veiligheid van de staat
sûreté de l'état
VSSE

LECTURE:

The Belgian civil intelligence service VSSE - general overview and current trends and threats, by Peter LANSSENS, director of the analysis department

Good evening to you all and welcome to this lecture on the Belgian civilian intelligence service and the evolution of the threat assessment in Belgium. If everything went well, you were able to read a text on this same topic that we published in our annual report of 2019 (which was published in June of this year). For those of you that would be interested in reading more on some specific topics that I will address during this lecture, I can refer you to our website where the whole report and other interesting documents are available in Dutch and in French, and a limited amount of texts also in English.

But let me first introduce myself, my name is Peter Lanssens and I am the director of the analysis department at the Belgian State Security Service VSSE. I will develop a little on my specific job further on in the presentation of my service. Unfortunately, due to the circumstances you are all aware of, it was not possible for me to address you in a life session at the University, but I will do my best to present you my service and the challenges we are facing through this on-line session as "lively" as possible. As I have understood, there will be a possibility to raise questions later on through a live chat session.

But let's get started with a few words on the institutional environment that we work in. As I said already, I represent today the Belgian State Security Service. This service is led by Administrator general Jaak Raes since 2014 and in his function, he is sided by his deputy, Pascal Petry. The Committee of directors at VSSE, that meets every two weeks to discuss current investigations on a strategic level, brings these two administrators together with three directors. Two of those are managing the so called "intelligence cycle", that is the analysis department and the operational department. The third department is the general staff department which contains human resources, judicial teams, training staff, ICT, logistics and so on. They make sure that the core of the intelligence work – that is performed by the operational and analytical teams – can be done in a comfortable manner.

Personally, I am the head of the analytical teams. My analysts are really the nerve center of the intelligence service since they orient the investigations. For that, we refer to what we call the intelligence cycle. This means that we establish collection plans (that are then executed by our operational colleagues), we process the information that is gathered by these colleagues, we analyze and evaluate the information and turn it into intelligence.

Once this is done, we assess whether we have enough relevant and reliable intelligence to go to the phase of dissemination. In this phase we put our intelligence at the service of our partners (national or international), judicial entities or political authorities. By doing this we want to answer to our triple mission: prevent – advise – disrupt. But I will come back to this later. If, however we were to assess that our information position is not sufficient, we can go back to the earlier phases of the intelligence cycle and adapt the collection plan. Thus, you have to see this not as something linear but as a kind of a treadmill where we go round and round. Fortunately, we effectively leave this treadmill from time to time to deliver crucial information that can lead to administrative measures or political decisions.

Our operational colleagues are thus the ones who collect the necessary information for us. For doing this, they can use different kinds of methods or specialties, that are commonly known as the -INTS. First of all, we have the good old HUMINT or human intelligence. Even in the 21st century this remains the core of intelligence work. Human intelligence means working with human sources that evolve in circles that we are interested in. Members of my service cannot infiltrate themselves in criminal, extremist or terrorist circles, but they can interrogate their "sources" that are actively involved or at least know of these activities.

OTHER -INTS THAT WE USE ARE:

OSINT or open sources intelligence and SOCMINT or social media intelligence: information that is collected from open sources (what you can find on the internet, but also information from all kinds of official databases) and from what people post on social media. Since people of interest for our service often communicate through social media applications, we do an active follow up of our targets' activities online. Rest assured: we do not collect bulk data of all that happens on social media, we stick to our targets.

TRAVINT: information about people that are travelling. In fact, the phenomenon of foreign terrorist fighters (FTF) that went to fight in Syria and Iraq, has drawn the attention to the travel movements of these fighters and related individuals. Several operatives of terrorist plots (both successful and failed/thwarted attempts) traveled intensively during weeks or months, including travel movements between the jihadist zones in the Middle East and Europe.

veiligheid van de staat
sûreté de l'état
VSSE

From 2018 on, all over Europe PIU's or Passenger Information Units were established that receive information from travel agencies, airliner companies, international coach services and so on. Belgium was one of the first European countries to actively advocate Passenger Name Records or – in short – PNR-systems on a European scale. This information allows us to follow up on the travelling of our targets (and, again, only that of our targets).

veiligheid van de staat
sûreté de l'état
VSSE

COLLECTION METHODS

MIGRINT: Terrorists also exploited the migration crisis of 2015 and the following years, to exfiltrate terrorist operatives. Although only a very small percentage of migrants might nurture terrorist plans, given the numbers of newcomers that arrive every year in Europe, even a "terrorist percentage" of 0,01% or lower may constitute a threat. Therefore, we developed what we call "MIGRINT", intelligence related to migration issues, focused on detecting in the large flow of migrants the few cases that may be problematic. For this, the VSSE has a permanent liaison officer with the Migration Office.

SIGINT or signals intelligence: information that is collected from data traffic. VSSE does not have an active SIGINT-capacity, but some of its partners do.

IMINT or imagery intelligence and GEOINT or geospatial intelligence: information from images that were made by satellites or aerial photography. Here also: VSSE does not have an active IMINT- or GEOINT-capacity, but some of its partners do. So, we can obtain useful information from our partner services as well.

Next to these specialized collection techniques, we can use special intelligence methods, but we can only do so when we can in no other way retrieve the information we are in need for. These special methods include shadowing, retrieving one's telephonic contacts, telephone tapping, opening of mail or the use of cameras. These methods exist in three categories, depending on the degree of intrusion into a person's private life. These most intrusive methods can only be performed when the preliminary agreement is given by an independent body of magistrates. After all, the methods we use must be proportionate to the case we work on (you don't burn down your house to smoke out a rat). Therefore, we have to explain to this commission of magistrates what we suspect our targets of, why we need to use this or that specific method and why it is impossible to obtain the results we want through any other less intrusive method. Next to that, these magistrates are not limited to giving their consent beforehand, but they also look whether the method was rightfully used. This must guarantee that our service does not use methods that are too intrusive into one's personal life when there are other possibilities to retrieve the necessary information.

So, these are the most important collection methods that we use to gather information that we have to transform into intelligence. We gather information on a selected number of threats that we are legally obliged to counter: espionage, interference activities, terrorism, extremism, non-proliferation of nuclear, biological, chemical or radiological weapons, harmful sectarian organizations and criminal organizations. We have to defend the Belgian internal and external security as well as the Belgian scientific and economic potential against these threats. This is what our law obliges us to do. Since 2015 however, our service is no longer actively working on criminal or sectarian organizations, for the simple reason that we have limited means and personnel. Exceptions are made for those organizations that have clear links with the other mentioned threats.

You will see these threats reflected in the way our service is organized, with three big pillars in the analytical as well as in the operational department: CI or counter-intelligence

(countering espionage and interference activities) - CE or counter-extremism (countering both ideological and religious extremism) - and CT or counter-terrorism. I will touch upon those later on in this lecture when I will talk about the current threats we are facing.

As I said already, we gather information, that we turn into intelligence to counter the threats mentioned in our law. Our aim is to prevent, to advise and to disrupt. We help to prevent our country from malicious attacks, whether it be a terrorist attack, a cyber-attack or still something else. We do this by sharing our intelligence with police services, the judicial system or other partners that can act to foil the planned attack. We advise Belgian political and administrative authorities about the threats they are facing and where possible give them the tools to counter this. We give awareness briefings about the danger of espionage in the European capital, we advise our police partners whenever a new phenomenon arises. All of this is done with the aim of enhancing their resilience and limiting the vulnerabilities. Finally, when possible, we disrupt any activity that might harm our country and its citizens. Disruption can come in many forms: we can inform a mayor on a neo-Nazi concert that is organized in his city so that he can take administrative measures against it; we can "burn" the network of a spy by talking to his contacts and by doing this, uncover his clandestine activities; we can inform the family of a youngster that plans to leave to go fighting in a jihadi conflict so that they can prevent him from travelling; and so on. All this with the one and only aim: to make an end to a possible harmful event.

I would like to end this general introduction by briefly touching upon the institutional environment we work in. The State Security Service falls under the authority of the Belgian Minister of Justice, although it has also a good working relationship with the Minister of Home Affairs and the Prime Minister's Office.

In fact, it is the Prime Minister who presides the National Security Council where strategic decisions are made about the national policies with regard to security. The administrator general of VSSE takes part in the monthly meetings of this National Security Council. This is the political side of the story where part of the tasking of our service takes place.

Furthermore, our service is closely monitored by an oversight committee that can inquire about how we collect information, how we process it and how we disseminate. This Standing Committee is active since 1991 and reports regularly to a parliamentary commission composed of all parties present in the national assembly. When I was talking about the special intelligence methods, I already touched upon the "a priori" control by a special commission of three magistrates. The Standing Committee is also doing an "a posteriori"

control of the methods used by my service. This means that there is a double check of our collection where both bodies look whether our use of methods is respecting the law on the level of "proportionality" and "subsidiarity". This means: can the information we are looking for not be obtained through a less intrusive way and is the level of intrusion in balance with the threat level? Finally, the Standing Committee is also asked to deliver recommendations to make my service perform ever better on a regular basis.

To end this part of my presentation, I would like to stress than an intelligence service is not a police service. We have no power to arrest or confine people nor are we looking for evidence of a crime that can be used in a courtroom. Our role is limited to the collection of information, turning it into intelligence and to share this with our partners. The vocation of our service is to be proactive; whereas the justice system is working reactively, as is the judicial police that has to provide the evidence to be used in court. But this is after the "act"; the work of an intelligence service is precisely to prevent this "act".

Who are now the partners I am always talking about? With the risk of always leaving an important partner out, our most crucial partnerships are with the federal and local police services, our military counterparts of SGRS, the national threat assessment center CUTA, the immigration office, the foreign affairs department, the national crisis center, the federal prosecutor's office, the prison system and different kinds of partners at a national, regional or local level. But of course, we also work closely together with our international partners. VSSE has working relations with no less than 115 partner services in 80 different countries, both on a bilateral and a multilateral level.

But this for a general introduction on my service and the role we play in the Belgian security landscape. What I would like to do now is to talk a little bit more on the challenges we face in 2020 and that we expect to be continually confronted with in the coming years – as was the general idea behind this briefing session.

For this I would like to return to what I said earlier on: our operational and analytical activities are organized around three pillars: we have a CT (counterterrorism) division, we have a CE (counterextremism) division that looks at both confessional and ideological extremism; and we have a CI (counterespionage) division where we look at foreign espionage, interference and proliferation activities.

Let's get started with CT, the division that has been in the center of everybody's attention in the last couple of years - until, of course, we were confronted with another enemy com-

ing from the east. All of you will remember the horrible attacks in Brussels and Zaventem in 2016, but my story begins more than 20 years before that. For my service (and a lot of our international partners), the rise of political Islam in the nineties and the shock of 9/11 were a wake-up call. Suddenly, intelligence services - that were thought to be useless after the Cold War had ended - were rediscovered, while they were still busy trying to adapt themselves to the challenges of the new era. This includes also: fresh recruitments. How bizarre it might seem nowadays, during the end of the eighties and the nineties, our service had not been allowed to recruit new staff for almost fifteen years, and budget cuts had become an annual recurring phenomenon. In other words, we were not in a good position to tackle the new challenges that we were about to face.

As early as 1995, Belgium was confronted with the GIA (in full: Groupe Islamique Armé), the first terrorism group that "exported" a predominantly local conflict to Europe, long before we were confronted with Al Qaeda or Daesh. Already at that time we noticed that terrorists were early adapters of the slogan "think locally, act globally". The Algerian networks of that time were clever enough to understand that the best way to draw the attention of the world (or, anyway, Europe) to its cause, was to export an at first sight purely internal, local conflict to other countries. So, the threat emanating from Daesh from 2012 on could not be regarded as something completely new.

In a certain way, the Algerian cases of the nineties were the first stages in a long evolution that, with the rise of IS and the security problems related to foreign terrorist fighters and returnees, has reached its temporarily final stage. But there is one very important difference: the members of the Algerian networks in Europe consisted mostly of Algerians who had recently arrived in Europe, and who were recruited for an essentially national agenda. This would change in the period after 9/11, when Al Qaeda and the groups it inspired paved the way for a truly international jihadist movement, with a global agenda. In other words, the ideological shift from a national, religious framework - the fight against an "un-Islamic" or "apostate" invader or regime in a specific country - towards a global framework – the establishment of an all-encompassing Caliphate, implicated that from now on all existing political regimes, with no or very few exceptions, were considered to be "un-Islamic" or "apostate", and thus to be eliminated.

From a more practical viewpoint - which is the kind of viewpoint security and intelligence services prefer - this meant that from now on every target (no matter what, no matter where) could be considered potentially legitimate for the new generation of jihadis, and, even more important, that recruitment of new potential terrorists was no longer restricted

to a nationality or ethnicity. Youngsters that were born and raised in Europe, but who felt excluded from mainstream Western society and alienated from the traditional Arab societies of their parents and grandparents, discovered a radical interpretation of Islam as cornerstone for constructing a new identity.

This was an important gamechanger for intelligence services, as it became increasingly clear that terrorist facilitators were quick to exploit this kind of problematic identity issues. The new war theatres of the global jihad exercised a growing influence and attraction upon mostly young, radicalized males. This led to a limited number of departures to jihadist zones such as Afghanistan, Iraq and Somalia, with support of Belgian recruitment and facilitation networks.

At that time, some ten years ago, foreign terrorist travel was certainly considered as one of the main topics of our CT section, but it remained all together limited to a few, clearly identifiable cases. Of course, this all has changed with the rise of Islamic State in Syria and Iraq, which led to foreign terrorist travel on an unprecedented scale. Between 2012 and 2017, in between 400 and 500 Belgian residents have traveled with terrorist purposes to Syria and Iraq. Compared to the size of the Belgian population, our country is one of the European countries with the highest number of FTF (this is short for foreign terrorist fighters). If you add to this the number of failed or thwarted departure attempts and the individuals who, at a certain moment, expressed their intention to travel to Syria as a foreign terrorist fighter, the total number of Belgian FTF and would-be FTF amounts to more than 600.

Nowadays, the general public thinks that the threat is gone since the Caliphate has ceased to exist in Syria and Iraq. But even in this area, local groups are still fighting with the regular armies and complicated, directed attacks were replaced by isolated, inspired and enabled attacks, using an easier modus operandi. Now that IS can no longer be seen as the centrally organized group it once was, the question remains what will happen next – including with the limited number of European foreign terrorist fighters that are still residing in the zone.

What threat picture results from this evolution, especially in Belgium? Regarding the terrorist threat in or against Belgium, I have selected five major CT challenges for our service.

First of all, there are the lone actor attacks. Our country has suffered at least four of this kind of attacks after the Brussels attacks in March 2016. Amongst them, the failed attack

with an explosive device against the Central Station in Brussels in June 2017. Without making too far reaching conclusions from this limited number of cases, some more general conclusions can be drawn.

First of all, I have to admit that, with only one exception, the perpetrators of these attacks were almost completely unknown to police and intelligence services. Second, in three of the four cases, we see a similar modus operandi: a perpetrator acting alone, using simple but potentially lethal weapons. Third, in the choice of the targets, there's a certain preference for visible, uniformed symbols of state power and state authority: policemen or military. Finally, and luckily, the perpetrators could immediately be neutralized by law enforcement, which also limited the damage done by the perpetrators.

Lone actor attacks are for all intelligence services a real challenge precisely because their perpetrators are individuals generally not known before for extremist behaviour or mindset. Therefore, their actions are very difficult to predict. On the other hand, although lone actors may be in general very isolated individuals in real life, many of them are active on the internet or via social networks. These virtual contacts may give away some clues on what's happening in the mind of a potential lone actor.

The second big challenge is, of course, the phenomenon of the foreign terrorist fighters. The more than 400 Belgian foreign terrorist fighters I mentioned earlier on are part of a large group of between 30.000 and 40.000 FTF of whom around 5.000 are European residents. According to our data, there is still a "dark number" of FTF in the region that we do not know the whereabouts of. Are they dead? Are they in custody? Are they still active in the region or in another jihadi area? Their number is rather limited, but we cannot become negligent as we have seen what they are capable of. These FTF are hardened in the battles they fought and might have some skills in different kinds of warfare, in the use of firearms or other weapons or have the capacity to make an improvised explosive device for instance.

Thirdly, the returnees that are now in a Belgian prison. In Belgium, a significant part of the returned FTF are in jail, as are other individuals that are condemned for terrorism or terrorism related activities; at the same time, 450 detainees present signs of radicalisation. This raises some important questions. First of all, how to insert these individuals in the already overcrowded prison system, how to limit the risks they will build new radical networks inside the prison community or revive old networks (including cross-overs with criminal networks and gangs in prison)? Second, how to arrange a follow-up of these individuals

once they have left prison – as will be the case for the majority of them within five or ten years? The VSSE has stepped up its intelligence gathering activities inside the prison system, in order to detect as early as possible signs of radicalisation among the prison population and to keep an eye upon the activities of detainees that have been condemned for terrorism. For VSSE, intelligence activities do not stop when enough actionable intelligence is collected, analysed and communicated to build up a judicial case against a potential terrorist; it continues when the individual has been condemned, imprisoned and even after his release.

And there we are, perhaps the biggest challenge of them all: most of the convicted FTF got sentences of more or less 5 years imprisonment. That means that a large number of them is starting to get liberated since last year. Together with local police departments and local social services we have to be able to do a follow up of these individuals. A lot of them returned disillusioned and will be able to reintegrate society, but a hard core of them will leave prison as radicalized as they entered it and will continue posing security questions.

Our fourth big CT challenge will be the so-called new jihadi theaters. We have seen the difficulties we encountered following up on the Belgian FTF that went to fight in Syria or Iraq. Our service is not active on foreign soil, so we were limited to looking at their social media, their contacts in Belgium and in part also on information coming from foreign partner services that were active in the region. This will only become more difficult when the jihadi theaters our FTF are active in become more far-flung and diverse. Until this day, Afghanistan and Pakistan continue to be a source of unrest; day after day attacks are committed by an amalgam of tribes and terrorist organizations. Even though the attraction for Belgian based FTF was always fairly limited, continued vigilance was needed. Further to the southeast, there were rumours about new "safe havens" for jihadis who fled other areas of conflict. Due to the relative calm in this region, it could serve as a place to regroup and continue to become skilled at guerrilla tactics. But above all, it is mainly the increased "jihadization" of conflicts in the Sahel region that worries us. This region in particular will have to be focused on in the next couple of years. A combination of relative proximity and migration flows (remember what I said earlier on about the importance of "migrint") from the south to the north can cause certain threats.

The last big challenge that I would like to talk about is perhaps the most difficult, AND the one challenge that not only touches CT but all the areas my service is active in. This is the technological challenge. The technological revolution in general, and more specifically the evolution in ICT and (social) media technology, has and will have an enormous impact on

the work of CT teams. This evolution confronts us with two major challenges. The first one is the problem of encryption. CT targets are very quick to exploit new social media platforms, and are even more quick to abandon one platform for another one that is more secure. This explains the fast-growing popularity of secure communication channels like Telegram, Whatsapp, Viber… and the difficulties intelligence services encounter to access these communications about attack planning and so on. The second problem concerns the abundance of information that can be gathered through - for instance - Sigint and Socmint. The large amount of data and metadata they produce, and the treatment of this kind of mass data requires special skills and adapted hardware. Next to that we have a legal obligation to respect the privacy of all citizens, by filtering out the information that we need to follow up on our targets without accessing all - for us - irrelevant data. This might thus well be the biggest challenge of them all.

This brings us to our second pillar, CE or counter extremism. As I already said, our service has a legal obligation to follow up on both confessional (more commonly said: religious) extremism and ideological extremism (this means extreme left-wing and extreme right-wing movements).

In the text that you were all able to read before this lecture, I explained that our regular work on both the external (IS in Syria and Iraq) and internal (homegrown) terrorist threat points to the same form of religious extremism as a breeding ground. The simple fact of having extremist thoughts is of course not enough to incite someone to commit a terrorist attack. There are numerous factors that interact there. But the underlying breeding ground for this type of terrorism can often be found in the most rigorous form of extremist Islam, namely Salafism. In recent years, we have for instance witnessed a strong growth in the Madkhalist branch of Salafism in Belgium; this is a branch that is characterized by intense proselytism and a strong aversion to the democratic constitutional state. As an intelligence service, not only do we perceive this religious extremism as a threat because it constitutes a breeding ground for terrorist action, we also consider it problematic because of its totalitarian, racist and anti-democratic nature. This makes it a significant threat to our inclusive society.

The most visible part of our activities in this domain is when it is mentioned in the press that "the Belgian State Security Service has refused the recognition of a particular mosque or opposes the establishment of a specific school". Let me be clear about this: it is not up to VSSE to decide on either of these. This decision lies with the communities (federated entities in Belgium). However, our service is - along with several other services - asked to

give her advice for what concerns the recognition of a mosque, which means that they receive some means from the government and that they agree to follow some rules and accept a certain oversight. To be able to give our advice, we look into different kinds of aspects with regard to the mosque in question: do we have information that extremist lectures or preaches are given in this mosque? Is it offering a place for any kind of education with extremist views? Is the official imam known to utter extremist ideas during the services? Is there any direct foreign financing in the mosque, which could mean that it cannot work fully independently and might be obliged to do some things that are not compatible with the exigences of a place of worship in Belgium? Or even: do we hold information that the mosque or anybody that has a role to play in it, is involved in criminal activities? Based on our answers to these questions, we formulate an advice for the Minister of Justice that will be joined with the advice of the other services and transmitted to the communities so that they can make their decision.

Next to that, our CE sections are working on different topics that are of a great importance for Belgian society. For those who have read our annual report from last year for instance (my apologies for the fact that it is only accessible in Dutch and in French), we there reported about the phenomenon of homeschooling and the fact that 20% of children that receive home schooling (and thus do not go to an official school), have parents that are linked to extremist groups. This information launched a (short-lived for sure) shock wave in political cycles. But there is a real problem with children that don't have the possibility to meet with other-minded youth and are thus secluded in a small, extremist community. We cannot stay blind for this.

This is just an example to show you that a main role for an intelligence service is to bring a phenomenon to the attention of policy makers that is fairly new and thus one that they are often not (yet) aware of.

Let's move over to ideological extremism. Our service has a long history in working on threats coming from both the extreme left and the extreme right side. I have not the intention to start a history lesson right now but from the 1970's onwards Belgium has been confronted with violent activities both coming from the left (remember the attacks by the Cellules Communistes Combattantes) and from the right (Front de la Jeunesse and Westland New Post for instance). In many of the stories around these last groups, a preponderant role is played by former employees of our service. This is not something to be proud of, but we can firmly state that this is now just a dark page in the history of our service. At this moment we look into the threat that is emanating from both sides according to our

principles of prevent, advise and disrupt.

Less visible perhaps than their antipodes of the extreme right wing, activists from the extreme left wing are quite active on a European level. The largest group of these extreme left-wing activists are the anarchists. Mostly they are seen as a rather loose collection of individuals, but they keep in touch with likeminded people all over Europe. They oppose everything that can be linked with "big" government or with the - in their eyes - "repressive authorities": army, police, prisons, weapon industry, telecommunications and energy infra-structure, big building projects and so on, all of these are "legal targets" for these leftist extremists.

Recent activities can be seen when they targeted the building of a new prison complex in the north of Brussels for instance. An even more dangerous aspect is when these groups of anarchists infiltrate legitimate protest movements, like the groups that are active in the sphere of climate change. By doing this they compromise these genuine opposition movements, that - let me be clear - are no targets for an intelligence service because they do not pose a threat. Therefore, it is our job to follow up on these extremist groups and individuals, to try to avoid them hijacking legitimate protest movements and to help to safeguard the liberty of expression that is one of the pillars of our society.

This is a crucial balance for us, that will sometimes be misinterpreted - accidentally but also consciously, to discredit our service.

Within the scope of the extreme left-wing activism, I want to direct your attention to one last particular phenomenon. One lesser known subgroup is what we call the "libertarian activists" who share with other leftist extremists their opposition against the state, which for them is equal to capitalism and fascism. Some of these libertarian activists were attracted to the already mentioned conflict in Syria and Iraq, so they enrolled with the Rojava, the Kurdish acronym for the International Freedom Battalion, to fight Daesh and other, often Al Qaeda affiliated, terrorist groups in northern Syria. Some may see this as a legitimate battle, but fact is that these volunteers have now returned to Europa with specific capacities in guerrilla warfare and weapons handling, which they can now use in another constellation.

The chapter of our latest annual report that got the foremost media coverage was the one on extreme right-wing terrorism. It is true, in 2019, it became clear in our neighbouring countries, but also in the United States or New Zeeland for instance, that the threat that

stems from extreme right-wing extremism and terrorism should not be ignored. The attack on a mosque in Christchurch in march 2019 was the first of a kind of "vague" of extreme right-wing violence in the western world. The perpetrators of this kind of violent actions are often proclaimed heroes by other extremists and so we risk that their "example" will lead to new attacks in the near future. The threshold between hate speech and the commitment to violence has never been this low. Here also we encounter the problem of the lone actors. Formal organizations will often hide their real intentions and cover up their links with violent actions; but their hate speech can inspire a lone actor to commit a violent act. And as I explained in the part of the challenges we encounter in our CT work; these lone actors are sometimes difficult to uncover.

Next to that we have the what we call "white collar extremists". Whereas most of the people will think of skinheads or guys with neo-Nazi tattoos when we talk about extreme right-wing extremism, this does not really correspond with the facts. One of the greater risks is the more civilized kind of right-wing propagandists that utter the most offensive language and incite others to become violent. One more recent phenomenon we look into are the identitary movements that are emerging all over the world. These groups are creating an "us against them" feeling that is not that innocent. Their hate speech can reach the more influenceable individual and convince him or her to commit a violent action. At the same time, they distance themselves from the action itself whilst they were actively involved in the incitement to action. This, combined with an eagerness to obtain weapons and to train themselves in the use of these firearms, creates a cooking pot that can explode at any time.

In our annual report we mentioned two themes that are abundantly discussed between right-wing extremists. The first is the idea of the "great replacement", that was also one of the key elements that appeared in the manifesto of the Christchurch mosque attacker. This idea refers to a mysterious conspiracy theory that the liberal elites all over the world are complotting against "the people" and that they want to replace the indigenous populations by coloured, mostly Muslim migrants. This idea is unfortunately widespread on hate speech channels like 4Chan, 8Chan and others. It goes without saying that these unfunded but widespread ideas play a polarizing role in society. The idea of the "great replacement" often goes along with the idea of "accelerationism". The civil war, or religious war or even the race war is imminent, so action must be taken immediately. Within a couple of years, the "great replacement" might have evolved thus far, that it will have become irreversible. The spreading of these ideas poses serious problems for security services all over the world. Polarization is growing, sometimes even encouraged by those in power.

This will certainly become one of the most important points of attention for our service in the years to come.

I feel it is time to touch upon our final big theme for tonight, which is counterespionage. In this section we do not only follow up on foreign spies, but we also try to counter foreign interference activities and the proliferation of chemical, biological, radiological or nuclear weapons. Since long, espionage has been the core business of every intelligence agency. Whereas in countering terrorism and extremism we closely collaborate with police services and judicial partners; counterespionage is the unique competence of intelligence services. Since it is difficult to pursue somebody for espionage or interference activities, our adagio of prevent, advise and disrupt is really the core of our activities in this matter.

My service has to protect the internal security of the state, the external security of the state and its international relations and finally the scientific and economic potential of Belgium. But in addition to that we have to monitor the activities of all foreign intelligence services on our soil. This is definitely not a task to take lightly.

Our aim to prevent illicit activities by foreign powers in Belgium will first of all be reached through strengthening the resilience of their targets, to create awareness of the dangers of hostile espionage and interference and to provide them with the guidelines to protect their own and the nation's security. Who are these targets I am talking about? That can be politicians on all kinds of levels, police officers, intelligence agents, scientists, but in fact everybody who can be in possession of a certain knowledge that is interesting for a foreign service. Most of these services have long-term aims and can be very patient. So, they are regularly establishing contact with people who are not (or not yet) in a position to possess useful intelligence, but whom they think might later on evolve into this kind of position.

In fact, a brilliant student with ambitions to become a leading figure in politics, administration or science might already be on the radar of foreign intelligence services. So don't say I didn't warn you!

But how do we create this awareness, how do we build this kind of resilience? First of all, we offer awareness briefings to all kind of people or enterprises, for instance a diplomat who will be joining a new posting abroad, a new cabinet member of a minister who will be in contact with foreign counterparts, employees of Belgian companies that are working together with firms from certain countries and so on. In these briefings we will explain the

modus operandi of foreign intelligence agents so that they notice any signs of what we call "elicitation" and know how to deal with this. 2019 for instance was an election year and we were aware that there was a possibility that foreign powers might try to interfere in this process. Therefore, we briefed them (that is: Belgian political parties) on this possibility, we offered them some tools to protect themselves from this and we published a brochure on "online safety during the election campaign" (which you can find - in Dutch and in French - on our website).

A rather new phenomenon in this area is that of "fake news" and "disinformation". Some foreign intelligence services are actively involved with inciting fake news and disinformation to circulate on all kinds of topics. The most recent example of this is the constant flow of disinformation around Covid-19. A lot of this disinformation would of course circulate without the manipulation by an offensive intelligence service, but there are foreign powers that hope to use this to sow polarization in our society, so they can choose to accelerate the spreading of it or target specific audiences with it. In a short brief we publicized in April of this year, we warned that social media are flooded with disinformation about Covid-19 in order to set population groups against each other. In order to manage this risk as effectively as possible, we have joined forces with our military colleagues and created a permanent dialogue based on our experiences during the last federal elections.

You might think that we are exaggerating and that this kind of disinformation or fake news only circulates in small circles with little or no impact in general, but if you think this, you are wrong. Some examples: in extremist right-wing circles a post is circulating that a Muslim cleric issued a fatwa calling infected Muslims to cough in the faces of nonbelievers. This message proved to be untrue, but again a seed was planted to put two communities up against each other. Russian trolling farms on the other hand helped spreading messages that link migration with the outbreak of the coronavirus, again with the idea of creating opposing sites in our country around the issue of migration. You will see, once western governments will start vaccination campaigns against Covid-19, Russian and other hostile intelligence services will prove to be a loyal partner of the anti-vaccine lobby. Not because they have a problem with vaccination, but only with the aim of enhancing polarization in society.

Another consequence of the current Covid 19-pandemic and more importantly the economic followings from it, is that foreign countries, like China for instance, are seeking strategic takeovers of companies that are struggling. Opportunities may arise predominantly in the high-tech industry allowing a nation to strengthen its strategic position and to estab-

lish itself in the European market. Our service has already drawn the attention to the risk of foreign powers exploiting their humanitarian aid operations to engage in interference in the decision-making process. This "corona diplomacy" is evidently not always in the interest of our country. With this I think I have covered our aim to advise our government and our national partners for the dangers in the field of espionage, interference and proliferation.

Besides prevention and advising, the third "pillar" of our work is disruption. There have already been a lot of discussions around this terminology and some people - even academics - get the wildest ideas about this. So here I am to counter the thought that we have a license to kill foreign spies or that we want to create a kind of Guantanamo bay where we can question our targets through "enhanced interrogation techniques". None of the kind, we are all civilized people at VSSE.

The idea to disrupt hostile activities has come from the simple fact that our service has the vocation to be a proactive one. In other words: we want to intervene before an attack or another malicious activity takes place. This is what we did when we prevented a bomb attack against a meeting of Iranian opponents in Paris in 2017. This case will be brought before a Belgian court at the end of this year. In addition to that, and because we are not only countering terrorist attacks, in Belgian law it is very difficult to pursue somebody for espionage or interference. So, we invest in prevention, we invest in advising the possible targets, but where we can, we try to disrupt hostile activities. And this can come in many forms.

Without getting into details I can refer to a recent case where we worked on an agent of the Chinese intelligence services imbedded in a think tank that was lobbying at the European institutions. By bringing this story out, by informing his contacts, we warned everybody that they would get involved in illicit activities if they would continue being in contact with him. In other words: we have disrupted hostile activities by a foreign intelligence agency.

If we notice illicit activities by foreign services in our country, we can also collaborate with the competent services to withdraw our target's residence permit or working permit for instance. In these cases, it is really difficult for us to pursue the offenders, but at least we can disrupt their activities and by doing so, limit the danger.

In our annual report we also talked about "hybrid threats" which is a common term for all the hostile activities by foreign intelligence services targeting our country and our society.

veiligheid van de staat
sûreté de l'état
VSSE

Disinformation or fake news and hostile takeovers are two of the core elements of these hybrid threats, as is the cyber threat emanating from countries as Russia, China, North Korea or Iran. We have to be honest, VSSE is not a big player when it comes to countering the cyber threat; the main role here is for the Belgian Center for Cybersecurity. However, this does not mean that we remain blind for it. Also, on this threat we maintain our preventive and advisory role, because the cyber threat is here to stay for the following years.

I would like to finish my presentation here, so that you would still have the time to pose all questions that you might have. With a little luck, I will even be in a position to answer some of them. But before that, I would like to make a little bit of publicity for our service. We are indeed always looking for bright young new colleagues. Since we are a government service, we do all of our recruiting via the official selection service of the federal government, Selor. Most of the time, you will have to pass a general selection before you can enter the specific VSSE exam to become an analyst, a data collector or a runner who works with human sources. So, if you are interested in working for VSSE, regularly look at the Selor website for general selections – it will always be notified when my service will do a specific selection on the basis of a general reserve.

And for further reading on my service, I would warmly recommend you to visit our website vsse.be.

Thank you.