significant threat to public order (Fedpol 2003, p.11 and 20; Fedpol 2005, pp.22-23; Fedpol 2006, p.22; BfV 2004, pp.137-138; BfV 2006, p.6; PET 2006, p.51; BIS 2008, pp.7-8). The Netherlands, Norway and Switzerland are the countries where right-wing extremism is reported to be weak or on the decline (AIVD 2004, p.45; AIVD 2005, pp.49-50; AIVD 2006, p.55; AIVD 2007, p.51; AIVD 2008, p.37; Fedpol 2008, p.40). The Swedish report provides too little information to make an assessment. Paradoxically, the rise and decline of right-wing extremist movements can be traced back to the same characteristic of right-wing extremism. Perhaps due to the ideological nature of the right-wing extremist movement, there is a need for strong leadership, which leads to a lot of infighting within the movement (Fedpol 2005, pp.10, 20 and 22-23). The effects can go two ways: either groups fall apart, which appears to have happened in the Netherlands or the members rally around the winner of the power struggle and become more united and ambitious as a result (AIVD 2007, p.49 and 53). Examples of the latter scenario can be observed in Germany, Austria and the Czech Republic (BfV 2005, p.88).

Most right-wing extremist groups in Europe lack a clear organisational structure. Especially the politically less articulate groups may resemble groups of thugs more than a political movement. In this regard, it is interesting to note that, for example in Switzerland, the right-wing extremist movement shows some overlap with the football hooligan scene (Fedpol 2002, p.24 and 85; Fedpol 2003, pp.23-24). They are unorganized, their violence is spontaneous and there is little to no long-term vision or planning. There are groups aspiring access in mainstream politics, but they cannot be seen as the political vanguard of the movement. The contacts in the right-wing extremist movement tend to be ad hoc, and infighting and splits are common. What is striking in this regard is that groups in the surveyed countries manage to maintain international contacts. Especially German, Swiss and Austrian right-wing extremists speak at each other's rallies and organise joint demonstrations and concerts (Fedpol 2003, pp.19-20; Fedpol 2004, p.19; Fedpol 2007, pp.11 and 36-37; BVT 2002, p.17; BVT 2004, p.18; BVT 2006, p.29; BfV 2004, p.155; BfV 2006, pp.88 and 128-133; BfV 2007, p.117; VSSE 2008, p.27).

Like all extremist movements, the right-wing extremist movement has to put a lot of effort in recruitment. The most important ways in which new members

are attracted, i.e. through music and over the internet, are not dissimilar to the recruitment tactics of the left-wing extremist movement. Music, mostly hard rock, heavy metal and punk rock, is probably one of the most important tools to recruit new members for the ideology or organizations. Several security services mention music as a crucial element of the right-wing extremist subculture.

There is a quite vibrant international right-wing extremist music industry, which relies on right-wing extremist networks for distribution. Although music is a potentially fruitful way to spread ideas, the propaganda value does not lie solely on the music by itself. The concerts and festivals where right-wing extremist bands play are ways for many people to get in touch with right-wing extremist ideas and can lead to radicalization and participation in the more organized structures. These gatherings create an atmosphere of camaraderie and offer potential recruits an identity and sense of belonging (BVT 2007, p.30; Fedpol 2006, p.20; Fedpol 2007, p.36; BIS 2004, p.10; BIS 2005, p.11; BfV 2005, pp.61-64; BfV 2006, pp.105-107; BfV 2007, pp.101-102).

Another very important tool for recruitment and a way to get right-wing people in touch with each other is the internet, which is also used for the distribution of music. For example, much of the right-wing extremist music imported to Germany comes from the US, where the restrictions on the distribution of music in this genre are less stringent (BfV 2004, p.55). Other than that, the internet provides the right-wing extremist movement and its sympathizers with a way to speak their minds on internet forums, to set agendas concerning rallies and demonstrations, identify targets for violence and maintain contact with like-minded organizations in other countries (BfV 2006, pp.53-54; PET 2003, p.40; PET 2006, p.59; BVT 2005, p.23; BVT 2007, pp.42-43; BIS 2004, p.10; BIS 2006, p.8; BIS 2007, p.6; Fedpol 2007, p.38). The profile of the right-wing extremist movement as portrayed by the security services thus looks as follows:

CHARACTERISTIC	STRENGTH/ WEAKNESS	EXPLANATION
WITHIN-MOVEMENT COHESION	Inconclusive	Although the movement is plagued by infighting, it is quite good at maintaining the loyalty of its members by cultivating an identity, e.g. through the spread of rightwing extremist music and organising concerts.
INTERNATIONAL COOPERATION	Strength	Like their left-wing counterparts, right-wing extremist groups regularly get in touch with their foreign counterparts to coordinate their actions.
VIOLENCE	Strength	Certain segments of the movement, especially the skinheads, are quite violent. They mostly target foreigners and left-wing extremists.
POPULAR APPEAL	Weakness	With the exception of the Czech republic, there are no reported cases of significant popular support for actions by right-wing extremist groups.
MEMBERSHIP	Strength	Little information is given about group size, but it is clear that, numberwise, right-wing extremism is still amarginal movement.
FANATICISM	Weakness	Large segments of the right-wing extremist movement do not have articulate views and lack political direction. Their loyalty is as much to their group as to its ideas.
OVERALL STRENGTH	Inconclusive	Most services do not consider the movement a serious threat, except to public order. On the other hand, most services also consider the movement to be on the rise.

Table 4. OVERVIEW STRENGTHS AND WEAKNESSES RIGHT-WING EXTREMISM

Islamist extremism

Before embarking on the actual analysis, some clarification regarding terminology may be helpful. Although this section has been framed in terms of extremism, the information provided by the reports, and consequently the analysis in this section, is mostly about islamist terrorism. However, extremism and terrorism are not the same thing. The label ‘extremism’ says something about a movement’s ideology, i.e. that it does not conform to certain norms that are widely accepted in a political discourse. ‘Terrorism’ on the other hand, says something about a movement’s modus operandi, more specifically about the kind of violence it uses. Security services focus mostly on the violent strands

of Islamist extremism, as they are the actors posing the threat to national security. This section will follow the lead of the services and discuss the threat posed by Islamist extremists who are willing – and sometimes planning – to commit terrorist attacks. First, we will give a brief overview of some general trends in Islamic terrorism. These are observations that go for all countries in the set. The next paragraph will outline the major differences in the threat perceptions.

One of the most salient trends in Islamist violent extremism concerns its organizational structure. Whereas the European security services speak of Islamist terrorism as an international organisation centrally guided by Al Qaeda in 2002 and 2003, this view changes quite dramatically in the next years. From 2004 on, the European security services, when referring to Islamist terrorism, speak of so-called 'home-grown terrorism'. This generally means that Islamist terrorist cells emerge locally and focus locally. Although these cells show, or at the very least claim, ideological similarity and affinity with Al Qaeda, they are not directly guided by Osama bin Laden and his inner circle. Directly connected to this trend is the observation made by the security services that the leadership of Al Qaeda becomes more and more spiritual and ideological rather than operational. The strength of Al Qaeda's leading centre, i.e. Osama bin Laden and his direct associates, is, from 2004 on, no longer framed in terms of planned and executed operations, but in terms of the ideological appeal it generates (AIVD 2006, p.31; PET 2006, p.37; Fedpol 2007, p.17).

A last important trend that is put forth in most of the reports, is the extensive use of the internet by Islamists for their communication, the spread of their ideology and the recruitment of new terrorists. In its report over 2006/2007 the PET states that '[t]he internet plays an increasingly important role for terrorists for terrorist groups and networks which utilize this medium to spread virtual training and to provide logistic support and operational planning' (PET 2006, p.45). Referring to the use of internet, the German report of 2007 speaks of 'virtual indoctrination' (BfV 2006, p.202). Especially since mosques are monitored closely by the security services, internet has partly replaced these as the forum for the spread of radical thought and as a ground for recruitment. The importance for the internet also increased because of the organizational disintegration and fragmentation of Islamist terrorism. The local cells which emerged with 'home grown' terrorism cannot make direct use of the logistical support or expertise of other cells and are thus forced to search the internet for the much needed knowledge to plan an attack. Both the PET and the BfV point out that autonomous Islamist terrorist

cells make use of relatively simple explosives for which the building manuals can be found online (PET 2006, pp.36-37; BfV 2006, p.227). This reliance on the internet has also impacted the modus operandi of Islamist terrorism.

Although there are general trends that are reported by all security services, the threat perceptions also differ in some important respects. The most salient difference is the one between those security services that consider their country a potential target for Islamist terrorist attacks and those security services that do not, the former including the German, Dutch and Danish services and the latter the Swedish, Swiss and Czech services. The BIS on the other hand, sees no significant threat to national security in Islamist extremism at all. In the report over 2004 the Czech security service claims that '[i]n the Czech Republic, the security situation did not change in 2004 comparing with the previous year. So far BIS has not ascertained any facts indicating that the Czech Republic or its interests in the world are directly threatened by a terrorist attack.' (BIS 2004, p.4) This could not be much further from the BfV's statement that Islamist terrorism is 'considered the most evident threat to Germany and Europe' (BfV 2006, pp.3-4 and 212).

The three security services that do consider their countries a potential target for Islamist terrorists attacks all have similar reasons to do so. The Netherlands and Denmark have both participated actively in the military missions in Iraq and Afghanistan. Germany did not participate in the war in Iraq but is one of the biggest military contributors to the ISAF mission in Afghanistan. In the 2003 and 2006/2007 annual reports the Danish PET explicitly states that the Danish presence in Iraq may have affected the risk of an Islamist attack in Denmark (PET 2003, p.10; PET 2006, p.36). The German BfV makes a similar claim about the German presence in Afghanistan in the reports over 2004 and 2007 (BfV 2004, p.189; BfV 2007, p.182).

Another significant element these three countries have in common is the large Muslim minorities they harbour. The presence of this minority makes 'home-grown' terrorism a real possibility. This explains the emphasis the BfV, AIVD and PET put on the radicalisation potential of the Muslim minorities, which they appear to monitor closely. Special attention of the AIVD, as well as the BfV, goes out to mosques and Muslim internet sites (AIVD 2004, p.20 and 30; AIVD 2005, p.17; AIVD 2006, p.20 and 27; AIVD 2007, pp.41 and 46-47; BfV 2006, p.3 and 5; BfV 2007, p.203). These two, according to the AIVD and BfV, play a crucial role in

the radicalization process of young Muslims and are used for the recruitment of new jihadists (AIVD 2004, p.20).

A completely different picture emerges from the information provided by the Swiss, Swedish, Norwegian and Czech security services. The Swiss Fedpol does not see Switzerland as a direct target for Islamist attacks, but more as a transit country (Fedpol 2003, pp.10, 12-13 and 39-40; Fedpol 2004, p.7). There are some references to characteristics that enhance Switzerland's profile as a target for terrorist activities, such as its role as a node in international trade and because of the presence of potential high profile foreign targets, such as the international organisations residing on Swiss soil. However, until 2006 there is no mention of active Islamist terrorist cells in Switzerland. According to Fedpol, there are only a few Islamist activists living or residing in Switzerland (Fedpol 2004, p.12 and 25). When in 2006 the Fedpol did identify a Swiss Islamist cell, it claimed that it was not planning an attack against a Swiss, but an Israeli target, the airline El Al (Fedpol 2006, pp.36-37).

The reasoning of the Swedish security service SÄPO regarding Islamist terrorism is quite similar to that of Fedpol. In the report over 2005 the SÄPO states that: '[t]he risk of a large terrorist attack in Sweden is limited, whereas the risk of attacks against certain foreign interests in Sweden has increased' (SÄPO 2005, p.16; SÄPO 2006, p.33). Like Switzerland, Sweden, and also Norway, primarily sees itself as a 'safe haven' for Islamist terrorists, to be used for the dissemination of propaganda, fundraising, logistical support and planning of attacks ((SÄPO 2002, p.37; SÄPO 2008, p.20; PST 2007, p.2; PST 2008, p.1). In the same vein, the reports from the Czech intelligence service indicate that Islamist extremism is not a very strong movement in the Czech Republic. In the report over 2005 the BIS states that it 'monitored the occurrence of activities the nature of which could allow support to or spreading of radical Islamic ideas. But it found no facts testifying to the radicalization of persons present in the Czech Republic.' Similar claims can be found in the reports of 2006 and 2007 (BIS 2005, p.3; BIS 2006, p.2; BIS 2007, p.2). As in Switzerland and Sweden, the only threat reported by the BIS on Czech soil concerns foreign targets on Czech soil. It should be noted that in its report over 2008 the AIVD is shifting towards the position of the SÄPO and Fedpol, arguing that home-grown terrorism has been neutralised and that the Netherlands is now mainly a recruiting ground for jihad abroad rather than a battleground (AIVD 2008, pp.21 and 23-23. See also AIVD 2009).

The answer to the question why Switzerland, Sweden and the Czech Republic do not consider themselves likely targets for Islamist terrorists is not as straightforward as might be expected. All three countries did participate, although modestly, in ISAF, but apparently the SÄPO, BIS and Fedpol do not see this as a factor that increases the risk of an attack against their countries or national interests. Also, Sweden has a sizeable Muslim minority, but there is no suggestion of a threat of home-grown terrorism in the Swedish reports.

CHARACTERISTIC	STRENGTH/WEAKNESS	EXPLANATION
WITHIN-MOVEMENT COHESION	Weakness	Due to the fragmentation of al Qaeda after the fall of the Taliban and the rise of home-grown terrorism, there is little contact between Islamist extremist cells to share expertise, intelligence etc.
INTERNATIONAL COOPERATION	Weakness	Several services report international contacts of some groups, but home-grown groups are generally thought to function autonomously.
VIOLENCE	Strength	Violent Islamist extremist groups have little qualms about engaging in mass casualty terrorism. Their operational goal is to cause as many casualties as possible.
POPULAR APPEAL	Weakness	Many services emphasise that only a very small portion of the Islamic community can be considered extremist.
MEMBERSHIP	Inconclusive	Little information is available about the size.
FANATICISM	Strength	The Quran is the touchstone for members of the movement. The interpretations may differ, but the purity of Islam is an important binding factor.
OVERALL STRENGTH	Strength	The movement is considered dangerous because of the combination of fanaticism and the willingness to engage in mass casualty terrorism.

Table 5. THE STRENGTHS AND WEAKNESSES OF VIOLENT ISLAMIST EXTREMISM

Animal rights extremism

It is striking that the Dutch and Austrian services are the only ones in our sample that report on animal rights extremism, with Austria providing more detailed information than the Netherlands.⁶ Although the information provided by these two countries does not give us much to go on, it is possible to see some similarities in the way animal rights extremists operate. First, the loosely based cell structure, a prominent characteristic of British and American animal rights extremist groups, is applied in the Netherlands and Austria countries as well (Department of Homeland Security 2008, p.8). The Austrian and Dutch services both report a leaderless resistance structure in the animal rights extremist movement (BVT 2002, p.47; BVT 2004, p.55; BVT 2007, p.82). Also, the actions by which animal rights extremists try to achieve their goals are largely similar: they release animals, threaten and harass people working for pharmaceutical companies or mink farms and demolish property of their victims or the organisations they want to stop (BVT 2004, p.56; BVT 2005, p.65; BVT 2007, p.84 and 86; AIVD 2004, p.45; AIVD 2006, p.54; AIVD 2007, p.51). The main difference between animal rights extremism in the Netherlands and Austria, is, going by the reports, that the radical animal rights movement in the Netherlands is steadily becoming more active and violent, whereas the pattern that emerges from the Austrian reports is quite ambivalent. For some years, the movement is reported as becoming more aggressive, whereas in other years, the report notes a decline in the numbers of violent incidents (AIVD 2005, p.48; AIVD 2006, p.53).⁷

There are also some observations about animal rights extremism in Austria that are not addressed in the Dutch reports. Bearing in mind one of the caveats mentioned in the introduction, this does not necessarily mean that these observations do not apply to the Netherlands. All we know is that the Dutch reports do not provide any information for comparison. For example, the Austrian reports frequently mention an increase in the international cooperation. Austrian animal rights extremists use their international contacts for the exchange of expertise and for the coordination of campaigns, for instance against one particular international company. Second, although animal rights are often perceived as a 'leftist' issue, in Austria there seems to be a cleavage

⁶ In its report over 2008, the PST notices a rise in the numbers of incidents perpetrated by PST. See PST 2008, p.3.

⁷ The VSSE also notices a rise in the number of violent incidents by animal rights extremist groups. See VSSE 2008, p.29.

between the left-wing extremist movements and animal rights extremism. There is some overlap as some people are active in both scenes, but there is no structural cooperation, and even some distrust, between organisations from the two scenes (BVT 2004, pp.55-56; BVT 2005, p.49; BVT 2006, p.64; BVT 2007, p.82).

Espionage

Since espionage can serve many kinds of different goals, we drew up a list of questions that covered at least the most important forms of espionage. For all states that were mentioned as security threats, we checked whether they were involved in the following illicit activities:

- *CBRN-proliferation*: is the foreign state trying to acquire knowledge, technology or materials for the construction of weapons of mass destruction?
- *Political / military espionage*: is the foreign state trying to acquire knowledge about the geostrategic plans and ambitions of other states?
- *Economic espionage*: is the foreign state trying to acquire knowledge, technology or materials that will help it improve its economy?
- *Monitoring of oppositional movements*: is the foreign state watching the activities of expatriate groups or communities that it considers a threat to its security?

All annual reports contain sections on the illegal attempts of foreign powers to gain information relevant for their geostrategic position or economic development. Overall, Russia and China can be considered the major espionage threats to Europe, pursuing political, military, economic as well as technological interests. Another common objective is the monitoring of oppositional groups abroad. These groups are considered threats to their homelands by the monitoring services. Iran is an example of a state that monitors these oppositional groups or dissidents abroad (BfV 2007, pp.296-297).

Russia is reported to be engaged in a wide variety of intelligence gathering activities, covering the political, military, economic and technological fields (BVT 2006, p.303; AIVD 2007, p.57). The Russian espionage activities differ from country to country. In Switzerland, Russian intelligence is suspected of being heavily involved in the raw materials trade by Russian enterprises (Fedpol 2007, p.20). This is presented by some services as part of a broader trend on the part of the Russian government to gain more and more influence over its companies abroad in an attempt to effectuate its strategy to acquire international prominence (Fedpol 2006, p.52; BIS 2006, p.6; BIS 2007, p.7). In the Czech

Republic, the main objective appears to be the establishment of sustainable channels of influence within the media and among opinion makers in order to influence the Czech government, mostly on themes regarding the relations of the Czech Republic with the EU and NATO. An example is the alleged Russian campaign in 2004 to turn Czech public opinion against the stationing of the US anti-missile system (BIS 2005, p.8; BIS 2007, p.4). The BIS also reports the threat of Russian economic espionage, its consequences, mostly in terms of loss of competitive advantages, and the use of this instrument for exerting political pressure (BIS 2007, pp.4-5). Unsurprisingly, little is divulged about the Russian methods, other than that foreigners travelling in Russia are sometimes contacted in attempts to gather intelligence and that, like most services, the Russians still largely rely on open source material (BfV 2006, p.304).

The second main espionage threat is posed by China. Its rise to superpower status is matched by an increase in espionage activities, although only few countries mention it specifically: Germany discusses Chinese espionage in all available annual reports; the Netherlands and the Czech Republic only do so in their reports over 2007. The German reports describe the methods used by the Chinese intelligence services in general terms, although with unsurprising results. China uses its embassies, representatives of Chinese media and its embassy personnel and its migrant communities abroad for influence, intelligence gathering and the obtaining of technological know-how (BfV 2005, pp.281-282; BfV 2006, p.316; BfV 2007, pp.301-302; AIVD 2006, p.62; AIVD 2007, p.56; AIVD 2008, p.45). The BfV reports attempts by Chinese intelligence agents to feign friendly ties with politically, economically or militarily valuable German contacts and create a sense of obligation to share valuable information (BfV 2004, p.262; BfV 2005, p.281; BfV 2006, p.316; BfV 2007, p.301). China is also strongly involved in electronic intelligence gathering through the internet. Germany and the Netherlands have reported their suspicions of Chinese involvement in cyber-attacks (BfV 2007, pp.302-303; AIVD 2007, pp.55-56).

Iran, North-Korea, Libya, Syria are reported as actively involved in espionage as well. All these countries spy primarily for economic reasons, that is, they attempt to illicitly acquire technology for their own industries. Particularly active is Iran, which is especially mentioned for its proliferation-related espionage, obviously aimed at obtaining technological know-how regarding weapons of mass destruction (BVT 2006, p.300; BIS 2004, p.8). It also monitors oppositional groups abroad (BfV 2007, pp.296-297). Like most countries, it also uses its embassies as a

base for spies with diplomatic cover (BfV 2006, p.312). Germany and the Czech Republic provide the most extensive information on North Korea. Unsurprisingly, most reported North Korean espionage activity concerns weapons of mass destruction and related materials and know-how (BfV 2004, p.263; BfV 2005, p.283; BfV 2006, p.300 and 318; BfV 2007, pp.303-304; SÄPO 2005, p.18). It also gathers intelligence on NATO and tries to keep an eye on the North Korean community in the Czech Republic (BIS 2006, p.17).⁸ Both the Czech Republic and Germany mention the spread by North Korean intelligence services of North Korean propaganda, aimed at the North Korean community in the Czech Republic as well as at South Korean dissidents in Germany (BfV 2007, p.303). (BfV 2006, p.314; BfV 2007, p.299; AIVD 2006, p.62).

Finally, there are Libya, Algeria and Syria, countries that are mostly worried about oppositional activities abroad. Germany mentions Libyan and Algerian attempts to monitor the activities of oppositional groups, and one of the Dutch reports gives an example of Libyan imams unmasked as spies (BfV 2006, p.314; BfV 2007, p.299; AIVD 2006, p.62).

The most important trends that can be discerned from the annual reports concern the rise of espionage on industrial technology and cyber espionage. Over the years, economic and technological espionage appears to be on the increase (Fedpol 2007, p.50; SÄPO 2003, p.26; BfV 2007, p.302; BfV 2006, p.321). Almost all countries give concrete examples of their industries or R&D sectors becoming a target of foreign intelligence services. Germany reports industrial espionage in its automobile industry, sustainable energy production, chemical industry and communication technology (BfV 2007, pp.290-291 and 307-308). Both Germany and Austria mention the involvement of a German and an Austrian citizen a case of espionage in the aviation industry by Russia (BfV 2007, p.294; BVT 2007, pp.69-70). Sweden discusses a case of industrial espionage at the Swedish telecommunication company Ericsson by a co-worker with access to industrial secrets, who offered classified information on the internet (SÄPO 2003, pp.25-26; SÄPO 2005, p.25). The Dutch AIVD reports espionage in high-tech industry and singles out Russia as a prominent culprit (AIVD 2007, p.55). Switzerland reports several incidents of economic and technological espionage

8 A small number of North Koreans, 144 in 2008, are working in the Czech Republic. See <http://www.thepraguepost.com/articles/2008/03/19/working-overtime.php>, accessed 4 January 2010.

in 2007, including one cyber attack (Fedpol 2007, p.50). Regarding the trends in the means of gathering intelligence, the increased use of the internet stands out. The internet seems, in accordance with its ongoing integration in society, to have become more and more important as an instrument for intelligence services to gather their information. In several European countries, public authorities and private companies have been electronically attacked, for example by attaching harmful software to e-mails sent to these targets in an attempt to gain information to be used for the development of technological tools (PET 2006, p.57; Fedpol 2006, p.11; Fedpol 2007, p.50). The German reports underline the importance of co-perpetrators in this kind of espionage. Insiders, for instance employees who work at or have access to the target area, could install additional computer hard- or software (BfV 2005, p.285). (Fedpol 2003, pp.82-83)

Organised crime

Organised crime is generally not considered part of the tasks of security services. In the reports studied for this project, only the Swiss and the Czech reports dealt with organised crime. In the Swiss case, this may be explained by the mandate of the institution issuing these reports. Fedpol's mandate also includes law enforcement. Notwithstanding the scant attention that security services pay to organised crime, the information provided by Switzerland and the Czech Republic two countries does show that organised crime can be a threat to national security, predominantly by using illegally obtained funds to penetrate and gain influence over companies and governmental bodies. The position of the Czech Republic on the eastern edge of the EU and the central location of non-EU member Switzerland in the heart of Europe are both seen as contributing factors in their respective vulnerability with regard to organised crime (Fedpol 2003, pp.82-83).

Both the Swiss and the Czech reports give names of persons and groups involved in organised crime. Most groups are identified by their geographical descent (Russian speaking, Chinese, ethnic Albanian) rather than by their activity (e.g. human traffickers or drug smugglers). Despite this willingness to give away some details, the Czech and Swiss services do not provide a clear-cut overview of organised crime in their countries, but, going by the information that is provided, it is safe to say that the more sophisticated criminal groups have already worked their way into 'legal' spheres (Fedpol 2002, p.54 and 61; BIS 2003, pp.14-15; BIS 2007, p.9). Criminal groups use their substantial financial assets and the collaboration of lobbies, which establish goal-directed contacts with officials

that have decision making power, to infiltrate the legal economies of both countries through investments in strategic economic sectors, such as transport, telecommunications, oil, aviation and banking (Fedpol 2002, p.60; Fedpol 2003, pp.64-65; Fedpol 2007, p.3; BIS 2003, p.4; BIS 2005, pp.5, 6, 8 and 13). This threat not only comes from within. There is a geostrategic dimension to this problem as well: the Russian intelligence service is working together with organised crime is involved in furthering Russian economic interests (BIS 2003, p.8; BIS 2004, p.8; BIS 2005, pp.8-9; BIS 2006, p.6; BIS 2007, pp.4-5; Fedpol 2005, p.55; Fedpol 2007, p.20). For example, criminal organisations may infiltrate in companies that they feel are profitable, or try to participate in tenders through obscure front companies. Regarding the public sector, the reports observe various forms of corruption and clientelism in relation to government and judicial officials at various levels. There have, for example, been cases where government officials altered official documents to benefit organised crime or other countries (Fedpol 2006, p.52; Fedpol 2007, p.20; BIS 2003, p.15; BIS 2004, pp.6-7 and 9; BIS 2005, p.5; BIS 2006, pp.4-5 and 14; BIS 2007, pp.3 and 9-10). Also, criminal organisations, sometimes with the backing of foreign states, recruit associates and 'friends' among students, future professionals, politicians, financial experts, civil servants and members of security forces (Fedpol 2003, p.48; BIS 2003, p.3 and 8; BIS 2006, p.15; BIS 2007, pp.3 and 9-10).

Overall, it appears that criminal infiltration occurs in both Switzerland and the Czech Republic, but not at the same level. The problem appears graver in the Czech Republic (Fedpol 2002, p.90; Fedpol 2007, p.32). In both countries, organised crime has become so big as to call for coordination among criminal organisations. To avoid clashes, criminal groups engage in high level meetings and strategic planning. For example, Russian groups in the Czech Republic got together to negotiate a division of the Czech Republic in spheres of influence or fields of business, resulting in the emergence of criminal leaders comparable to 'bosses' or 'dons' in more traditional mafia constellations (BIS 2006, p.14; BIS 2007, p.9; Fedpol 2003, p.51). Another way in which Illegal immigration and organised crime contributes to the insecurity of especially the Czech Republic is their involvement in human trafficking, as it is feared that some of the individuals that are illegally entering the country are extremists (BIS 2004, p.4; BIS 2005, p.15; BIS 2006, p.16; BIS 2007, p.10). The Czech Republic already faces the results of criminal infiltration into police and judiciary systems, which endangers the functioning of the state (Fedpol 2003, p.51; BIS 2005, pp.15-16; BIS 2006, pp.14-15; BIS 2007, pp.9-10). Some Caucasian groups are already well

established in governmental and political circles, and Armenians run 'routine legal enterprises' offering security services (BIS 2005, p.14; BIS 2006, p.16; BIS 2007, p.9). Furthermore, the Czech Republic is seriously affected by the collusion of the Russian intelligence services and organised crime from CIS countries (BIS 2006, p.8; BIS 2007, p.6). Problems of this kind occur in Switzerland as well, but not on the same level. Although the threat of infiltration into the legal economy and public institutions is perceived by both Swiss and Czech services, and Russians have already succeeded in infiltrating strategic Swiss companies, the Czech Republic is more deeply penetrated in economic, political and governmental spheres, and most dangerously of all, in the police and judiciary systems. Also, in Switzerland a different range of groups is active, of which the Italian Mafia organisations are the most renowned. Other than that, there are West African criminal organisations which are led by Nigerians and mostly active in drug smuggling and human trafficking, Lebanese groups with Swiss ties, who managed to acquire a central role in drugs trade in Europe, and gang crime and groups with Caucasian origins (Fedpol 2002, p.64; Fedpol 2003, pp.53-54 and 83; Fedpol 2007, p.25).

Conclusion

This report shows that security services display significantly different levels of openness and inform the public in different ways. Where the Dutch AIVD, the Swiss Fedpol and first and foremost the German BfV provide detailed information about a wide range of themes, the BIS, the BVT and the SÄPO are more reluctant to share this knowledge with the outside world. It is striking that the results for openness about the services' own activities are quite different. Here the BfV is on roughly the same level as the SÄPO, the BIS and the BVT. Fedpol is less forthcoming in this regard. Overall, the Dutch reports are the most informative. The AIVD reveals relatively much about both its activities and threats to Dutch national security. In comparison to other secret services, the AIVD can be considered open with respect to both democratic oversight and public information.

Since the majority of the security services rarely provide details about individual extremist groups or organisations or particular countries involved in espionage, this analysis relied on general threat qualifications. Noticeably, the threat categories discussed in the annual reports differed little from country to country. For instance, right-wing extremism in Germany does not appear essentially different from right-wing extremism in Denmark. The overall picture that emerges from the information presented in the annual reports reveals that the threat posed by the left-wing extremist movement in Europe is limited. In almost all surveyed countries, the left-wing extremist movement is weak and isolated and is facing a decline in membership. The right-wing extremist movement in the surveyed countries, albeit growing and more violent than its left-wing extremist counterpart, is scattered and tends to lack political direction. Regarding islamist extremism, the annual reports reveal that the fragmentation, i.e. the lack of direct contacts between the branches and cells that make up the movement, has affected their operational capabilities. Currently, extremist movements in north and central Europe operate in the margins of society and, going by the information provided by the security services, can do little more

than disturb public order. This also seems to apply to animal rights extremism, although this estimation is based on information of only two countries, the Netherlands and Austria.

This is quite different for the threat posed by organised crime to the functioning of the state system. It is interesting to see that the threat posed by organised crime is in many ways the opposite of extremism. Extremist groups have to make their presence known, isolate themselves from the state apparatus and, if there is a political agenda to speak of, try to affect the state from the outside. Organised crime on the other hand, has to operate secretly and quietly to work its way into the state apparatus, the way it is doing in Switzerland and the Czech Republic. Unfortunately, only the Czech Republic and Switzerland provide information regarding organised crime. To assess the severity of the overall problem we would need to have more information. Nevertheless, the threats described go beyond mere violations of the law and move into the national security realm. Also, they seem similar in nature – though not in size – in two quite different countries. The scale and extent of this threat in Europe cannot be established on the basis of the sources used for this research project, but these two observations warrant a deeper examination of what might be a disturbing trend. There are, however, signs that these risks are already being taken seriously. For example, the Dutch National Risk Assessment for 2008/2009 contained a section on infiltration of crime in public policy making (Minister of Internal Affairs and Kingdom Relations 2009) and a Dutch parliamentary working group has drawn up a report on the intertwining of the public sector and organised crime (Minister of Internal Affairs and Kingdom Relations 2009; Parlementaire werkgroep verwevenheid onderwereld/bovenwereld 2008). Similarly, SÄPO reported in its report over 2008 that it has been assigned the task of 'preventing, mapping and countering the unlawful pressure exercised by serious organised crime on key societal functions' (SÄPO 2008, p.39).

What applies to organised crime also applies to espionage: unlike extremisms, its very nature requires secrecy. Like organised crime, espionage also takes place in the public as well as the commercial sector. The breadth of the threat is a reflection of the scope of national security: the annual reports show that everything that is of importance to a country's national security, or, even broader, its well-being, is also interesting for other countries. It can concern political decision making, economic activities as well as technological innovation. Russia and China, emerging from the reports as the two most prominent players in this

than disturb public order. This also seems to apply to animal rights extremism, although this estimation is based on information of only two countries, the Netherlands and Austria.

This is quite different for the threat posed by organised crime to the functioning of the state system. It is interesting to see that the threat posed by organised crime is in many ways the opposite of extremism. Extremist groups have to make their presence known, isolate themselves from the state apparatus and, if there is a political agenda to speak of, try to affect the state from the outside. Organised crime on the other hand, has to operate secretly and quietly to work its way into the state apparatus, the way it is doing in Switzerland and the Czech Republic. Unfortunately, only the Czech Republic and Switzerland provide information regarding organised crime. To assess the severity of the overall problem we would need to have more information. Nevertheless, the threats described go beyond mere violations of the law and move into the national security realm. Also, they seem similar in nature – though not in size – in two quite different countries. The scale and extent of this threat in Europe cannot be established on the basis of the sources used for this research project, but these two observations warrant a deeper examination of what might be a disturbing trend. There are, however, signs that these risks are already being taken seriously. For example, the Dutch National Risk Assessment for 2008/2009 contained a section on infiltration of crime in public policy making (Minister of Internal Affairs and Kingdom Relations 2009) and a Dutch parliamentary working group has drawn up a report on the intertwining of the public sector and organised crime (Minister of Internal Affairs and Kingdom Relations 2009; Parlementaire werkgroep verwevenheid onderwereld/bovenwereld 2008). Similarly, SÄPO reported in its report over 2008 that it has been assigned the task of 'preventing, mapping and countering the unlawful pressure exercised by serious organised crime on key societal functions' (SÄPO 2008, p.39).

What applies to organised crime also applies to espionage: unlike extremisms, its very nature requires secrecy. Like organised crime, espionage also takes place in the public as well as the commercial sector. The breadth of the threat is a reflection of the scope of national security: the annual reports show that everything that is of importance to a country's national security, or, even broader, its well-being, is also interesting for other countries. It can concern political decision making, economic activities as well as technological innovation. Russia and China, emerging from the reports as the two most prominent players in this

field, are active in all of these spheres. Espionage by other countries, however, appears more focused, for instance on information that will help build nuclear arsenals or on the political activities of their nationals abroad. This is probably a matter of resources: countries that have or aspire super power status, are capable of taking a broad approach, whereas the smaller ones have to pick their fights more carefully.

Sources

Annual reports

AIVD. *Annual report 2004*, The Hague: AIVD.
 AIVD. *Annual report 2005*, The Hague: AIVD.
 AIVD. *Annual report 2007*, The Hague: AIVD.
 AIVD. *Annual report 2008*, The Hague: AIVD.
 AIVD. *Annual report 2009*, The Hague: AIVD.

BfV. *Verfassungsschutzbericht 2004*, Berlin: Bundesministerium des Innern.
 BfV. *Verfassungsschutzbericht 2005*, Berlin: Bundesministerium des Innern.
 BfV. *Verfassungsschutzbericht 2006*, Berlin: Bundesministerium des Innern.
 BfV. *Verfassungsschutzbericht 2007*, Berlin: Bundesministerium des Innern.

BIS. *Annual report of the Security Information Service (BIS) for 2003*.
 BIS. *Annual report of the Security Information Service (BIS) for 2004*.
 BIS. *Annual report of the Security Information Service (BIS) for 2005*.
 BIS. *Annual report of the Security Information Service (BIS) for 2006*.
 BIS. *Annual report of the Security Information Service for 2007*.
 BIS. *Annual report of the Security Information Service for 2008*.

BVT. *Verfassungsschutzbericht 2002*, Vienna: Bundesministerium des Inneres.
 BVT. *Verfassungsschutzbericht 2004*, Vienna: Bundesministerium des Inneres.
 BVT. *Verfassungsschutzbericht 2005*, Vienna: Bundesministerium des Inneres.
 BVT. *Verfassungsschutzbericht 2006*, Vienna: Bundesministerium des Inneres.
 BVT. *Verfassungsschutzbericht 2007*, Vienna: Bundesministerium des Inneres.

Fedpol. *Bericht innere Sicherheit der Schweiz 2002*, Bern: Bundesamt für Polizei.
 Fedpol. *Bericht innere Sicherheit der Schweiz 2003*, Bern: Bundesamt für Polizei.
 Fedpol. *Bericht innere Sicherheit der Schweiz 2004*, Bern: Bundesamt für Polizei.
 Fedpol. *Bericht innere Sicherheit der Schweiz 2005*, Bern: Bundesamt für Polizei.
 Fedpol. *Bericht innere Sicherheit der Schweiz 2006*, Bern: Bundesamt für Polizei.

Fedpol. *Bericht innere Sicherheit der Schweiz 2007*, Bern: Bundesamt für Polizei.
 Fedpol. *Bericht innere Sicherheit der Schweiz 2008*, Bern: Bundesamt für Polizei.

PET. *Annual report 2003*, Søborg: PET.
 PET. *Annual report 2004/2005*, Søborg: PET.
 PET. *Annual report 2006/2007*, Søborg: PET.

PST. *Threat assessment 2007*.
 PST. *Threat assessment 2008*.

SÄPO. *Annual report 2002*, Stockholm: Säkerhetspolisen.
 SÄPO. *Annual report 2003*, Stockholm: Säkerhetspolisen.
 SÄPO. *Swedish Security Service 2005*, Stockholm: Säkerhetspolisen.
 SÄPO. *Swedish Security Service 2006*, Stockholm: Säkerhetspolisen.
 SÄPO. *Swedish Security Service 2007*, Stockholm: Säkerhetspolisen.
 SÄPO. *Swedish Security Service 2008*, Stockholm: Säkerhetspolisen.

VSSE. *Jaarverslag 2008*, Brussels: VSSE.

Other sources

AIVD, 2009. *Lokale jihadistische netwerken in Nederland: veranderingen in het dreigingsbeeld*, The Hague: AIVD.


CCSS, 2005. *Democratische controle inlichtingen- en veiligheidsdiensten*, <http://www.hcss.nl/en/publication/36/Democratische-Controle-Inlichtingen--en-Veiligheid.html>. [Accessed February 3, 2010]

Department of Homeland Security, 2008. *Ecoterrorism: environmental and animal rights militants in the United States*. Available at: <http://wikileaks.org/leak/dhs-ecoterrorism-in-us-2008.pdf> [Accessed February 12, 2009].

Minister of Internal Affairs and Kingdom Relations, 2005. *Aanbieding onderzoeksrapport democratische controle inlichtingen- en veiligheidsdiensten*.

Minister of Internal Affairs and Kingdom Relations, 2009. *Scenario's Nationale Risicobeoordeling 2008/2009*, Available at: <http://www.minbzk.nl/onderwerpen/veiligheid/nationale-veiligheid/@123149/scenario's-nationale> [Accessed February 3, 2010].

Parlementaire werkgroep verwevenheid onderwereld/bovenwereld, 2008.
Verwevenheid van de bovenwereld met de onderwereld, Available at: http://www.tweedekamer.nl/images/Eindrapport_verwevenheid_onder_bovenwereld_118-173243.pdf [Accessed March 3, 2010].



The role of security services in democratic societies remains a thorny subject. Many policy measures to combat terrorism, extremism and radicalisation are based on classified information. There is, however, a clear incentive to inform the public about what security services know and what they are doing, as these measures directly affect citizens' lives. Clearly, security services struggle to strike a balance between openness and the obvious need for secrecy.

This report examines the ways in which nine European security services deal with this dilemma in their annual reports. The choices they make are markedly different. The results show that the Dutch AIVD leans more towards openness than the other services.

In addition, this report presents the nature of several prominent security threats in central and northern Europe as perceived by the security services. This assessment shows that security threats are remarkably similar throughout Europe.