УДК 323.2:004

The EU Intelligence Agencies: Flawed by Cognitive Overflow

M. Malfait

Milka Malfait, https://orcid.org/0000-0002-7438-4700, The Brussels Bar, 106 Avenue Louise, Brussels 1050, Belgium, milkamalfait@gmail.com

This article demonstrates the flaws of EU intelligence agencies the past decade in the field of counterterrorism, in particular regarding Jihadi terrorism. Since 2014 the West European countries fell victim to the violent actions of Islamic State (IS), which has a huge presence on social media, both on the surface web and on the Darknet. The goal is to outline the most important case-studies of Jihadi terrorism that were plotted and carried out by the terrorists and yet, not prevented by the classical intelligence authorities. A political analysis will explain why these attacks have not been thwarted despite the fact that most of the attackers were on the radar of the EU police and intelligence agencies. Recommendations are given how intelligence work on fighting radical Islamic terrorism can be done more efficiently, through Artificial Intelligence (AI). Artificial Intelligence is a game changer for risk management in intelligence as it provides the classical intelligence agencies with tools and AI solutions to identify and mitigate potential risks and prevent Jihadi terrorist attacks from the very first moment individuals start radicalizing.

Keywords: EU, Jihadi terrorism, intelligence, Artificial Intelligence, social media, risk management, private sector.

Received: 30.01.2020 / Accepted: 06.03.2020 / Published: 01.06.2020

Разведывательные службы ЕС: проблемы информационной перегрузки

М. Малфет

Малфет Милка, адвокат DLA Piper UK LLP, Брюссельская коллегия адвокатов, Бельгия, milkamalfait@gmail.com

Эта статья демонстрирует недостатки спецслужб ЕС за последнее десятилетие в области борьбы с терроризмом, в частности, в отношении джихадистского терроризма. С 2014 г. западноевропейские страны стали жертвами насильственных действий Исламского государства (ИГ), которое имеет огромное присутствие в социальных сетях, как в поверхностной паутине, так и в Даркнете. Цель работы – очертить наиболее важные случаи джихадистского терроризма, которые были задуманы и осуществлены террористами и которые, тем не менее, не были предотвращены классическими разведывательными органами. Политический анализ объяснит, почему эти атаки не были предотвращены, несмотря на то, что большинство нападавших были на радарах полиции и разведывательных служб ЕС. Даются рекомендации о том, как разведывательная деятельность по борьбе с радикализованным терроризмом может быть более эффективной с помощью искусственного интеллекта (ИИ). Искусственный интеллект – это игра, меняющая ситуацию в области управления рисками в разведке, поскольку он предоставляет классическим разведывательным службам инструменты и решения ИИ для выявления и снижения потенциальных рисков и предотвращения террористических атак джихадистов с самого начала, когда отдельные лица начинают радикализировать свою деятельность.

Ключевые слова: ЕС, джихадистский терроризм, разведка, искусственный интеллект, социальные сети, управление рисками, частный сектор.

Поступила в редакцию: 30.01.2020 / Принята: 06.03.2020 / Опубликована: 01.06.2020

DOI: https://doi.org/10.18500/1818-9601-2020-20-2-228-235

Introduction

Special attention is paid to the flaws and successes of EU crime prevention and thwarting Jihadi terror attacks. Fourteen case-studies of extremist terrorism in Western Europe proved that the national authorities of nearly all West European countries were unable to prevent all these massacres. The author also emphasizes the fact that despite many of these attackers were known to the police and intelligence services in the EU, the attacks could have been prevented. The problem that presented itself was the cognitive overflow of information that data analysts were not able to cope with, day after day. These failures can be overcome and compensated by the private security and surveillance industry, which shows a lot of successes. Instead circling around bulk data meta data is used and on top of it, with the help of revolutionary software, filters are used that reveal the most useful information and filter out the most useless data to detect radicalizing individuals. The risk management strategy of private AI companies is about better and more targeted data. In the EU there is currently a strong interdependency between the governmental and private sector in counterterrorism as a result of all the threats that plagued West European countries as well as all the innocent victims that fell. Concrete this means that today efforts are being made in the EU by the government and corporate world to establish better risk analysis and risk evaluation based on software that charts the OSINT of social media networks of radicalizing individuals

White swans in Islamic terrorism

In the aftermath of 9/11, and especially since 2014 all of Europe has come into the focus of transnational radical Islamic terrorism. The peak occurred in 2015–2016 [1, p. 114]. An overview on the most salient cases of terrorism proves this. As for many of the terror attacks which happened the past two decades, it can be concluded there were no real 'black swans'. According to Rice, Black swans are major events we never see coming [2]. It are hard-to-predict, and rare events that are beyond the realm of normal expectations in history, science, finance, and technology. Many of those terrorists were on the radar of the agencies, especially those related to the most recent attacks in Western Europe – with the exception of the Madrid bombings in 2004 and the assassinations of two Dutch politicians in 2002 and 2004, which occurred before 2014 when IS – a notable user of social media – gained global prominence. The truth is that the intelligence agencies actually could have known this would happen (see infra). Those terror attacks were in fact 'white swans'.

In Spain, the Madrid railway explosions of 11 March 2004 killed 193 people and injured around 2,000. Many of the perpetrators were of Maghrebian origin. The bombings are the deadliest terror attacks in Spain's history. As if this was not enough for Spain, on 17 August 2017, Younes Abouyaaqoub – who was born in Morocco – drove a van into pedestrians on La Rambla in Barcelona, killing 13 people and injuring at least 130 others, one of whom died 10 days later. Abouyaaqoub fled the attack on foot, then killed another person in order to steal the victim's car to make his escape. Nine hours after the Barcelona attack, five men thought to be members of the same terrorist cell drove into pedestrians in nearby Cambrils, killing one woman and injuring six others. All five of those attackers were shot and killed by police. The night before the Barcelona attack, an explosion occurred in a house in the Spanish town of Alcanar, destroying the building and killing two members of the terrorist cell, including the 40-year-old imam thought to be the mastermind. This attack was qualified as a jihadist attack by the Spanish authorities. Later responsibility for the attack was attributed to IS. Abouyaaqoub was later killed by police on 21 August 2017.

After 9/11, the Netherlands experienced on 6 May 2002 also a shock of its own: the murder of Pim Fortuyn, a Dutch politician, was assassinated by the Dutchman Volkert van der Graaf in Hilversum, nine days before the Dutch general election of 2002. He prompted controversy in the eyes of his assassin with his views on multiculturalism, immigration and Islam in the Netherlands. Another wake-up call on terrorism followed two years later on 2 November 2004 with the assassination of Dutch film producer Theo van Gogh. Mohammed Bouyeri, a Moroccan-Dutchman, shot van Gogh in the stomach. After van Gogh staggered to the other side of the street, Bouyeri shot him several more times and slashed his throat with a curved machete. Bouyeri then pulled a smaller knife from his bag that he used to pin a letter to the body of van Gogh. The letter was addressed to Ayaan Hirsi Ali who, together with van Gogh, produced the movie 'Submission', criticizing the abuse of women under Islam [3, p. 286].

The UK, also a breeding ground for radicalization, remained not spared. The 7 July 2005 London bombings [4, p. 50], were a series of coordinated Islamic terrorist suicide attacks that targeted commuters travelling on the city's public transport system during the morning rush hour. Apart from the bombers, 52 UK residents of 18 different nationalities, were killed, and more than 700 were injured in the attacks, making it Britain's deadliest terrorist incident since the 1988 bombing of Pan Am Flight 103 near Lockerbie, Scotland, and England's deadliest since World War II, as well as the country's first Islamist suicide attack. Three of the bombers were British-born sons of Pakistani immigrants; one was a convert born in Jamaica. A suicide bombing attack took place in Manchester Arena, United Kingdom on 22 May 2017. A radical Islamist detonated a homemade bomb as people were leaving the Manchester Arena following a concert by the American singer Ariana Grande. 23 people died, including the attacker, and 139 were wounded, more than half of them children. Several hundred more suffered psychological trauma. The bomber was Salman Ramadan Abedi, a 22-year-old local man of Libyan ancestry.

France was also seriously hit by Jihadi terrorism, maybe the most of all. On 7 January 2015 the Charlie Hebdo shootings were done by two French brothers from Algerian origin: Saïd and Chérif Kouachi. Armed with rifles and other weapons, they killed 12 people and injured 11 others. The gunmen identified themselves as belonging to the Islamic terrorist group Al-Qaeda in the Arabian Peninsula, which took responsibility for the attack. Several related attacks followed in the Île-de-France region on 7–9 January 2015, including the Hypercacher kosher supermarket siege where a terrorist, named Amedy Coulibaly held 19 hostages, of whom he murdered 4 Jewish people. This perpetrator of Malian-French nationality was close friends with Saïd and Chérif Kouachi from the Charlie Hebdo shootings. On 21 August 2015, a Thalys Train was on its way from Amsterdam to Paris, crossed the Belgium border to France and a Moroccan man Ayoub El Khazzan, who boarded in Brussels, opened fire. In May 2015, some months before the Thalys train attack, the Belgian intelligence service received an information request from its Spanish counterpart about a young Moroccan who was already 'flagged' to the Belgian Intelligence service in October 2012. The message was one out of the 22,000 the security services received in 2015 and had no urgency notification. No further action was undertaken. On August 17, the Spanish sent the request to identify three mobile numbers in

connection with the target's case. The Belgian Intelligence replied with those identifications on August 22, a day after the subject in question was overtaken while attacking passengers in the train. Being on the radar of two intelligence services, the fact that the terrorist was able to move undetected, had a lot to do with the fact that the urgency was not taken into account [5, p. 8]. The Bataclan attacks in Paris on 13 November 2015 were planned in Syria and executed from Belgian soil [6, p. 928]. The attackers killed 130 people, including 90 at the Bataclan theatre. Another 413 people were injured, almost 100 seriously. Most of the Paris attackers had French or Belgian citizenship such as Brahim Abdeslam and Bilal Hadfi, two other perpetrators were Iraqis, and some had fought in Syria. Some of them had entered Europe among the flow of migrants and refugees. The mastermind of the attacks Abdelhamid Abaaoud was a Belgian-Moroccan Islamic militant who had spent time in Syria. The Abdeslam brothers would later be linked to the Brussels bombings in 2016. Another interesting fact is that there have been early warnings concerning these attacks. In 2009 there was a terror attack in Cairo and the Bataclan was mentioned. In the summer of 2015, some months before the attacks, the threat against rock concert halls comes up, due to a detained Syriafighter who informed the French authorities he has been given orders to carry out an attack on a rock concert hall by the very same person that would be the mastermind of the Bataclan attacks just some months later. The ringleader was clearly recruiting. He was seeking for someone 'physically and mentally' capable to execute the attack. Because his connection refused, the mastermind took later the initiative. According to a French parliamentary committee there was no connection between the 2009 and 2015 warnings. The Bataclan attacks also happened despite the heightened state of alert due to warnings coming from several foreign intelligence agencies. On the evening of 14 July 2016, a 19-tonne cargo truck was deliberately driven into crowds of people celebrating Bastille Day on the Promenade des Anglais in Nice, resulting in the deaths of 86 people and the injury of 458 others. The driver was Mohamed Lahouaiej-Bouhlel, a Tunisian resident of France. The attack ended following an exchange of gunfire, during which Lahouaiej-Bouhlel was shot and killed by police. IS claimed responsibility for the attack. The south of France is a stronghold of Islamist militancy. From a Jihadi point of view, Nice was the most perfect attack with worldwide media coverage. The terrorists used the city of Nice for a 'PR stunt'. Among the 86 victims, there were more than a dozen nationalities. It was a media scoop of high level publicity, with a maximum of 'resonance'. The terrorists also wanted to oppose themselves against 'the French nationality' on the French National holiday. On 26 July 2016, only two days after the massacre of Nice, two 19-year-old Islamist terrorists, Adel Kermiche and Abdel Malik Petitjean, were perfectly able to attack unhindered participants in a Mass at a Catholic church in Saint-Ėtienne-du-Rouvray in Normandy, northern France. Wielding knives and wearing fake explosive belts, the men took six people captive and later killed a 85-year-old priest Jacques Hamel, by slitting his throat, and also critically wounded an 86-year-old man. The terrorists were shot dead by the police as they tried to leave the church. The attackers had pledged allegiance to IS which claimed responsibility for the attack

The Charlie Hebdo shootings, the failed attack on a Thalys train and the Bataclan attacks also compelled the Belgian government to seriously commit to national security. There were indications of a similar danger brewing on Belgian territory. A large – scale anti-terror raid was set up in the town of Verviers and rolled up a terrorist cell. Within hours of the Bataclan attacks it became clear that the terrorist's base of operations was a municipality on the outskirts of Brussels, Sint-Jans-Molenbeek [7, p. 478]. It was only a matter of time until some evil would slip through the mazes of the net. Later, the country itself fell victim to terrorist attacks on 22 March 2016 [7, p. 465]. The perpetrators involved in the November 2015 attacks in Paris were based in Molenbeek, and Brussels went into lockdown for five days from 21 to 26 November to allow the police to search for suspects. According to the Belgian authorities the 'European bubble' in Brussels as well as the Rue du la Loi and the Avenue Louise were already mentioned in the November-lockdown as potential targets, all of them places where there is a huge concentration of Belgian government officials, European politicians and expats working and living. According a former Eurojust officer, in 2016 a Joint Investigation Team (JIT) was set up between the French and Belgian agencies. Based on information gained from several raids in Brussels, the police were able to arrest on 18 March 2016, 4 days before the bombings, Salah Abdeslam, a suspected accomplice of the Paris attack. Those anti-terrorist raids killed another suspect and injured two others. Though the effective combined efforts of the French and Belgian services led to a quick and much-needed victory, it would prove to be a very short one. Four days later, the Bakraoui siblings conducted two coordinated attacks, the first in the departure hall of Brussels airport and shortly afterwards on a carriage of the metroline to the EU quarter of the city. Causalities went up to 32 dead and over 700 wounded [6, p. 940]. Their names had already been flagged in connection to the Paris attacks by the JIT. Also during his interrogation, four days earlier, Abdeslam was presented with photographs of the Bakraoui siblings. How could indications of an obviously carefully coordinated attack have been missed? Among the disconnects were the faulty follow-up on these convicted criminals by the correctional services; the failure to communicate information about the Molenbeek hide-out address which turned out to have been in the possession of the Malines police in Bel-

gium as early as three weeks later after the bloodbath in Paris – but was not shared [7, p. 479] and the fact that one of the Brussels attackers was arrested by the Turkish authorities attempting to cross into Syria in June 2015. Notification reached Belgian police only after he had been deported, while judicial authorities separately issued an arrest warrant, long after the bird had flown [6, p. 942]. The other airport bomber, who escaped and was apprehended in April 2016, had appeared on MI5's radar. Only post factum the pieces were put together. Belgian investigators believe that Abdeslam's arrest may have hastened the Brussels bombings. These were all completed, non-thwarted attacks and in many of the cases JITs were established between the French and Belgian authorities. According to the Belgian Interior Ministry authorities knew of preparations for an extremist act in Europe, but they underestimated the scale of the attack. A New York Times article noted how a list containing the names of the terrorists has been sent to the mayor of Molenbeek a month before the attacks [7, p. 479]. Interesting fact is that this particular mayor could stay in power by votes from radicalized individuals, their families and clans living in Molenbeek. It is clear Belgium became a breeding ground for radicalized Islamic terrorism, but these were not the only terrorist cell active on Belgian territory: In the end of 2007 there were Al Qaida's exhortations to attack the countries that were part of the military intervention in Afghanistan. Investigation services in Belgium had indications for a possible terrorist plot to be organized on the Brussels Grand Place [6, p. 933]. In May 2014, a gunman and Syriafighter named Mehdi Nemmouche attacked the Jewish Museum of Belgium in Brussels, killing four people [6, p. 937]. The extremist imams and groups such as Sharia4Belgium were declared as a terrorist organization by the correctional tribunal of Antwerp in February 2015 [5, p. 6]. In Belgium, a point of concern are the activities conducted at mosques and the potential for prison radicalization. As an illustration some 600,000 Muslims – largely of Moroccan or Turkish origins – live in Belgium out of a population of about 11 million and attend slightly over 300 mosques [5, p. 6], while Belgium, a highly civilized West European country that mainly has or better 'had' the Christian civilization as cornerstone of its society, counts 4296 Catholic churches [8]. Relatively this is a great percentage of Islam infiltration in a small Catholic country. Out of this 'percentage' there will always be a very small amount radicalize and precisely these individuals form a threat for the indigenous citizens. According to a Flemish Minister, the religion Islam in itself is not the primary problem, it is a secondary one, yet the problem is that Islam is often used and abused by extremists.

Although Sweden is miles away from the nerve centre of IS in the Levant, it has also been proven that terrorism does not respect borders and even penetrated Scandinavia. The 2017 Stockholm truck attack was an Islamist terrorist attack which took place on 7 April of that year in central Stockholm. A hijacked truck was deliberately driven into crowds along Drottninggatan – one of the busiest shopping streets of Stockholm – before being crashed into an Åhléns department store. Five people were killed including an eleven-year-old girl and 14 others were seriously injured [9, p. 1]. The perpetrator was Rakhmat Akilov, a 39-year-old rejected asylum seeker and a citizen of Uzbekistan, who was apprehended several hours later. He had sworn allegiance to IS in a self-recorded video the day before the attack, and Uzbek authorities said he had allegedly joined the group. Akilov was convicted of murder and terrorist crimes, and sentenced to life in prison and, if released, deportation to Uzbekistan and lifetime expulsion from Sweden.

Also, Germany, the country that is coming off worst of the EU migration crisis, has experienced the darksides of the Wir schaffen das-policy [10, p. 1]. On 18 July 2016, Afghan refugee Riaz Khan Ahmadzai attacked and injured four people, two critically, on a train near Würzburg in Germany [11]. A fifth person was injured outside. The attacker was a 17-year-old asylum seeker, armed with a knife and hatchet. Germany marked it a terrorist attack with an Islamist religious motive. On 24 July 2016, only a week later, fifteen people were injured, four seriously, in a suicide bombing outside a wine bar in Ansbach, Germany. The bomber, identified as Mohammad Daleel, was a 27-year-old Syrian refugee who had pledged allegiance to Abu Bakr al-Baghdadi, leader IS. He was the only fatality in the incident. According to German authorities, Daleel was in contact with IS and had been planning more attacks before his backpack bomb exploded accidentally. On 19 December 2016, a truck was deliberately driven into the Christmas market next to the Kaiser Wilhelm Memorial Church at Breitscheidplatz in Berlin, leaving 12 people dead and 56 others injured. The perpetrator was Anis Amri, a Tunisian failed asylum seeker. The attacker has been known by the police as a radicalized individual. He was on the radar of other EU intelligence agencies too. Knowing that the German authorities were informed by the Moroccan agencies that he wanted to plot an attack, the attack still happened. Four days later he was by accident detected in a station in Milan, shot a police agent and was shot in return. Coincidence and luck. Do we have to rely on this for counterterrorism?

Better risk management through AI: a solution?

London, Boston, Paris, San-Bernardino, Brussels, Orlando, Nice, Würzburg, Ansbach, St. Etienne-du-Rouvray, London, Stockholm, Manchester. Fourteen terror attacks. The background of these attackers were quite diverse, but there seemed to be a pattern: at each attack at least one of the terrorists was known to the police, in each attack the perpetrators were part of a network, in each attack the terrorists were communicating electronically

with each other, in each of the attacks there was a digital footprint indicating radicalization, months and sometimes even days before the attacks. How can it be that despite all these traces and evidence, the intelligence had no idea that these attacks were being plotted? What kind of information and programs need intelligence services to protect us from the most dangerous attacks? According to Edward Snowden, *when we look at the Boston Marathon Bombings on 15 April 2013, which was during the height of American mass surveillance, it is clear that these surveillance programs did not stop the attack, even though the US has been specifically warned by foreign intelligence services that these individuals, the Chechen Kyrgyzstani-American brothers Dzhokhar Tsarnaev and Tamerlan Tsarnaev, were associated with terrorism. Much the same happened in Brussels. In the Brussels attacks, Belgium had been warned – by the Turks in this case – that some individuals were associated with terrorism*. Also the terrorists of the Paris attacks were known to the police, as well as those of the Berlin attacks, which were in this case signaled by the Moroccan authorities. The same is true for all the other mentioned cased. Snowden questions why mass surveillance failed to catch these terrorists. *It is not because they used encryption or because they were particularly skillful or clever, it is because when you collect everything, the communications of everyone in a nation, you understand nothing. People are drown in so much information that they can't find what is actually relevant.* So the fact that many of these terrorists were on the radar, but where not in time arrested does not necessarily indicate that the security agencies were not provided with enough information, *a contrario*, there is the problem of overload of information. Snowden was not the only one making this claim. Many data analysts in EU governmental agencies the past decade complained in their memo's about 'overcome by overload', 'flood of collection', 'too many choices', 'cognitive overflow', 'a tsunami of intercept is declared', 'overwhelming data'. They are literally drowning in their information. The complaint on mass surveillance, according to some former governmental agents is not one of civil liberties, but one of efficacy: it just doesn't work well enough. This also means that EU intelligence services were always about one year behind in evaluating data. As a result, every terrorist got at least one year to plot the attack. In fact, the planning of the attack in Nice, began exactly one year in advance as shown by analysis of the computer owned by the attacker.

A solution for this problem may be found in the private sector, under the condition that these private companies contribute to better prevention and mitigation of radical attacks, and don't make the same mistakes as the classical intelligence agencies, namely collecting too much irrelevant data. Juxtaposed to state security is the need for private security that contributes to crime prevention and community safety. In the EU, the private security sector as well as the corporate surveillance industry has grown from a handful of small companies at the end of the Second World War into a multibillion Euro industry with thousands of firms and millions of security staff [12, p. 245]. Governmental cooperation with both the private security sector and the corporate surveillance industry happens through the governance model of Public-Private Partnerships (PPP) and the outsourcing of intelligence.

In the EU the private security industry has assumed a substantial position in the provision of policing in most member states [13; 14, p. 214–215]. In a number of countries there are statistics, admittedly of varying quality, showing more private security staff employed than public police officers (Republic of Ireland, UK) and in other countries there are substantial private security sectors employing well over 150,000 staff (Germany, Spain and the UK) (Small Arms Survey 2011) [15]. The EU strongly endorses public-private cooperation, particularly with regard to investigations into money-laundering, illegal profits, financing terrorism and cybercrime [16, p. 55]. It is an example of New public management (NPM) and it has thus a profound impact on the administration and management of law enforcement and intelligence practice. These trends are not unique to the EU, with many other areas of the world also experiencing substantial growth in size and role of the private security industry. In the European Single Market, public procurement rules have been changed so companies can bid on contracts anywhere in the EU [17, p. 409].

Aside from the private security sector the corporate surveillance industry that deals with risk management is also huge. Since the boom of technological communications, the balance of intelligence changed from HUMINT to SIGINT dramatically, both in the governmental as well as in the private sector. SIGINT produces enormous procurements and much of the intelligence in the world is outsourced. Private contractors may contract with governments for a variety of surveillance services or products. It ranges from high-tech camera's in space, spy-planes, logistics, arms supply by private military companies (PMC), drones to AI-software. This huge lucrative business of hundreds of billions of dollars annually is leading to everything: counterterrorism, border control, crisis management, surveillance drones, CCTV, satellite surveillance techniques. The private surveillance monopolies have taken over in the world. In many countries the classical intelligence services are so dependent on the private sector that without these corporate surveillance giants everything would break down at the governmental agencies. To illustrate, in the EU, the Commission tried to develop in 2003 a 'EU military surveillance complex' and 'the Group of Personalities' in order to be competitive with the international surveillance market. Or take for instance the research project 'Feel Europe' which aims to measure human feelings and emotions through remote con-

trolled sensors and surveillance cameras. Basically, the goal is to detect terrorists assuming they would be agitated the hours before executing the attack.

Working with private security partners can entail many benefits for the traditional law enforcement and intelligence agencies. The private security sector can help traditional law enforcement to bridge the gaps and provide vital services in technology and resources as well as expertise that would not otherwise be available. Such operation can take the form of the secondment of staff, licensing of software, the use of equipment and buildings and in-kind donations. The mutual benefits are huge: private entities can offer a dynamic insight into new technologies in the areas of cybersecurity, biometric identification or ballistics. Information and communication technology has proven it became the backbone of economic growth. Also corporate surveillance is very useful. For instance, large international hotels in Africa or in the Middle East can be mobilized as intelligence services. They may be asked to carry out surveillance (for example, by hanging cameras on the street that can film terrorists). Another example are taxi companies such as Uber. According to a former Eurojust officer, driving taxis may be asked to take photographs if there is a threat of terrorism in a city or if attacks have just taken place, in order to film the suspects. AI in public administration can be used for forecasting high crime risks. Public administration has for instance adopted information and communication technology in order to construct new intelligence systems and design new risk prevention strategies in transportation management [18, p. 467].

Now that the benefits of approaching the private sector are clear, the question is whether these terror attacks in the EU could have been prevented. The Viennese start-up KIVU Technologies for instance which raised already more than 1.8 million EUR in seed financing, has developed a technology that enables investigating authorities to search for terrorist propaganda on the net. Their goal: the prevention of online radicalization through software engineering and AI. Their team – which consists of specialists of different backgrounds such as data scientists, mathematicians, hardcore software engineers and AI experts – has developed a sophisticated software program to prevent and predict radicalized forms of terrorism with the help of AI. Machine learning is combined with graph theory, algorithms and probabilistic methods.

The work environment 'par excellence' of IS is social media. Their propaganda happens mainly through online radicalization [19]. IS ringleaders in the Levant recruit people from Europe on social media. IS acts swiftly and responds to the invention of new technologies. Their aim is to get mass media attention. Their terrorism is about a lot of people watching, not about a lot of people dead. Attention is always the core of what these terrorists want to achieve. This is mirrored by the fact that their aim is to carry out attacks with the simplest possible means. Corporate AI companies can therefore make an efficient analysis of relatively big social networks with the help of mathematical methods of software engineering. Concrete this means that all radicalized individuals which are active on social networks can be represented in graphs. The individuals can be anonymized with dots and later it can be seen how the dots are connected: with whom are they connected, what is their geographical location, what is the frequency by which they contact each other, how many connections do they have.

According to Robert Wesley from KIVU technologies, the world is a network. *Everyone is connected both online as offline. The ability to present everything as a network, means we can run AI on top of the classical SIGINT and HUMINT strategies of the government. You can predict a lot from OSINT. With our program we identified some radicalizing individuals in Europe six months in advance compared to the traditional authorities*. There are religious problems, but also individual problems. *It is just a tactic. If you want to prevent contemporary terrorism, you need to take away the benefits from them, which is in this case their social networks*. According to Jan van Oort their software works at a high velocity: *We are talking here about milliseconds while others needs minutes or hours to track potential perpetrators*. According to one of his partners, Christian Weichselbaum, you can see on social media that they radicalize. *All their data is accessible to anyone online because their goal is to reach as many people as possible*. They are very open in sharing their data to the public and AI companies are very grateful for that. *All our data originates from OSINT, which is all the data openly available online. We use information available on sites such as Facebook, Twitter, blogs, but we also collect data from the darknet. With all these data we can analyze everything without needing to hack into mobile phones or emails (Cfr. SIGINT). This means we are not violating the privacy of the users nor the devices because this information is public and we don't need more*. Wesley also states that access to more data doesn't always lead to better intelligence. *It is an assumption that if you have more data, you can make more sense of the data. As we have seen from the past, even if you have all the data from all the communications, it is still difficult to make the connections, develop good intelligence and prevent attacks from happening*. Wesley states that mass surveillance is no guarantee. *Therefore, there is a need for more targeted efforts, more sophisticated strategies: not having more access to information, but better access to information, more targeted information collection through filters so that data analysts are not drown in data.* Wesley's team believes that machine learning and huge networks can solve this problem in counterterrorism. *AI can tell us things we were not observing before. The goal of KIVU technologies is to use OSINT to prevent terror attacks*.

Instead of collecting everything and then searching for keywords, a different approach is used. The content of a phone call, text message, or email becomes irrelevant. What become relevant is: who communicates with whom? When? How? How often and from where? In short, the metadata is important. Metadata is data that provides information about other data. In other words, it is data about data. It is also the data that is used to transport the content data around the networks. However, in the past decade the EU intelligence agencies have all been fundamentally circling around the bulk acquisition of data of any type, which proved to be inefficient and a waste of time. The conclusion is that there is an overload of bulk data on which SIGINT is based. The overload of information stands efficiency in the way, because there are not enough filters. This appears as well in the efficiency argument in a Weberian bureaucracy. Intelligence work should be done efficiently. On this problem private AI companies are currently working to assist governments.

If the classical intelligence agencies in the EU would have used software programs like the one of KIVU technologies and similar companies, this means the attackers would have been on 'top of the list' and the agencies would have been warned. Does the system also protects people's privacy? The team in Vienna is also aware that their program could also be used for something other as networks of terrorists. It will depend how governments will use this type of software. *We know since Snowden that surveillance tools are not only used to prevent crime, but also for spying activities of all kind, including spying on your own partner.* The team's response to the question of abuse is 'privacy by design'. This means that protection of privacy is built-in into the system. Antoine de Saint Exupéry wrote about technology and tried to answer the question: what is secure technology? What is highly developed technology? [20] Since he was a pilot his answer focused on aviation technology, but it can also be applied generally. *Good technology is technology that I do not have to think about*; *This means if I sit on a plane as a passenger, I don't have to worry about the engines*, states Jan van Oort, an aviation engineer. Regarding their software, this means that their meta data analysis collects only data related to suspects, which is encrypted immediately. After the quest is made to access the data by the government, an independent authority will generate three keys for decryption: one for the police and intelligence agencies, one for the judiciary and one for the legislative oversight. Only when all three keys are employed together, data can be inspected and used. Every access is locked. A digital record is generated every time data is accessed. That way the parties involved have the chance to justify themselves in a court of law in the case of abuse or error. Never has a program come closer to a solution that factors in both security and the fundamental right to privacy to equal degrees.

Conclusion

In intelligence there is thus need, not only for HUMINT and SIGINT, but also for OSINT. Collaboration between the classic law enforcement agencies is clearly not enough in the EU. That is why the private sector must also be involved in order to play its role. Private corporations may help governments in finding better risk management strategies to track radicalizing terrorists. OSINT is used as starting point and from these OSINT data, the metadata are used, which are in turn an extra filter. In the intelligence world risk analysis and risk evaluation (i.e. together risk assessment) should combine the best of both worlds: the traditional HUMINT and SIGINT from the governmental services and the progressive OSINT from the corporate world, translated into AI software. In case of the terrorists which infiltrated Western Europe and made it an unsafe place, their digital footprint showed their radicalization online, even one year, months or days before the attacks were executed. Conclusion: all these attacks could have been prevented, if there was made use of the right technologies.

References

1. Malfait M., Chernyavskiy S. I. The Russia-EU perspective: national security and counterterrorism from a different angle. *Political Science Issues***,** 2019, vol. 9, iss. 6 (46), pp. 114–124.
2. Rice C., Zegart A. *Political Risk: How Businesses and Organizations Can Anticipate Global Insecurity*. New York, Hachette Book Group, 2018. 336 p.
3. Den Boer M. G. W. Wake-up call for the Lowlands: Dutch counterterrorism from a comparative perspective. *Cambridge Review of International Affairs*, 2007, vol. 20, no. 2, pp. 285–302. DOI: https://doi.org/10.1080/09557570701414658
4. Gaines S., Goodwin R. Terrorism perception and its consequences following the 7 July 2005 London bombings. *Behavioral Sciences of Terrorism and Political Aggression*, 2009, vol. 1, iss. 1, pp. 50–65. DOI: http://dx.doi.org/10.1080/19434470802482167
5. Lasoen K. Belgian Intelligence SIGINT Operations. *International Journal of Intelligence and Counterintelligence,* 2019, vol. 32, no. 1, pp. 1–29. DOI: https://doi.org/10.1080/08850607.2018.1488501
6. Lasoen K. Indications and Warning in Belgium: Brussels Is Not Delphi. *Journal of Strategic Studies,* 2017, vol. 40, no. 7, pp. 927–962. DOI: https://doi.org/10.1080/01402390.2017.1288111
7. Lasoen K. For Belgian Eyes Only: Intelligence Cooperation in Belgium. *International Journal of Intelligence and Counterintelligence*, 2017, vol. 30, no. 3, pp. 464–490. DOI: https://doi.org/10.1080/08850607.2017.1297110
8. Jaarrapport de Katholieke Kerk in België. *Kerknet.* Available at: https://www.kerknet.be/sites/default/files/2018_Jaarraport%20Bisschoppenconferentie%20-%20light.pdf (accessed 3 February 2020).

[9] Ekström A., Eng-Larsson F., Isaksson O., Kurland L., Nortberg M. The effect of a terrorist attack on emergency department inflow: an observation study using difference-in-differences methodology. *Scand. J. Trauma Resusc. Emerg. Med.,* 2019, vol. 27, no. 57. DOI: https://doi.org/10.1186/s13049-019-0634-2

[10] Galantino M. The migration–terrorism nexus: An analysis of German and Italian press coverage of the 'refugee crisis'. *European Journal of Criminology*, 2020, 147737081989621, pp. 1–23. DOI:10.1177/1477370819896213

[11] Goertz S. Radikalisierung im Phänomenbereich Islamismus und islamistischer Terrorismus sowie Prävention. In: *Terrorismusabwehr*. Wiesbaden, Springer VS, 2019, pp. 147–182. DOI: https://doi.org/10.1007/978–3-658-20899-8_6

[12] Button M., Stiernstedt P. The evolution of security industry regulation in the European Union. *International Journal of Comparative and Applied Criminal Justice,* 2017, vol. 41, no. 4, pp. 245–257.

[13] Jones T., Newburn T. (eds.). *Plural policing: A comparative perspective*. London, Routledge, 2006. 256 p.

[14] Sarre R., Van Steden R. The Growth of Private Security: Trends in the European Union. *Security Journal*, 2007, vol. 20, no. 4, pp. 211–221. DOI: 10.1057/palgrave.sj.8350052

[15] Small Arms Survey, A booming business private security and small arms, 2011. Available at: http://www.smallarmssurvey.org/publications/by-type/yearbook/small-arms-survey-2011.html (accessed 27 January 2020).

[16] Den Boer M. G. W. Police, policy and politics in Brussels: Scenarios for the shift from sovereignty to solidarity. *Cambridge Review of International Affairs,* 2014, vol. 27, no. 1, pp. 48–65. DOI: https://doi.org/10.1080/09557571.2013.810588

[17] Button M., Stiernstedt P. Comparing private security regulation in the European Union. *Policing and Society,* 2018, vol. 28, iss. 4, pp. 398–414. DOI: https://doi.org/10.1080/10439463.2016.1161624

[18] Kouziokas G. The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment. *Transp. Res. Proc.,* 2017, vol. 24, pp. 467–473.

[19] Baugut P., Neumann K. Online propaganda use during Islamist radicalization. *Information, Communication & Society*, 2019, pp. 1–23. DOI: https://doi.org/10.1080/1369118X.2019.1594333

[20] Blakemore E. In Flight with Antoine de Saint-Exupéry, *JSTOR Daily*, 2015. Available at: https://daily.jstor.org/flight-antoine-de-saint-exupery/ (accessed 15 January 2020).

Образец для цитирования:

Malfait M. The EU Intelligence Agencies: Flawed by Cognitive Overflow [*Малфет М.* Разведывательные службы ЕС: проблемы информационной перегрузки] // Изв. Сарат. ун-та. Нов. сер. Сер. Социология. Политология. 2020. Т. 20, вып. 2. С. 228–235. DOI: https://doi.org/10.18500/1818-9601-2020-20-2-228-235

Cite this article as:

Malfait M. The EU Intelligence Agencies: Flawed by Cognitive Overflow. *Izv. Saratov Univ. (N. S.), Ser. Sociology. Politology,* 2020, vol. 20, iss. 2, pp. 228–235. DOI: https://doi.org/10.18500/1818-9601-2020-20-2-228-235