GLOBSEC INTELLIGENCE REFORM INITIATIVE

REFORMING TRANSATLANTIC COUNTER-TERRORISM

www.globsec.org

GLOBSEC POLICY INSTITUTE

Table of Contents

Abbreviations

AQAP	Al-Qa'ida in the Arabian Peninsula
CdB	Club de Berne
CEPOL	EU Agency for Law Enforcement Training
CoE	CT Centre of Excellence
CT	Counter-Terrorism
CTF	Counter-Terrorism Fusion Centre
CTG	Counter-Terrorism Group
CTIC	Western Counterterrorist Intelligence Centre
DGSI	Direction Générale de la Sécurité Intérieure
ECTC	European Counter Terrorism Centre
EEAS	European External Action Service
EU INTCEN	EU Intelligence Analysis Centre
FIU	Financial Intelligence Unit
GIRI	GLOBSEC Intelligence Reform Initiative
HUMINT	Human Intelligence
ISIL	Islamic State in Iraq and the Levant
JIC	Joint Intelligence Committee
JTAC	United Kingdom's Joint Terrorism Analysis Centre
LinCT	Leadership in Counter Terrorism
MS	Member States
PNR	Passenger Name Record
SATCEN	EU Satellite Centre
SIENA	Secure Information Exchange Network Application
SIGINT	Signals Intelligence
SMART	Scotland's Strategic Multi-Agency Response Team
STRA	Strategic Threat and Risk Assessment
TEU	Treaty on the European Union
TFTP	EU-US Terrorist Finance Tracking Programme
TFEU	Treaty on the Functioning of the European Union

Executive Summary

This report's primary focus is the Salafi jihadist terrorist threat. Since 2014, there has been a significant increase in attacks by these groups and, in Europe alone, at least 274 civilians have been killed and over 960 wounded. Building on the experience of foreign fighters, terrorist tactics are evolving rapidly to blend small, overlapping and informal networks of extremists capable of conducting both sophisticated and crude attacks. These groups retain the intent and capability to cause further harm.

These attacks have revealed major seams in some nations' law enforcement and intelligence capacities and capabilities, and highlighted failures in both domestic and transnational counter-terrorism liaison. Better liaison is not only possible, but also a political responsibility. It is time to adapt and address existing barriers to better law enforcement and intelligence integration and transnational liaison. These include issues of trust, standardisation, legislation, counter-terrorism approaches and culture. These must be addressed incrementally through existing best practises and models.

The key problem the Globsec Intelligence Reform Initiative (GIRI) addresses is that of intelligence and personal data sharing and its operationalisation at the domestic as well as transnational level. Altough many intelligence agencies have been at the centre of counter-terrorism efforts since 9/11, this report recognises that as terrorism is fundamentally viewed as a crime in both Europe and North America, law enforcement is increasingly at the centre of better pan-European and transatlantic counter-terrorism cooperation. Crucially, better fusion of intelligence processes, and intelligence and law enforcement agencies, is needed to provide the means for pre-empting terrorist attacks before they occur, rather than relying on effective investigation after the event.

The GIRI report is based on extensive interviews and consultations with GIRI's network of serving and former counter-terrorism officials and academics from Europe and North America. Our approach is not to recommend new top-down institutions or bureaucracies. Rather it is to build capacities and capabilities to address existing problems by implementing best practises already utilised by some nations, through existing institutions and innovative technologies. It also argues for better joint training to encourage standardisation.

Based on existing models, the report introduces four, bottom-up practical solutions to these largely operational and tactical CT challenges. Its first proposal calls for the establishment of a permanent Core Transatlantic Counter-Terrorism Hub, which would mark an initial step toward providing a secure space for linking existing national CT centres with high degrees of mutual trust. The success of this core hub, would encourage less capable and/or willing nations to improve their services in order to join. Experience has shown that co-location leads to collaboration, and through strategic coordination, can lead to integrated approaches built on a solid foundation of trust enabled through enhanced social relations. Secondly, the report advocates for operational Case-Based Task Forces to be set up within the Hub, designed to react to current, emerging and residual CT challenges. Such task forces would promote proactive, intelligence-led operations through the fusion of enhanced, assessed intelligence/personal data. Thirdly, the report advocates for a single search interface to enable real time information exchange. This so-called "hit-no-hit" single search interface would enable each nation to hold and control its data, but encrypted searches would help identify information or patterns for follow-up, enabling member states to be better equipped to protect the safety and security of their citizens. No longer should the word secret be an inhibitor to good and effective information exchange. GIRI's fourth recommendation is to establish a transatlantic CT Centre of Excellence, which would enable joint risk assessments, standardisation and training. It would also create a much-needed bridge between intelligence and law enforcement professionals on CT issues, and promote the social relations upon which trust rests.

1. Introduction

A new transatlantic security architecture is needed. Salafi jihadist terrorist attacks in France, Belgium, Germany and Denmark, as well as in the United States, have exposed major loopholes in some nations' security architecture and highlighted that counter-terrorism co-operation needs to be better integrated at the transnational level to address the 21st century threat. More specifically, they have highlighted a pressing need to raise some nations' intelligence and law enforcement capabilities, and better integrate these capabilities to stop small, informal overlapping networks of violent extremists from conducting both sophisticated and crude terrorist attacks. This evolving nature of transnational terrorism necessitates a joint transatlantic approach and updated security strategies that rest on 21st century means, technology and alliances.

Clearly, many of the problems behind the rising threat from jihadist terrorism in Europe and North America are related to macro factors beyond the scope of this report, such as issues concerning EU immigration, social exclusion, and unrest in Iraq, Syria and Libya, some of which, it should be recognised, may have been exacerbated by the past policies of some Western nations. However, in the wake of the Brussels attacks, public criticism of counter-terrorism failures has reached a new pitch, increasing political pressure for the reform of European and transatlantic counter-terrorism cooperation.

The GLOBSEC Intelligence Reform Initiative (GIRI) is a pan-European and North American network of serving and former counter-terrorism officials and academics who recognise the need for change in the transatlantic security architecture. At the heart of the GIRI Initiative lies this report. Based on extensive consultations and interviews with former practitioners and experts in the intelligence, law enforcement, defence, and home affairs sectors across Europe and the US, this report identifies key tactical and operational counter-terrorism issues within intelligence and law enforcement. It then proposes practical solutions to these issues based on pre-existing "best practice".

GIRI's primary focus is on the growing internal security threat across the European and North American continents. The key problem this report addresses is that of intelligence and personal data sharing and its operationalisation at the domestic as well as transnational level. Altough many intelligence agencies have been at the centre of counter-terrorism efforts since 9/11, this report recognises that as terrorism is fundamentally viewed as a crime in both Europe and North America, law enforcement is increasingly at the centre of better transatlantic counter-terrorism cooperation. Crucially, better integration of both intelligence and law enforcement agencies is needed to provide the means for pre-empting terrorist attacks before they occur, rather than relying on effective investigation after the event. The sharing of intelligence provides a richer picture in terms of what is collectively known, and therefore allows the "collective" to focus on what it does not know, directing sensitive sources to fill those "gaps". This helps deliver greater confidence in the collective understanding of the threat and identify the strategies needed to manage and mitigate these threats before they manifest themselves and threaten the very fabric of our communities.

Our approach is not to recommend new top-down institutions or bureaucracies. Rather it is to build capacities and capabilities to address existing problems by implementing best practises already utilised in some nations, through existing institutions and innovative technologies. The report argues that we need both ad hoc, threat-focused networks, which initially engage a core number of nations in order to gradually encourage wider cooperation, as well as broader search systems, to enable better counter-terrorism information and intelligence sharing. It also argues for better training to encourage standardisation and trust.

We recognise that while the EU must play a role, CT intelligence and law enforcement reform cannot be solely an EU project. Not only are threats transatlantic, but especially after Brexit, some of the key European players in security will be outside the Union, as is the US. Even within the EU, according to the Lisbon treaty, national security is the sole responsibility of member states (MS). More specifically, Article 4 (2) of the Treaty on the European Union (TEU) stipulates that national security remains the sole competence of MS, preserving the prerogative for national security to be under exclusive national (and not EU) control. However, information exchange between all relevant security stakeholders at EU level, including the security intelligence community and law enforcement authorities, is possible under Article 67 (3) of the Treaty on the Functioning of the European Union (TFEU) which sets out that the Union shall endeavour to ensure a high level of security through measures for "coordination" and "cooperation" between police, judicial and other competent authorities. These competent authorities can be understood to include security and intelligence services. Thus, while the EU does have a prerogative to improve CT information exchange between MS, the responsibility for capacity building and liaison primarily rest with MS and their ability to network and build trust.

Our focus on Salafi jihadist terrorism is justified by the fact that it has been the most lethal form of terrorism in Europe and North America since 2014. We also contend that many of our proposed solutions are applicable to other forms of terrorism and, potentially, the rising cyber threat. Nevertheless, we recognise that addressing the root causes of terrorism, as well as containing it beyond European and American borders, are fundamental to solving this complex global security threat.

It should be noted from the outset that drawing on experiences from numerous nations, and respectful of the different politics, legal foundations and cultures across the transatlantic space and within Europe, GIRI has endeavoured to present unpartisan and inclusive practical solutions through which all nations concerned could benefit. While we recognise that some of our proposals would require legislative changes in certain nations, we argue that the changing nature of terrorism will eventually force these changes on these nations anyway.

1.1. Terminology

As this paper argues, effective transatlantic counter-terrorism (CT) is increasingly reliant on the integration of intelligence, security and law enforcement agencies, and on the fusion of the "intelligence" and "personal data" that these agencies primarily deal with. The main purpose of intelligence is the accumulation of political, strategic, operational and tactical advantage over adversaries.[1] Intelligence therefore helps decrease uncertainty to enhance decision making. Throughout the paper, the term "intelligence and security agencies" or services refers to nations' internal and external organisations that collect, analyse, share and operationalise sensitive information often gathered by covert means. These range from purely intelligence collectors to those that have a domestic responsibility to protect their nation from threats. "Law enforcement" agencies refers to national-level, local and/or specialised police and border control forces.

It is also important to distinguish between information sharing and liaison between law enforcement and intelligence services. Both are sensitive but in different ways. "Personal data" sharing refers to that often conducted by law enforcement and includes information such as databases of: passports, criminal records, fingerprints, vehicle registrations, DNA, advance passenger movements, and credit card and bank details which ought to be accessible by investigators with the right legal authority. As the section below outlining recent attacks highlights, there is scope for major improvement here before the sharing of intelligence is better integrated. "Intelligence liaison" refers to establishing capacity

[1] Hatlebrekke K.A. (2011), *Towards a Theory of Intelligence: The Art of Knowing beyond the Limits of Formal Logic, Why Intelligence is Art and its Impact on The Problem of Induction and Discourse Failure*, Doctoral Thesis of Philosophy in War Studies, Department of War Studies, King´s College, London, p. 275.

and rules among transatlantic allies to enable the sharing of secret information assessments, as well as selected raw intelligence, often collected by covert or sensitive means. Importantly, as this report shows, law enforcement agencies involved in the investigation of serious and complex crimes including terrorism also increasingly rely on covert and/or “intelligence techniques”, so the distinction between the two communities can be blurred.

“Liaison”, also referred to here as “sharing”, is used in a twofold way. First, domestic liaison refers to cooperation between intelligence and law enforcement agencies within a particular nation. Transnational liaison is that between intelligence or law enforcement agencies from multiple nations, either conducted bilaterally or multilaterally. To date, multilateral transnational liaison in the field of law enforcement has most prominently been developed within Europol and Interpol. In terms of intelligence, a prime example of long-standing transnational intelligence liaison is the “Five Eyes” system, comprising of Australia, Canada, New Zealand, the United Kingdom and the United States. Within the European CT context, the Club de Berne’s (CdB) Counter-Terrorism Group (CTG) is also of increasing prominence.

2. The Evolving Jihadist Threat

The Salafi jihadist terrorist threat inside Europe has never been more pressing. While we recognise that separatist and transnational terrorism was more lethal in some years of the 1970s and 1980s, and that the threat from al-Qa'ida endures, since 2014 there has been a significant increase in attacks by individuals and groups linked to Islamic State in Iraq and the Levant (ISIL) across the Continent. Between May 2014 and August 2016 at least 21 serious ISIL-related attacks have occurred inside the EU, killing 274 and wounding 968 citizens, 217 of whom were critically injured. The lethality of these attacks has demonstrated ISIL's clear intent to target Europe, while the terrorists' evolving capabilities have also highlighted failings among European nations' intelligence, security and law enforcement services. During the same period, the most lethal terrorist attack in the US since 9/11 was conducted by an ISIL sympathiser, while major attacks in Tunisia, on a Russian airliner, and in Turkey indicate the transnational nature of the jihadist threat. Violent jihadist attacks have included those directed or planned by ISIL as well as those inspired by ISIL propaganda. The latter are sometimes referred to as "lone actors", but rarely act without the support of others. Understanding the nature of these attacks is crucial for assessing this evolving terrorist threat and the challenge it poses to transatlantic security. Below we present the first open-source comprehensive, collective analysis of recent attacks. Those familiar with the evolution of terrorist attacks since 2014 may wish to skip to Section 2.3.

Since Europe's first ISIL-related attack in May 2014, when a lone gunman, Mehdi Nemmouche, shot dead four people in a Jewish museum in Brussels, there have been at least ten other "lone actor" attacks on the Continent and in the US. A French/Algerian citizen, Nemmouche had fought for ISIL in Syria, and the attack was the first incident of a European jihadist committing an act of terrorism after returning from Syria. Although viewed as a lone actor attack, Nemmouche had likely been instructed to attack Europe whilst in Syria. The next incident occurred on 20 December 2014, when a French man of Burundian origin, Bertrand Nzohabonayo, entered a police station near Tours in France and attacked officers with a knife, injuring three before he was shot dead. Prior to the attack, Nzohabonayo had been reported to French security services and had links to ISIL.[2] In the following days, another two attacks occurred in Dijon (11 injured) and Nantes (1 killed, 10 injured) involving the running-over of pedestrians by men in vehicles, allegedly shouting Islamist phrases during the incident. One of the attackers was previously known to police, but both men had psychiatric issues, and their links with terrorist groups were disputed.[3] However, it is worth noting that ISIL propaganda at this time had been encouraging lone actor attacks of this sort, and similar tactics have since been used to great effect.

On 7 January 2015 brothers Cherif and Said Kouachi – armed with assault rifles – attacked the offices of the Charlie Hebdo magazine, killing two policemen, ten civilians and wounding a further 11 before fleeing Paris. The following day, a policewoman was shot dead and a passer-by wounded in a Parisian suburb by another jihadist, Amedy Coulibaly. Coulibaly had pledged allegiance to ISIL and was in contact with the Kouachis during the attacks. Indeed, when the Kouachis were killed after a brief hostage situation in a factory north of Paris on 9 January, a major standoff with more hostages took place between Coulibaly and the security forces in a Parisian supermarket. By the time French special forces entered the supermarket and killed Coulibaly, four more civilians were killed and another 11 wounded. This brought the total to 15 dead and 23 injured in what became known as the "Charlie Hebdo" attacks.

The attacks were significant for a number of reasons. Firstly, the attackers used firearms bought from criminal networks, rather than smuggled from warzones. Secondly, the coordinated and dynamic assaults on numerous soft targets severely tested the French security forces' ability to respond

[2] "French anti-terror department investigates knife attack in Nice", *Euronews*, 4 February 2015, retrieved 17 November 2015.

[3] "France endures deadly attacks", *Reuters,* 22 December 2014, retrieved 17 November 2015.

rapidly, while the willingness of the attackers to sacrifice themselves meant that counterterror forces would therefore need to intervene more rapidly and robustly in future. Meanwhile, it emerged that the Kouachis and Coulibaly knew each other, had been radicalised in France, and that their actions had likely been coordinated by another jihadist. Cherif Kouachi was a known jihadist who had been imprisoned in France on terrorism charges in 2008, and the Kouachis had travelled to Yemen in 2011 where they received training and funding from al-Qa'ida in the Arabian Peninsula (AQAP). Indeed, in the wake of the attacks it also emerged that the US provided the French authorities with intelligence on the Kouachis' activities in Yemen. Although the French began monitoring them, this was stopped in spring 2014, most likely for resourcing reasons. Thus, the Hebdo attacks also represented a failure to direct and prioritise targets, and hence an intelligence and operational failure.

The Hebdo attacks were followed by numerous, smaller-scale incidents across Europe, indicating that ISIL was supplementing lone actor attacks with larger assaults conducted by cells with supporting networks. On 15 January 2015 in Verviers, eastern Belgium, two jihadists were killed and another arrested during a CT raid against a group suspected of planning a "major" attack on Belgian police. The suspects, all Belgian nationals of Arabic descent, opened fire when special forces closed in on them. According to Belgian media, they had recently returned from Syria and were in the final stages of a plan to attack a police station and publicly behead an officer.[4] Meanwhile, over 14-15 February, a radicalised Danish citizen of Arab descent conducted a series of shootings in Copenhagen which killed two civilians and left five police officers wounded before the gunman was shot dead. The attacker had been known to the police previously, and Danish intelligence were aware he had been radicalised in prison. Four men, who helped the attacker procure weapons before the attack, and gave him ammunition and a change of clothes during the attacks, were charged with terrorism offences in January 2016.[5]

On 26 June 2015, two ISIL-inspired attackers decapitated one person and blew up a gas canister in a factory in Saint-Quentin-Fallavier, near Lyon, France. One person was killed and twelve were injured, as well as the assailants. Then, on 21 August 2015, a shooting and stabbing incident took place on board a Thalys train in France on its way from Amsterdam to Paris. Three people were injured before Ayoub el-Khazzani, from Morocco, was arrested for the attack. El-Khazzani was apparently known to French authorities and had been tagged with a "fiche S" (security file), in order to monitor him. He had been similarly profiled by Belgian, Spanish, and German authorities. Upon leaving Spain for France in 2014, the Spanish authorities informed the French of their suspicions. El-Khazzani also spent two months in Syria in 2015. Meanwhile, in Berlin, on 17 September 2015, an Iraqi extremist was shot dead after he stabbed a policewoman in the neck.[6]

2.1. The Paris Attacks

The largest-scale terrorist attack in the EU since the 2004 Madrid bombings occurred on the evening of 13 November 2015 in Paris, when numerous ISIL-inspired terrorist cells attacked multiple soft targets in the centre and north-western districts of the city. Three separate teams, made up of three men each, near-simultaneously attacked the Stade de France, Parisien cafés and restaurants, and the Bataclan Theatre, using suicide vests and assault rifles. The attackers, who were led by ISIL fighter Abdelhamid Abaoud, killed 130 people in total, including 89 at the Bataclan where they took hostages before engaging in a stand-off with the police. Another 368 people were injured, 99

[4] "Belgian anti-terror raid in Verviers leaves two dead", *BBC*, 16 January 2015, http://www.bbc.co.uk/news/world-europe-30840160, retrieved 10 April 2016.

[5] "Copenhagen Attacks: Danish Police Charge Two Men", *The Guardian*, 16 February 2015, http://www.theguardian.com/world/2015/feb/16/copenhagen-attacks-danish-police-charge-two-men, retrieved 10 April 2016.

[6] "Islamic extremist shot dead in Berlin after stabbing police officer", *The Independent*, 17 September 2015 http://www.independent.co.uk/news/world/europe/berlin-terrorist-attack-police-stabbed-islamic-extremist-10506370.html, retrieved 10 April 2016.

seriously. Seven of the 11 assailants died in the assault – for which ISIL claimed responsibility – many by detonating suicide vests.

The attacks were notable for their complexity, co-ordination, and brutality, including tactics developed to mitigate the response of CT teams. For example, French court documents revealed that in the Bataclan siege well-trained gunmen were positioned to kill fleeing civilians and defend the building from French CT teams. The assailants used disposable mobile phones and those taken from their victims to communicate, and also used encrypted computers and simple written notes to send messages to avoid detection before and during the attacks. The successful use of suicide vests containing the highly unstable TATP explosive made from over-the-counter items also indicated a marked increase in bomb-making capability. The co-ordinated assaults were conducted by at least 11 men of Arab descent, some of whom had fought in Syria, where they gained considerable tactical experience. As such, the Paris attacks marked a significant escalation in the capabilities, intent, and attack methodology of ISIL-related terrorist cells in Europe.[7] Indeed, Michael Leiter, former director of the United States' National Counterterrorism Center, said the attacks demonstrated a sophistication not seen in a city attack since the 2008 Mumbai attacks, and would change how the West regards the threat.[8]

The Paris attacks also revealed strong links between jihadists in Belgium and Syria. Abaoud, who had escaped to Syria after being implicated in the Thalys attack, was killed in a stand-off with police in Paris on 18 November. The leader of the cells, as well as the main planner, Abaoud had been responsible for recruiting the Paris attack teams, including the Abdeslam brothers. Indeed, as investigations proceeded, the link between the attacks and the Mollenbeek district of Brussels – from which the Abdeslams and other attackers hailed – grew, with evidence emerging that weapons bought in Brussels had been transported into Paris and that Salah Abdesalam had also been waved through a Belgian police checkpoint hours after the Paris attacks. He also evaded arrest until 18 March 2016 with the help of some members of the Mollenbeek community, highlighting the Belgian police's lack of sources among the community. Moreover, Salah had criminal links and had been quickly radicalised, traits that were to become increasingly common in future attacks.

2.2. The Brussels Attacks

In the wake of the Paris attacks there were numerous other security scares, but on the morning of 22 March 2016 – likely prompted by the arrest of Salah Abdeslam in Mollenbeek four days previously – three coordinated suicide bomb and gun attacks occurred in Belgium: two at Brussels Zaventum Airport, and one at Maalbeek metro station in central Brussels. Thirty two victims and three suicide bombers were killed in the attacks, while 316 people were injured, 62 critically. ISIL again claimed responsibility. Two Belgian-Moroccan brothers, the El-Bakraouis, and another Moroccan attacker, Najim Laachraoui, detonated suicide vests. The El-Bakrouis were serious Mollenbeek-based criminals well-known to Belgian police. Khalid was also the subject of an international arrest warrant in relation to terrorism, while Laachraoui had previously travelled to Syria and is suspected of being the bomb maker for the Paris and Brussels attacks. Another attacker is on the run, supplying further evidence from the Abdeslam case that a network within France and Belgium are supporting these cells. Indeed, on 24 March French police arrested another ISIL operative, in a north-western suburb of Paris after they unveiled a plot that was in its advanced stages and planned to detonate an "unprecedented" amount of explosives. The plotter is believed to have travelled to Syria in 2014 and 2015, had links with Abaoud, and made several trips between France, Belgium and the Netherlands.

[7] "How ISIS Built the Machinery of Terror under Europe's Gaze", *The New York Times*, 29 March 2016 http://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html, retrieved 6 April 2016.

[8] "Responsibility for Paris Terror Attacks Remains Unclear", *NBC News*, retrieved 14 November 2015.

He was previously known to the French police but not thought to be a terrorist. Two Algerians linked to the plot were detained in Brussels and there were several arrests in Rotterdam, including a Frenchman. All men are believed to be linked to ISIL's external operations wing that planned the Paris, Brussels and the foiled Paris attacks, and which was led by Abaoud. On 10 April, another cell member, was arrested along with five others in Brussels.[9]

ISIL attacks since Brussels appear to indicate a move back toward simpler tactics perpetrated by seemingly lone actors but often enabled by a supporting network. This may be in response to increasing pressure from security services, and in all these attacks the perpetrators were killed by CT forces or had killed themselves. On 10 May one civilian was killed and three wounded in an ISIL-related stabbing attack in Munich, while on 13 June a Parisian police officer and his wife were stabbed to death at their home in Magnanville by a man who had pledged allegiance to ISIL. Prosecutor François Molins said the attacker, appeared to be acting on a recent general order from ISIL commander Abu Bakr al-Baghdadi to "kill miscreants at home with their families".[10] The assailant had been convicted of terrorism in 2013 and placed under surveillance after his release but this ended in late 2015. Two other men were charged with supporting his attack. Just over a month later, 84 people were killed and 308 injured – 53 critically – in the 14 July Nice attacks in which a Tunisian man, Mohamed Lahouaiej-Bouhlel, drove a truck over crowds celebrating Bastille Day on the Promenade des Anglais. ISIL later claimed responsibility for the attack, which Molins said had been planned for months and had help from seven accomplices who were arrested.[11] Lahouaiej-Bouhlel was known to French police for prior criminal offences, but was not registered as a Fiche 'S' and he was not known by French or Tunisian authorities to have links to terrorist organisations.[12] Authorities believe Lahouaiej-Bouhlel radicalised quickly shortly before the attack with Molins stating he had a "clear, recent interest in the radical jihadist movement".[13] Lahouaiej-Bouhlel was also known to have psychiatric problems, characteristic that has increasingly been found in some attackers. On 18 July a 17 year-old alleged Afghan asylum seeker attacked passengers on a train with an axe and a knife in Würzburg, Germany wounding five people. Videos later emerged of the teenager pledging allegiance to ISIL. Six days later, a Syrian refugee blew himself up outside a festival in Ansbach, Germany, wounding 14 people. He had also pledged allegiance to ISIL and had a history of psychiatric problems.[14] Similarly, a suspected cell that was shut down in Germany may have had ties with the Netherlands. Two days later, an Algerian-born 19 year-old and French-born 19 year-old attacked a church service in Saint-Étienne-du-Rouvray, Normandy, with a handgun, knives and fake explosive belts, killing a priest and wounding another civilian. Both of the attackers were known to the police, with one having been convicted of terrorism offences in 2015 and sentenced to prison, where he radicalised further.

While the worst of the attacks in the last 24 months have been concentrated in France, Belgium, and more recently Germany – indicating the major problems these nations are facing – other European states are not immune. For example, in November 2015 the then British Prime Minister David Cameron stated that seven major plots had been disrupted by British intelligence that year,[15] a number that has increased since then. Indeed, unfortunately it is now a matter of when, not if, further

[9] "Belgium attacks: Mohamed Abrini 'admits being man in the hat", *BBC*, 9 April 2016, http://www.bbc.co.uk/news/world-europe-36005709, retrieved 10 April 2016.

[10] "French jihadist police killer 'obeyed Islamic State order", *BBC*, 14 June 2016, http://www.bbc.co.uk/news/world-europe-36530710, retrieved 2 August 2016.

[11] "Nice attack: Prosecutor says suspect had accomplices", *BBC*, 21 July 2016 http://wayback.archive.org/web/20160721181557/http://www.bbc.co.uk/news/world-europe-36859312, retrieved 2 August 2016.

[12] "France Says Truck Attacker Was Tunisia Native With Record of Petty Crime", *The New York Times*, 15 July 2016 http://www.nytimes.com/2016/07/16/world/europe/attack-nice-bastille-day.html?_r=0, retrieved 2 August 2016.

[13] Nice killer Mohamed Lahouaiej Bouhlel 'only started going to mosque this April", *The Sydney Morning Herald*, 17 July 2016 http://www.smh.com.au/world/nice-killer-mohamed-lahouaiej-bouhlel-only-started-going-to-mosque-this-april-20160717-gq7esi.html, retrieved 2 August 2016.

[14] "Ansbach suicide bomber confirms Isis loyalty in video", *The Local*, 25 July 2016, http://www.thelocal.de/20160725/ansbach-suicide-bomber-confirms-isis-link-in-video, retrieved 2 August 2016.

[15] "UK has thwarted seven Isis plots in a year, says David Cameron", *The Guardian*, 16 November 2015 http://www.theguardian.com/politics/2015/nov/16/uk-thwarts-seven-isis-plots-in-a-year-says-david-cameron, retrieved 10 April 2016.

ISIL-inspired attacks take place on European soil. These may be relatively minor attacks, or the more coordinated and prolific attacks of Paris and Brussels, and indeed the simpler mass casualty attack as seen in Nice. A very rough estimate based on data since May 2014 indicates that if you are a member of the public in France or Belgium, you now have a greater than 1/10,000 chance of being killed or wounded in an ISIL attack in the next two years. This is obviously significantly higher for urban residents, commuters, and certain groups, such as Jewish communities. Moreover, it marks a vast increase in the chances of death or injury from terrorism since the end of 2004. Unfortunately, it appears this trend is likely to continue as evidence suggests that ISIL are actively seeking to establish networks of hardened fighters within Europe, with one former ISIL operative warning his interlocutors from France's intelligence service after his arrest "it's like a [European terrorist] factory out there [in Syria]. They are doing everything possible to strike France, or else Europe."[16] At present, records from France's domestic intelligence agency show at least 21 fighters trained by ISIL in Syria are known to have been dispatched back to Europe with the intention of causing mass murder. Records from France's domestic intelligence agency show.[17] Other reports put this number as high as 400.[18]

However, the Salafist jihadist threat to the transatlantic space is not confined to the European continent. The January 2013 In Amenas attack in Algeria, conducted by a group with links to al-Qa'ida, killed at least 39, while, in June 2015, 37 European citizens – the vast majority British – were killed in a gun attack by Seifeddine Yacoubi at a beach resort in Sousse, Tunisia. Yacoubi had pledged allegiance to ISIL and is understood to have received operational support from others. The downing of a Russian civilian aircraft over the Sinai in October 2015, killing 224, and an ISIL attack on Istanbul airport in June 2016 that killed 45 civilians, further highlight the transnational nature of the threat.

For its part, North America has also experienced increasing numbers of jihadist terrorist attacks. The April 2013 Boston Marathon bombings killed four and wounded over 280 civilians, while the July 2015 Chattanooga attack killed five servicemen and left another three injured. Both attacks were carried out by young Muslim men who were US residents, and the Chattanooga attacker had a history of mental illness and drug abuse. On 2 December 2015 in San Bernardino, California two extremists killed 14 people and wounded 22 at the Inland Regional Centre. After the attackers – Siyad Farook, a US citizen of Pakistani origin, and his Pakistani wife, Tashfeen Malik – were subsequently killed by police, it became clear neither had a criminal record, and neither was on Terrorist Screening Database lists. They had also self-radicalised, pledged allegiance to ISIL and received the support of an accomplice. On 6 June 2016, the worst mass casualty terrorist attack in the US since 9/11 took place at a gay club in Orlando, Florida killing 49 and wounding 53 others. The perpetrator, Omar Mateen, was a US citizen of Afghan extraction held extremist Islamist views and said that the attack came in revenge for the killing of an ISIL member in Iraq the week before. Meanwhile, on 10 August, Canadian police received a tip-off from the FBI that a young radicalised Canadian citizen was about to conduct an attack in Ontario. The attacker was killed by police after he detonated a rudimentary device, and although he was known to the Canadian authorities as an ISIL supporter, his intentions only became known after he uploaded a martyrdom video.

ISIL's successful attacks, and the disruption of other terror plots in Europe and North America since, indicate that the threat to Europe and North America from Jihadi terrorists is not only rising, but is also highly dynamic and evolving rapidly. Moreover, the tempo and scope of ISIL cells operations has revealed a mismatch between them and some European intelligence and police services' ability

[16] "How ISIS Built the Machinery of Terror under Europe's Gaze", *The New York Times*, 29 March 2016 http://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html, retrieved 6 April 2016.

[17] Ibid.

[18] "ISIL have 400 fighters trained to target Europe", *Euronews*, 24 March 2016 http://www.euronews.com/2016/03/24/isil-have-400-fighters-trained-to-target-europe/, retrieved 10 April 2016.

to prevent attacks, rather than simply "react to explosions."[19] Finally, al-Qa'ida and other jihadist groups should not be written off. Globally speaking, it is ISIL that currently holds the greatest appeal for active and aspiring jihadists. It is emblematic of this new power balance and the rivalry between the two that none of the official branches of al-Qa'ida have joined ISIL. However, like ISIL, units belonging to al-Qa'ida also retain the intention and capability to strike at targets in Europe. They remain a major threat in some regions and may enjoy a resurgence as ISIL comes under increasing pressure. The multitude of terrorist groups that seek to do Europe and North America harm therefore provides another motivating factor for better CT cooperation. Some of the wider problems in the transatlantic security architecture are identified below.

2.3. Common Denominators

Today's terrorists are evolving rapidly. According to a former senior US intelligence policymaker, terrorists are different today from the generation that executed the 9/11 attacks. Then, terrorists were subject to "quality control", usually attended training camps abroad before being sent to conduct specific attacks, and terrorist organisations were hierarchical, enabling the intelligence services to engage traditional intelligence capabilities against them. However, the more recent terrorism outlined above often has its origins in criminal networks and is often perpetrated by known criminals. Both terrorists and "criminals" know no boundaries. They can transit international borders with relative ease thanks to the interaction with criminals who can provide fraudulent documents; they can procure weapons "in country" by simply paying the required sum and they can share intelligence and bribe officials thus enabling them to keep ahead of law enforcement. As such, they share experience and expertise across environments, communities, and prisons with a flexibility and agility that law enforcement and security services can only wish for themselves. Thus, our intelligence collection approach needs to appreciate this and adapt. This strengthening relationship between jihadism and criminality is a defining characteristic of the more recent terrorism.

The terrorists of today can therefore be more difficult to find. As one CT expert put it, "these people leave a lot fewer bread crumbs [traces] on the way to terrorism", with the speed of self-radicalisation and use of crude weapons in attacks particularly difficult to detect. Moreover, today's terrorist networks increasingly blend often rapidly self-radicalised Muslims with European citizenship and links to criminal gangs with cell leaders trained in Syria and Iraq, and refugees radicalised on the internet.[20] As one former head of an intelligence agency has stressed, these networks "are small, informal overlapping networks of violent extremists from which small groups may coalesce and emerge at short notice to conduct attacks that vary from the sophisticated [Paris] to the crude [Nice]." Often drawing on the experience of the cell leaders, these networks plan their own operations with minimum operational direction from ISIL central. Moreover, online and physical networks have proven adept at influencing mentally unstable young men to commit terrorist attacks. Indeed, it is increasingly clear that the mental health services need to be better integrated into CT efforts. The internal nature of the threat, the rapidity of self-radicalisation, the professionalism and technological sophistication of some attack cells or the simplicity of others, and their operational flexibility all indicate a growing intent and capability to strike multiple soft targets in European cities, or on crowded tourist beaches, near simultaneously.[21]

Their capability has also changed. Even if seemingly lone actors, attacks are almost always supported by a network of individuals, while the more sophisticated assaults have involved degrees of tactical,

[19] Interview, 15 April 2016.

[20] "Terror alert over Isis plot to put bombs under beach sunloungers", *The Times*, 20 April 2016 http://www.thetimes.co.uk/edition/news/terror-alert-over-isis-plot-to-put-bombs-under-beach-sunloungers-662bm0txs, retrieved 20 April 2016.

[21] "Terror alert over Isis plot to put bombs under beach sunloungers", *The Times*, 20 April 2016 http://www.thetimes.co.uk/edition/news/terror-alert-over-isis-plot-to-put-bombs-under-beach-sunloungers-662bm0txs, retrieved 20 April 2016.

operational and technological proficiency not seen before in Europe. Terrorists are actively learning about CT counter-measures and using ways and means to negate them, for example by using secure apps, encrypted computers, and in the future will probably utilise cyber-attacks and drones as vectors of disruption.

2.4. Time to Adapt

As we reflect on the past, consider the present and seek to predict the future, we can be confident that ISIL's intent and terrorist capabilities are unlikely to diminish in the coming years. According to General John Allen, the former US Special Representative for Countering ISIL, this is being driven to a large degree by the success of the coalition's efforts against ISIL in Iraq and Syria during the past 18 months. ISIL has lost strategic momentum in its core areas during this period. As a result, ISIL command views the European theatre as a second front which it can maximise for propaganda value to reverse its defeats in the Levant. According to Allen, ISIL views the coalition as an "existential threat" and Europe as the battleground for its coming counterattack. This view is supported by ISIL's own documents, media reports citing ISIL members of increasing numbers of European ISIL fighters being ordered home to prepare European missions, and the organisation's establishment of an external operations wing.[22] Furthermore, according to a former head of German external intelligence, the magnitude of terror suspects in Europe is becoming acute, with up to one thousand terror suspects in Germany alone.[23] As ISIL loses ground in its heartland, more foreign fighters could be expected to trickle back home to carry out attacks. While the degree to which this threat will actually materialise is of course debatable given the fact that failing states could offer ISIL further operating space, the group's current emphasis on Europe underscores the urgency of tracking people returning from overseas and countering radicalisation, and is partly a technological issue and partly a policy decision.

Yet this perspective is only just beginning to be understood in Europe, a fact which has led to complacency amongst some intelligence and security services.[24] Faced with this threat, the European continent is now at an inflection point – similar to that in the US after 9/11 – where it has the ability to change course. For Allen, however, Europe's position is unique as it still has the opportunity to adapt its intelligence and law enforcement services' practises and architecture without the massive trauma caused to the US in 2001. The recent attacks have clearly revealed institutional, organisational and functional seams which need addressing to better prevent further attacks. For Allen, the European intelligence architecture is under major pressure and "the enemy is mapping the gaps".[25] Former senior police and CT officials and numerous policymakers across the EU, UK and North America echo such a view and are aware that reform is needed.[26] Perhaps now is the time to do so.

[22] "Islamic State files leak: security fears as dozens of European fighters granted 'leave' to return home", *The Daily Telegraph*, 19 April 2016 http://www.telegraph.co.uk/news/2016/04/20/islamic-state-files-leak-fears-as-dozens-of-european-fighters-gr/, retrieved 20 April.

[23] Panel at GLOBSEC 2016, 17 April 2016.

[24] Ibid.

[25] Interview, 15 April 2016.

[26] Interviews, 15-16 April 2016, "Better Border Control", *The Daily Telegraph*, 19 April 2016 http://www.telegraph.co.uk/opinion/2016/04/19/letters-outside-the-eu-britain-would-be-free-to-spend-its-money/, retrieved 20 April 2016.

3. Current Intelligence and Law Enforcement Architecture

The following section discusses the key pillars of the European intelligence and law enforcement architecture and its liaison capacity. It recognises that both intelligence and law enforcement are critical for effective CT, especially today when lines between criminals and terrorists are increasingly blurred. Some national intelligence and law enforcement agencies need to adapt to this new type of terrorist, need to be trained in who to look for, where to look for them, and what the most effective ways of looking for them are.[27]

3.1. European Intelligence Architecture

The continent's intelligence capacity firmly rests with national states. This is problematic as, in short, many nations in the EU have integrated their borders without any integration or sufficient cooperation among their intelligence services. While we are not advocating the complete integration of the latter, as a result, in the EU, each MS is arguably now only as strong as its weakest link.[28] Hence, in the context of CT intelligence, liaison is increasingly important. Today, aside from bilateral relationships between individual intelligence liaison in Europe and the transatlantic space is conducted through a number of informal cooperation arrangements, including the platform of the CTG, the G6, while some joint intelligence bodies have also been established within the EU.

Intelligence liaison within the EU have been a process of top-down, incremental change. It began approximately 15 years ago with shared diplomatic reports, later evolved into sharing selected intelligence assessments, and, most recently, has started producing joint analysis. Although the Union's development of intelligence liaison has been substantial, it largely focuses on strategic intelligence, leaving the operational and tactical levels to its MS.[29] Moreover, it lacks its own substantial intelligence collection capabilities.[30] The EU's joint CT and intelligence architecture either falls under the High Representative (HR) of the EU for Foreign Affairs and the European External Action Services (EEAS), which houses the EU Intelligence Analysis Centre (INTCEN),[31] its military intelligence counterpart INTDIR and SATCEN, the EU Satellite Centre.[32] The European Council is home to the EU's Counter-Terrorism Coordinator, who lacks executive powers but is the EU's go-to figure on issues of counterintelligence,[33] and several working groups on terrorism.[34] Finally, other – largely law enforcement – bodies discussed in detail below contribute to the CT cause: Europol, Frontex and Eurojust.[35]

At the informal level, the CdB is the best known intelligence-sharing mechanism in Europe, but other groups such as the G6 and Prum Convention also discuss internal intelligence matters. Established

[27] Roundtable 15 April 2016.

[28] Ibid.

[29] Ibid.

[30] With the exception of SATCEN, which does collect some of its own IMINT, but mostly via MS' technology.

[31] "EU INTCEN", *Europa.eu*, http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf, retrieved 22 March 2016.

[32] "The Centre", *European Union Satellite Centre*, https://www.satcen.europa.eu/centre.php?menu=1, retrieved 24 March 2016; "European Union Satellite Centre (Torrejón)", *EEAS*, http://eeas.europa.eu/csdp/structures-instruments-agencies/eu-agencies-on-csdp/eu-satellite-centre/index_en.htm, retrieved 24 March 2016.

[33] "Counter-Terrorism Coordinator", *European Council*, http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/, retrieved 24 March 2016.

[34] "Working Party on Terrorism (TWP)", *European Council*, http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-terrorism/, retrieved 28 March 2016.

[35] More on the EU's working groups and organisations dealing with CT and/or intelligence see: Fägersten, B. "Intelligence and decision-making within the Common Foreign and Security Policy", *Sieps – Swedish Institute for European Policy Studies*, October 2015 http://www.sieps.se/sites/default/files/2015_22epa_eng.pdf, retrieved 20 March 2016; Fägersten, B. (2014), "European Intelligence Cooperation". In Duyvesteyn, I. de Jong, B. & van Reijn, J. (eds.), The Future of Intelligence - Challenges in the 21st century, London: Routledge.

in 1971, the CdB consists of the heads of EU MS internal intelligence services, and those of Norway and Switzerland. It is functionally divided into working groups on domestic terrorism, cyber security, and counter-espionage. Although there are no official connections to the EU, the rotating presidency of the Club is synchronised with that of the EU and some of its threat assessments are made available to high level committees of the EU. Criteria have also been set for the CdB's new MS in order that they meet the operational security requirements of the Club.

The nature of intelligence exchanged within the CdB framework has traditionally been strategic and hence, as one interviewee put it, "it is more like a gentlemen's club or a think tank".[36] However, following 9/11, a branch of the CdB, the Counter-Terrorism Group (CTG) was established to deal specifically with terrorism and to provide a forum for collaboration within and outside the group on major CT issues. Set up to focus on Islamic extremist terrorism, it meets regularly to facilitate operational liaison among its members and is also believed to generate threat assessments which are passed on to EU policymakers."[37] Moreover, within the CTG framework, MS in cooperation with US envoys seconded to the Group produce common threat assessments that are also shared with some EU committees.[38] Although there is no formalised link between the two, a CTG team is seconded to the EU's intelligence analysis centre, INTCEN, in Brussels.[39]

In the wake of the recent ISIL attacks, the CTG is increasingly being used on a more regular basis to address some of the issues identified by the evolving jihadist threat. Hosted by the Dutch domestic intelligence and security service, the AIVD, we understand representatives from its MS are now meeting on a weekly basis. It also recently established its own database, the effectiveness of which is yet to be determined. While the CdB does have some liaison links with the EU's main intelligence and law enforcement hubs, INTCEN and Europol, the CdB has traditionally been reluctant to share intelligence with these bodies. Liaison could and should be much stronger; and one starting point elaborated on below should be a Europol-CdB hit-no-hit database search capability.

3.2. European Law Enforcement Architecture

For much of the past two decades, Europol has been the most prominent pan-European institution in terms of law enforcement liaison. The EU's centralised law-enforcement body began operations in 1999, predominantly to facilitate joint analysis and exchange of criminal intelligence, including terrorism, between all EU MS. To date it has had sustained success in countering organised and cyber-crime, but some important MS are more reluctant to share CT intelligence.[40] Without its own collection capabilities (barring the Internet Referral Unit discussed below) Europol collects, stores, processes, analyses and exchanges information and intelligence provided by MS and cooperation partners, notifying MS when it has "information concerning them and of any connections identified between criminal offences" and providing "threat assessments, strategic analyses and general situation reports".[41] Using operational data from MS and third partners (international organisations or countries such as the US) as well as open source intelligence, the Secure Information Exchange Network Application (SIENA) enables fully secure information transfer between MS, Europol and other third parties. Europol has some of the strictest information handling codes of EU MS and acts as an EU benchmark in this regard.[42] It also hosts permanent liaison officers from all MS, the

[36] Interview, 15 April 2016.

[37] "Counter Terrorist Group – CTG", *Harvard Law School PILAC*, http://pilac.law.harvard.edu/europe-region-efforts//counter-terrorist-group-ctg, retrieved 5 April 2016.

[38] Walsh, J. (2006) "Intelligence-Sharing in the European Union: Institutions Are Not Enough", *Journal of Common Market Studies*, Vol. 44. No. 3 625-43, http://jamesigoewalsh.com/jcms.pdf, retrieved 5 April 2016.

[39] Fägersten, "Intelligence and decision-making…", Fägersten, "European Intelligence Cooperation", 98.

[40] Interview, 17 August 2016.

[41]"Europol Council Decision (ECD)", *Official Journal of the European Union (OJEU)*, L 121/37 - L 121/66, 15 May 2009 http://jamesigoewalsh.com/jcms.pdf, retrieved 6 August 2016.

[42] Interview, 17 August 2016.

US and other third partners, and since January 2016 it also is responsible for hosting the Financial Intelligence Unit (FIU) system, Europol is therefore functioning well in many respects, but its CT capability remains curtailed by the distrust with which numerous national intelligence agencies view it, predominantly due to its multilateral nature.

In respect to terrorism, in January 2016 the European Counter Terrorism Centre (ECTC) was established at Europol. The establishment of the ECTC highlights that, given the gravity and increased complexity of the threat, for the first time in terms of EU CT policy, there exists increasing political and operational consensus that a cornerstone for cooperation at EU level is required to support national CT efforts. Focused on CT intelligence, it utilises new integrated databases and computer networks to store and exchange data between MS, and partners such as Interpol and Eurojust.[43] It aims to become the EU hub for CT information sharing and analysis, and operational coordination in the event of terror attacks. It builds on existing databases and Europol's past experience of establishing ad hoc teams from it and interested MS to share and operationalise intelligence on specific terrorist groups.[44] The ECTC has four areas of competency; tracking foreign fighters (Europol's Focal Point Travellers Database is the most advanced in Europe on the movement of foreign fighters and in April 2016 it enhanced its cooperation with the FBI); tracking/preventing illegal arms trafficking; tracking terrorist financing under the EU-US Terrorist Finance Tracking Programme (TFTP);[45] while the recently established EU Internet Referral Unit collects and analyses terrorist-related content online and flags it to internet providers. It's "Check the Web" portal enables MS to share information on internet activities of jihadist terrorist groups. The ECTC uses SIENA for secure data exchange and the Europol Information System (EIS) as central criminal information and intelligence database. Security and data ownership control are a key feature of the EIS. The EIS user's right of access to the data stored in the EIS is dependent on the user profile and the restrictions defined by the data owner. Access rights may be limited by the owner of the information on a case by case basis, allowing for a hidden hit mechanism to notify the owner. Against this background, some intelligence services which are designated at MS level to also constitute "competent" authorities under the legal framework of Europol have contributed data on foreign terrorist fighters to the EIS.

While Europol is still developing its CT capabilities, it is having an increasingly effective impact, especially in terms of law enforcement CT issues. Its operational function is also regarded as increasingly strong. In the wake of the Paris and Brussels attacks, "Europol immediately performed cross checks in its databases on the names of the identified perpetrators to look for possible accomplices, produced a significant number of unique financial intelligence leads, monitored extremist propaganda online and offered these and other operational services, including weapons trafficking expertise, to the French and Belgian authorities."[46] Over 3,000 pieces of information were shared with the French alone, and these actions resulted in the generation of new investigative links.[47] As a result of these successes, increasing numbers of MS now trust Europol and are more actively sharing CT police information and intelligence. As police-to-police information sharing goes back at least a century, there is often a good level of trust between forces. However, curtailed by a lack of CT intelligence provided by MS intelligence agencies, Europol's major weakness in this regard is that it works best in the aftermath of an attack. Clearly, progress is being made, but our research revealed that numerous MS' intelligence services remain very reluctant to share their information with Europol. More can and should be done in this regard, especially as the TFEU and the legal framework of Europol do allow information exchange between law enforcement and intelligence services.

[43] "History of Eurojust", Eurojust, http://www.eurojust.europa.eu/about/background/Pages/History.aspx, retrieved 6 April 2016.

[44] "Convention based on Article K.3 of the Treaty on European Union, on the Establishment of a European Police Office (Europol Convention)" https://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/projects/carpo/output_3_-_special_investigative_means/Europol_Convention.pdf, retrieved 10 March 2016.

[45] "Europol Joins Forces with EU FIUs to Fight Terrorist Financing and Money Laundering", *Europol*, 28 January 2016 https://www.europol.europa.eu/content/europol-joins-forces-eu-fius-fight-terrorist-financing-and-money-laundering, retrieved 10 October 2016.

[46] "Europol Review 2014: General Report on Europol Activities", *Europol*
https://www.europol.europa.eu/content/europol-review-2014, retrieved 10 March 2016.

[47] Interview, 17 August 2016.

Beyond Europe, Interpol is also making progress in CT law enforcement. The organisation includes many states in the Gulf and Sahel regions that are particularly relevant to the rising jihadist threat. Primarily, it circulates alerts on terrorists and weapons threats to police forces in its Notices and Diffusion system. Interpol's relatively new Counter-Terrorism Fusion Centre (CTF) investigates the organisational hierarchies, training, financing, methods and motives of terrorist groups. The CTF's activities are global in scope and implemented through a number of regionally focused but interlinked projects. The aim is to improve the exchange of law enforcement information across borders and to enrich law enforcement practises. Interpol also runs a foreign fighter tracking programme, and another to boost border police capability through integrated police databases. Clearly, like Europol, Interpol is making some headway in integrating CT law enforcement capabilities, but also like Europol, our research revealed that many nations' intelligence services remain highly reluctant to share CT intelligence with it.

Finally, some commentators have suggested that NATO would represent a suitable platform for addressing the terrorist threat. This report argues, however, that this is a misconception. NATO's primary concern in the intelligence domain is sharing intelligence to support its military operations. Moreover, it does not have a remit to cover CT inside its MS. For its part, the four major intelligence departments in NATO do not collect any of their own CT intelligence, are under-resourced, primarily focus on military intelligence, and perhaps most importantly, suffer from similar problems as the EU agencies in terms of a lack of trust.[48] Interoperability and standardisation of capabilities remain problematic and overall intelligence sharing in NATO has been described as "a big challenge".[49] Recognising this, NATO MS agreed at the 2016 Warsaw Summit to establish a new Joint Intelligence and Security Division to be led by an Assistant Secretary General for Intelligence and Security. This new Assistant Secretary General "will direct NATO's intelligence and security activities, ensuring better use of existing personnel and resources, while maximizing the efficient use of intelligence provided by Allies."[50] Overall, however, NATO's primary goal is not focused on CT efforts within its MS and outside the military theatres it is engaged in.

[48] Interview, 16 April 2016.

[49] Interview, 16 April 2016.

[50] "NATO Warsaw Summit Communique", 9 July 2016 http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en, retrieved 3 August 2016.

4. CT Intelligence and Law Enforcement Issues

Many key European intelligence and law enforcement figures agree there is a problem. After the Brussels attacks, the EU's Home Affairs Commissioner, Dimitris Avramopoulos stated "There is a shortage of trust between member states… The 'deep state' resists and we must change this attitude. I know it is not easy to start thinking in a more European way, but it is a must."[51] Rob Wainwright, director of Europol, recently stated that: "The fragmented intelligence picture around this dispersed community of suspected terrorists is very challenging for European authorities", while the EU's Counter-Terrorism Coordinator, Gilles de Kerchove, stated, "I do my best to put pressure, to confront them [Member States] with blunt figures, and we are making progress, but not quickly enough."[52] The following section discusses some of the key problems inhibiting the effective work of, and most prominently liaison, between intelligence and law enforcement bodies on the old continent.

4.1. Trust in Transatlantic Intelligence and Law Enforcement Liaison

Bilateral as well as multilateral intelligence and law enforcement structures and organisations are heavily reliant on trust. According to our interviews with practitioners, trust remains a key problem of European intelligence liaison and is also far from guaranteed in CT law enforcement. Moreover, trust issues are not simply a problem of EU MS, but are also present across the transatlantic space, both in respect to international as well as domestic cooperation. Organisational rivalries and distrust remain between the 16 US intelligence, security and law enforcement agencies, despite the progress that the federal and state governments have made. This progress, however, was most chiefly facilitated by the shock of 9/11 as well as the fact that it was comparably easy to integrate due the US' federalised state. Similarly, a fear of competition from growing EU institutions, such as Europol's ECTC, may also be a factor in explaining the reluctance of some intelligence services to cooperate more fully with Europol.

A number of factors impede transnational trust. Since the mid-1990s, there has been a welcome increase in parliamentary and judicial oversight, as well as liaison between national intelligence and law enforcement organisations. Nevertheless, recent attacks have shown that there are wide discrepancies between European states' intelligence as well as law enforcement capabilities and capacities. While Europol is making good progress in integrating European law enforcement, there remain differences between police forces' capabilities. Some of those identified have involved the adequacy of evidence gathering, case management, and prosecution. In respect to intelligence liaison, a number of interviewees have indicated that trust remains an issue between European nations with longer democratic traditions and those that have only recently democratised. The background and divided loyalties of some intelligence leaders, unclear control mechanisms of their intelligence organisations, and the possibility of leaks beyond the European intelligence community have, at times, strained these relationships. There are also often well-founded historical and political reasons for discrepancies between CT legislation and personal data and intelligence sharing.

This inequality impedes the sharing of CT intelligence and personal data, as the more capable states are reluctant to share their "goods" with states with lesser capacity. For example, databases on foreign fighters remain separated and reliant on a core of five main contributing MS services. In terms of signals intelligence (SIGINT), capabilities of transatlantic partners are largely determined by their intelligence architecture, its evolution, size and legislation, with the UK being the most prominent European nation that regularly collects bulk data.

[51] "Brussels attacks: Why Europe missed warning signs", *BBC*, 24 March 2016
http://www.bbc.co.uk/news/blogs-eu-35891078, retrieved 10 April 2016

[52] 'First on CNN: Top U.S. intel official: Europe not taking advantage of terror tracking tools', *CNN*, 7 April 2016
http://edition.cnn.com/2016/04/07/politics/christopher-piehota-us-intel-europe-terror-tracking/index.html, retrieved 10 April 2016.

Moreover, there also needs to be trust that if a specific piece of intelligence is passed on, it is not actioned without the originator's consent, and that the originator's legal framework is considered. One potential issue here is whether European intelligence services can share "live" information on their CT investigations and trust the US not to act unilaterally, especially as the US has a different legal framework allowing it to target some terrorists abroad as it would on a battlefield. Both sides may need to compromise and take a longer-term view in order to build trust.

All of this is closely related to the issue of "security culture". In many organisations, the traditional approach to security has focused on addressing physical and information security issues. Nevertheless, the "people" or cultural element, which is equally important, is often overlooked. As most interviewees agreed, "the actions and attitudes of people can make all the difference". A significant factor affecting how people act is the security culture of the organisation. This can be defined as the styles, approaches and values that the organisation wishes to adopt towards security. It can range from whether employees adhere to a clear desk policy to whether they share sensitive information on social networking sites or with outsiders. In organisations with a strong security culture, employees will tend to think and act in a more security-conscious manner. This helps to reduce risk and vulnerability, which in turn helps protect against reputational damage, business impact and ultimately national security threats. Organisational and security culture are as important as risk management, business continuity and other disciplines and, of course, they pervade the whole organisation with less visibility and less controls.

Over the past decade, transnational trust has further been undermined by the Wikileaks and Edward Snowden revelations, which drew attention to the problem of certain nations "spying on friends". Although the fact that even allies eavesdrop on each other did not come as a surprise to those familiar with the trade, the public uproar and wide publicity these developments received did impact mutual trust. For instance, after Snowden alleged that the US had been spying on German citizens, this led to a temporary but significant damage to the trust between these nations. Concerns about privacy therefore remain strong in some European nations. Nevertheless, there does appear to be a growing recognition in these nations that the evolving terrorist threat requires reappraisal of legislation designed when other threats were perceived as more pressing. This has been helped by the steady spread of intelligence, law enforcement and judicial oversight.

A lack of joint operational information sharing history also exists between some national intelligence agencies and the CTG on the one hand, and Europol on the other, with the former regarding the latter's information security and ability to prevent leaks as suspect, despite the fact that it has some of the most stringent information security systems in place in the EU. While the reserved approach of the CTG to routinely share with Europol does reflect the intelligence services' inherent distrust of multilateral personal data and intelligence sharing platforms, it does also indicate a cultural unwillingness to adapt to changed strategic circumstances. Indeed, a senior intelligence official has estimated that only one-two percent of CT intelligence collected by MS is truly secret and should not be shared with Europol or any other body. Therefore, changing the cultural approach to sharing amongst MS intelligence services and transnational bodies is also sorely needed.

4.2. Domestic Inter-Agency Trust

Trust issues have also had a major effect on domestic cooperation between law enforcement and intelligence agencies. A number of countries within the transatlantic community struggle with domestic dissemination failures. Better integration of information held by the police into the intelligence picture is key, as after attacks it has emerged that often they did in fact hold a number of important "crumbs". Moreover, European terrorism is increasingly a local law enforcement issue, relying on good relations and deep familiarity with local communities to collect actionable human intelligence (HUMINT). Law enforcement is essentially on the frontline of today's CT efforts. Nevertheless, numerous European intelligence, law enforcement, security and legal services have not succeeded in developing a strong sense of a single intelligence and security community, including the relevant law enforcement bodies, to enable joint mission planning, investigations, evidence gathering and where necessary disruption operations. This is a lesson the British had to learn from hard experience of countering attacks in Great Britain during their long Northern Ireland CT campaign, and that the Dutch have also incorporated. In many other nations, services are still functionally divided, curtailed by rivalry, and reportedly under-resourced. They therefore do not share information between services – or with their governments – to the same degree, and can struggle to share information rapidly in order to identify and pre-empt attacks. Moreover, in many countries, law enforcement forces have not traditionally been viewed as central to CT efforts. As a consequence, law enforcement officers have not been tasked to potential problem areas with sufficient urgency and in sufficient numbers in order to help build the community relations that are vital to generating good CT intelligence.

One interesting example of effective best practice in this regard was the British realisation after the 2005 London bombings that its CT effort needed to decentralise from London and move out to the regions, in each case co-located with the police, enabling integrated planning and operations that harnessed the output of all the intelligence agencies. British CT experts argue that this has transformed the effectiveness of domestic CT. Following the recent attacks in France, it is also beginning to recognise the power of an integrated CT approach, which rests on the cooperation between intelligence, security agencies and the police. Moreover, excessive centralisation in Paris has also been recognised as a problem. Although the US intelligence, security and law enforcement agencies have integrated since 9/11, it should be also noted that some functional seams and organisational rivalries remain.

4.3. Operationalisation

Failures and loopholes have also been identified when it comes to operationalising – following through and acting on – “personal data” and “intelligence” received from allies or international law enforcement organisations. Arguably, operationalisation failures have been caused primarily by failures to prioritise information concerning threats, the relatively free movement of people across Europe, and by capacity issues.

4.3.1. Capacity

The capacity problem in respect to operationalisation is noteworthy. With the growing number of radicalised Europeans with known associations to ISIL or other terrorist organisations, European intelligence services are still under resourced, despite recent increases in personnel. As three police or intelligence teams of five-six personnel are usually required for each 24-hour period of surveillance of a person of interest, monitoring suspects is manpower intensive and therefore requires prioritisation. France’s Direction Générale de la Sécurité Intérieure (DGSI) employs roughly 3,300 officers to monitor 20,000 people on the country’s watch list. The Belgian intelligence agency, Surete de L’Etat, has 600 personnel to monitor a suspected 900 terrorists on its territory. In the wake of the Paris attacks its budget was increased by 20 percent to €50 million. Nevertheless, before the Brussels attacks a Belgian intelligence official stated: “We just don’t have the people…we don’t have the infrastructure to properly investigate or monitor hundreds of individuals suspected of terror links…It’s literally an impossible situation.”[53] By comparison, the Dutch have 1800 intelligence and military personnel in total to monitor a larger population, but only a small amount of these are involved in the surveillance of about 40 jihadist suspects. Despite attempts to reform, and help from the US, our research revealed that Belgian intelligence is currently viewed as a “weak link” by other nations’ intelligence services.

[53] “Belgian Authorities Overwhelmed By Terror Investigations”, *Buzzfeed*, 22 March 2016 http://www.buzzfeed.com/mitchprothero/belgian-authorities-overwhelmed-by-terror-investigations#.pszkgBYr5b, retrieved 9 April 2015.

The free movement of people within the EU, combined with arguably porous borders in the south-east and the loopholes in information exchange and intelligence liaison has led to suspects falling off the radar. A number of the Brussels and Paris attackers were considered a threat. Their radicalisation and engagement with ISIL in Syria was known to the authorities, yet they fell off the radar while moving between Western Europe and the Middle East with relative ease. This problem has manifested itself in respect to the recent CT challenges in the following way: an estimated 5,000 European citizens have travelled to join extremist groups like ISIL in Syria and Iraq, but there are 2,786 in one database, 1,473 in another, and 90 percent of the names added recently came from only five EU governments.[54] Although some have suggested that European suspects known to have associations with ISIL should be monitored while in the Middle East, this proposal represents a major challenge as the West's intelligence capacity to track suspects in countries such as Syria and Iraq is limited, and cooperation with some governments in the region controversial.

4.3.2. Privacy and Digital Tools

Another obstacle is some MS' historically-conditioned emphasis on privacy, although there are signs of increasing recognition that a more pragmatic balance needs to be struck between this and the new threat facing EU citizens. Yet, legislation is lagging behind the threat in many nations and those that have introduced new CT legislation do not want their model to be widely adopted in the EU as they fear this may attract too much attention, provoke opposition, and could be judged to be illegal by the European Court of Justice.[55] Powerful digital intelligence and data mining tools are essential for CT, not least to trigger investigations and pre-empt attack planning. But the very power of these tools means that there must be adequate safeguards and oversight to ensure that they cannot be misused; for most nations this means new legislative frameworks need to be considered.

The Director of the US' Terrorist Screening Center, Christopher Piehota, recently commented on the issue of operationalisation. According to Piehota, all European countries cooperate with the US to varying degrees and information sharing has greatly improved in response to the ISIL threat.[56] Nevertheless, he stated that European countries can do more to screen terrorists and take full advantage of tools the US has offered in the fight against terrorism: "It's concerning that our partners don't use all of our data. We provide them with tools. We provide them with support, and I would find it concerning that they don't use these tools to help screen for their own aviation security, maritime security, border screening, visas, things like that for travel." Piehota said that the US shares its watch lists with EU countries, but that EU countries do not systematically utilise it to identify suspected terrorists or screen incoming migrants. Simultaneously, some former senior European policymakers have expressed concerns about sharing "live" information on their CT investigations with the US. They ask: "Can we trust the US not to act on this information unilaterally?"

With its systems of warrants and information sharing databases (Schengen II and the more recently accelerated EU arrest warrants being the most prominent), and the recently passed Passenger Name Record (PNR) legislation, the EU now possesses avenues to physically exchange information on suspects. These resources have, however, thus far predominantly been used to fight organised crime and are yet to be adopted as common ways of CT information-sharing between European and other transatlantic allies. With respect to the newly adopted PNR legislation, it remains to be seen how this data will be used for CT purposes. According to a former member of the post-9/11 administration in the US, PNR data was crucial to the US's large-scale CT effort. This information combined with other intelligence force multiplies capabilities and pinpoints suspects. Nevertheless, contrasting the US, there are so many land and sea entry points into Europe that many who are

[54] Roundtable 15 April 2016.

[55] Interview, 7 March 2016.

[56] First on CNN: Top U.S. intel official: Europe not taking advantage of terror tracking tools", *CNN*, 7 April 2016 http://edition.cnn.com/2016/04/07/politics/christopher-piehota-us-intel-europe-terror-tracking/index.html, retrieved 10 April 2016.

entering are doing so without being identified. Thus, simply sharing PNR data may not prove as effective as it has in the US. The decentralised framework of processing PNR data, as established by the "new EU instrument", also offers certain limitations in terms of the non-uniform way in which data will be processed, stored and exchanged within and between 28 different national arrangements. As such, an opportunity was lost to introduce a more coherent, centralised architecture in the EU.

4.3.3. Speed

Although technically possible, sharing among EU and transatlantic allies can be slow and restricted, which represents another obstacle to operationalisation. One possible explanation for this is the EU MS' varied ability to respond effectively and in a coordinated fashion to operational intelligence. Given ISIL's tempo of operations, in the current architecture, by the time a piece of intelligence had been cleared for sharing, then shared bilaterally, it can be too late. Unlike in the Cold War, in which most of Europe's intelligence services were designed to operate, the required tempo of information fusion and speed of reaction is much higher today. In the Cold War, intelligence was separate from reaction; now it goes out of date in hours. The speed of reaction, in terms of intelligence and CT response, is now critical to saving lives. Interoperability is therefore key. Moreover, states prefer to share a piece of intelligence multiple times bilaterally than in one single multilateral release, leading to the situation where those excluded could have vital pieces of relevant information but are not aware of it. Hence, any effective solution to the problem of sharing will not be based on an equal share for all. The core of any future transatlantic intelligence liaison will therefore be limited numbers and common standards that are conducive to increasing common trust. A more positive outlook is emerging at Europol, however, as it develops into an increasingly effective transatlantic information sharing hub, involving EU Member States and (to date) 12 federal agencies.

4.3.4. Political Will and Decision Making

Political will and decision makers' understanding of CT challenges are fundamental to the effective operationalisation of personal data and intelligence. Following 9/11, US practitioners and policymakers tasked with CT briefed the President every day on major threats, as did their British counterparts. These regular updates made the leaders focus on the issues of security and terrorism more, because "knowing" made them feel responsible.[57] Former high-ranking intelligence policymakers interviewed for this report agree that regular briefings of politicians on CT challenges are of essence. They, however, advocate for a less frequent, albeit regular, briefing schedule outside of time of major crisis as that of 9/11 or the 2005 London bombings. The responsibility of policymakers' to understand the nature of threat and the work of their intelligence apparatus is crucial to the latter's work. For instance, according to reports, Belgium had asked for an increased intelligence budget after 9/11 but this was rejected. In the Netherlands about one-third of the budget for the General Security and Intelligence service was cut in 2012. In both countries, this was the result of a disengaged political culture.[58]

To reinvigorate the political ownership of the responsibility to combat terrorism, citizens can use the fact that the Lisbon Treaty states security is the responsibility of MS to pressure states which represent "the weakest link". This national responsibility which extends to intelligence can now be used to point at MS and tell them that they need to reform their practises, legislation, and engage in training to adopt new 21st century standards. Weaker nations need to be encouraged at the political level and to see greater liaison as equated to shared common borders within the EU, and greater transatlantic cooperation. According to a ministry of interior representative of an EU MS, some European countries will simply not share or improve their capabilities unless they are forced to by external political pressure.

[57] Roundtable, 15 April 2016.

[58] Roundtable, 15 April 2016.

4.3.5. The Politics of CT Intelligence Reform

Moreover, there are discrepancies in European nations' attitude towards CT reforms, which would encompass changes within the realm of intelligence as well as law enforcement. A senior European intelligence official recently stated that while some nations have pushed for the EU to take the lead on the systematic reform of intelligence operations, and in particular intelligence liaison, they have had their "knuckles wrapped" by another major European nation unhappy about sharing CT intelligence in a multilateral environment.[59] This has forced a re-assessment of what is currently politically possible in this regard, and the dilution of current proposals. There are similar political divides within the EU itself. The EU Commission, led by President Jean-Claude Junker, is driving forward with plans to better integrate EU intelligence liaison, as evidenced by its recent information sharing roadmap and Junker's September speech calling closer EU cooperation on defence and security. However, the EU Council, which directly represents MS governments and their interior ministries, remains far more circumspect about such proposals. As such, there are political fault lines preventing better integration both between EU MS and within the EU itself.

4.3.6. Transnational Threat and Risk Assessment Deficit

Finally, European and transatlantic intelligence and law enforcement agencies need to know what they are up against, in the short, medium, as well as the long term. A transnational CT strategic threat and risk assessment is necessary for identifying gaps and problems of how agencies operate and cooperate. These assessments are critical for prioritising threats, generating effective CT strategies, and focusing effort and allocating resources to fulfil these strategies. Remarkably, according to a senior European law enforcement official, in the midst of the current surge in terrorist activity, the EU has not invested in producing such an assessment. This seems to be largely caused by the lack of coordination at the top of the EU. To date, it is unclear whether such assessments have been considered or commissioned by other existing international networks, such as the CdB's CT Group.

[59] Interview, 17 August 2016.

5. Recommended Reforms

Intelligence challenges related to CT are profuse and some are not easy to tackle within the short-midterm timeframe. Hence, in the following section, this report discusses a number of existing intelligence models which have been successful, could be used to tackle CT challenges, and be exported from the national to the transnational level. Moreover, it also details some of the ways these models could be used to fight the current wave of terrorism in the transatlantic space.

This paper takes the position that the reform of current intelligence architecture and practises from the bottom-up is the most pragmatic approach. While we are aware of the work being undertaken by the EU Commission on its Information Exchange Roadmap of 6 June 2016, and by Europol, to better integrate CT efforts, a number of complementary suggestions for practical improvement are examined below.[60] Within this process the distinction should be made between the three forms of intelligence: strategic (which is less sensitive and routinely shared); operational (more sensitive and therefore less frequently shared); and tactical (which is the most sensitive and currently mainly shared between Five Eyes Plus on a regular basis, and with others in the aftermath of an incident or on an ad hoc basis). While appreciating that there are other – strategic – seams in the current European and transatlantic intelligence architecture crucial to long term security, the following section focuses on selected short term CT tactical and operational solutions to the problems within the realm of intelligence and law enforcement identified by this report.

In order to react with the required speed and coherence to mitigate the current terrorist threat, the GIRI Initiative proposes a set of practical improvements. Our aim is to uniformly raise capabilities in MS and beyond, and to promote more efficient analysis and sharing. These recommendations are designed to treat some of the key problems identified above. They are predominantly based on existing models proven to be effective, but also present novel solutions, especially in terms of CT intelligence liaison.

5.1. Existing Models

Today, many – but not all – European nations have joint CT analysis centres. One of the oldest such centres is the United Kingdom's Joint Terrorism Analysis Centre (JTAC). Established in 2003 and housed in the MI5's headquarters, JTAC's role is to analyse and assess all intelligence relevant to the country's CT efforts – domestically as well as abroad. In addition to setting threat levels, JTAC produces substantive analysis on various terrorist networks and their capabilities. Its strength lies in its capacity to integrate CT expertise from 16 relevant government departments, including law enforcement and the country's intelligence agencies, to jointly analyse and process CT-relevant information. The Centre's head reports to the Director General of MI5 who reports on JTAC's activities to the government's Joint Intelligence Committee (JIC). Its efficiency and quality of its assessments are monitored by an official Oversight Board, chaired by the Cabinet Office.[61] Similarly, when Scotland created its "Crime Campus", six agencies co-located, collaborated and coordinated their intelligence, resources and training which led to significant improvements across Scotland. Very soon the number of agencies grew to 16 as those outside the "club" saw the obvious benefits of joining; individually they were good but collectively they were even more effective.

Another such model in place today is the Dutch joint intelligence analysis centre known as The Netherlands Counterterrorism Information Box, or CT Infobox. Established after the 2004 Madrid bombings, the CT Infobox is a fusion centre housing elements of ten Dutch agencies, including the

[60] "Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area", *Council of the European Union*, 6 June 2016 http://statewatch.org/news/2016/jun/eu-council-info-exchange-interoperability-roadmap-9368-rev1-6-6-16.pdf, retrieved 11 October 2016.

[61] Joint Terrorism Analysis Centre", https://www.mi5.gov.uk/joint-terrorism-analysis-centre, retrieved 11 October 2016.

prosecutor's office, police, security and immigration, intelligence, financial crime, and, innovatively, social welfare services. All CT Infobox personnel work on the same corridor, are subject to the same level of screening as well as the same security regime. The CT Infobox is not a direct information exchange platform between participating bodies, meaning that information shared here does not leave the CT Infobox and flow back to the individual services' headquarters. In fact, it could rather be described as a safe space, or a "closed box", which enables the participating parties to share information in-house, conduct joint-multidisciplinary analysis of suspects and subsequently formulate joint recommendations on how a particular suspect should be dealt with. These recommendations are passed onto the relevant organisations and they are 'advised' to act on it and speak with other agencies on certain cases. The Infobox monitors whether its recommendations are implemented and if they are not, it is ready to consider alternative approaches. Crucially, when putting suspects on its list, it follows so-called "placement criteria" and if, for instance over time, the subject ceases to fulfil these, they are "de-listed" from the CT Infobox's list. A March 2015 assessment of the CT Infobox's success found the mechanism particularly helpful in terms of its ability to: processes data quickly and efficiently; and conduct comprehensive assessments, based on various viewpoints and expertise, of information. These are all areas identified above as problematic within the European and transatlantic CT intelligence context.[62]

The CT Infobox is led by the Head of the CT Infobox. Its Coordinating Board, which consists of one board-level representative from each of the participating bodies, is in charge of strategy, policy issues and oversight.[63] Its work is overseen by a three-person steering board that reports on an annual basis, with the CT Infobox's head reporting to it on a quarterly basis. The steering board acts as a watchdog especially in terms of privacy legislation, although in reality the presence of the prosecutor's office in the Infobox, and the experience of the Infobox's leader, means they rarely have to take action in this regard.

In practice, the process is the following. As the CT Infobox does not have a central database, each representative to the Infobox manages and controls information from his/her mother service. They also remain the data owner for all information placed in the CT Infobox. Hence, when an investigation begins, each representative looks for relevant information on the subject within their home systems. Relevant information obtained from these home channels is then put into an "in-house system", available to all Box personnel to access as well as update. This pooling of relevant information into one system helps create a coherent picture of the subject, carry out a comprehensive risk assessment, and propose adequate actions aimed at mitigating the threat. Data in the system can contain information on sources, or not, according to the data owner's discretion. Crucially, if any agency wants to extract information from the Infobox it must ask the data owner's permission. Although it has never occurred, any transgression would result in the offender being removed from the Infobox. According to the 2015 assessment, "the chosen system of communication reveals possible responses which might not have been devised had the underlying information only been viewed from a single perspective…creative thinking will result in novel forms of intervention."[64] Notably, having been in existence for 12 years, and with staff serving four-year terms at a time, the CT Infobox has developed such high levels of inter-agency trust that a single permanent database using the information in the Infobox is now in operation, allowing users to track historical records of relevant cases. However, at present the CT Infobox itself has no formal liaison with Europol or the CdB, as this is usually the responsibility of each service.

At the national level, another successful CT hub has been Scotland's Strategic Multi-Agency Response Team (SMART). SMART is a multiagency forum for the mutual exchange of intelligence leading to the creation of a number of products, varying from strategic multi-agency threat and

[62] de Poot, C.J. and Flight, S. (2015), *Ruimte om te delen. De CT Infobox tien jaar in werking*, The Hague, Ministerie van Veiligheid en Justitie, p. 76-85.

[63] Ibid.

[64] Ibid.

risk assessments to operational “Prevent Professional Concerns”, where an individual of concern is discussed and an action plan formulated and led by the most appropriate agency. In addition, a Current, Emerging and Residual Threat Assessment was completed for each of the 32 Local Authority Areas informing them of the transnational, national, and more importantly, local threats and risks. This allowed the authorities to brief and educate their employees as to what to look for, allowing hundreds of thousands of people to know and understand the threats in their communities. This in turn allowed them to identify, harvest and disseminate intelligence/information which ultimately monitored community tensions and matters out of the ordinary. It is accepted that not all this will develop into CT intelligence but it served to deliver confidence that the state recognised that communities’ health is important and that it wants to identify vulnerabilities prior to exploitation by those who would seek to take advantage.

Could these models work at the transnational level? According to an assessment of the CT Infobox, one of the most prominent reasons for these models’ efficiency is the common understanding of the severity of the terrorist threat among all parties and their willingness to contribute to this common goal even if this does not result in new gains for each participating service. While quality of data, standardisation and professional capacity would all pose initial issues in adapting a CT Infobox to the transnational level, its basic principles of data ownership, separated systems, and oversight, which are all conducive to slowly developing trust, seem especially important. Crucially, it allows access to more relevant information, and the penalty for transgressions is removal, with its own political consequences. Moreover, ideally, a transnational CT Infobox would need a hit-no-hit single search interface with both Europol and CdB databases.

5.2. Recommendation 1: CORE TRANSATLANTIC CT HUB AND TASK FORCES

The Initiative does not propose the establishment of new institutions. Yet, it does advocate for creating/strengthening existing networks and task forces which would enable better CT coordination through a perception of shared threat and the development of mutual trust.

5.2.1. Core Transatlantic CT Hub

We recognise that “the best of the bilateral relationships work very well; the worst don’t work at all.”[65] The first proposal calls for the establishment of a more permanent Core Transatlantic Counter-Terrorism Hub, initially consisting of a core group of nations which have high intelligence and law enforcement capabilities and are willing to share multilaterally on a routine basis.[66] This would initially need to be based around nations with high degrees of trust and the political appetite to share large amounts of sensitive information. Unlike the so-called “Alliance Base”, a publically unacknowledged Western Counterterrorist Intelligence Centre (CTIC) based in Paris operating between 2002 and 2009, the CT Hub’s emphasis would be on CT liaison and setting common standards.

Following the successful models discussed above, the proposed Core CT Hub would represent the first step towards a secure space to link existing national CT centres from Europe and North America. In the EU, the ECTC at Europol and the CTG should be involved. Moreover, the founding members would develop common definitions/procedures for alerting and threat warning, secrecy and capability requirements. The success of this core, and the access to information within it, would encourage less capable and/or willing nations to improve their services in order to join. For example, a US-UK CT hub could form the nuclei around which other nations such as France, Germany, the

[65] Comments, former intelligence agency chief, 3 October 2016.

[66] Interview, 16 April 2016.

Netherlands and Italy could join if they commit to appropriate investment and standards. While this process is likely to be gradual, it would potentially create political pressure and incentives for better intelligence capabilities across Europe and the transatlantic space.

In addition to sharing intelligence, this Core CT Hub could serve as a hub for more intense shared analytic efforts. For those transatlantic partners who are yet to establish joint CT centres or are in need of reforming their existing CT frameworks, a number of models could serve as a template. Ultimately, however, nations must choose the model that suits them best.

Finally, a joint transatlantic CT Strategic Threat and Risk Assessment (STRA) could be created based on the fusion of intelligence from invested member states. Such an assessment would assist in informing politicians and practitioners of the collective knowns and, in so doing, identify the most pressing gaps and problems. Once the "knowns" as well as the "unknowns" have been identified and understood, the CT Hub will be equipped to create and push their members to adopt adequate intelligence requirements, to fill those gaps. In essence, the STRA would be a strategic, long term, forward-looking document that identifies, assesses and prioritises the threats, risks and opportunities facing intelligence and law enforcement agencies in the CT domain. It would present and interpret the findings of intelligence/information analysis, set priorities and allow relevant stakeholders in CT Hub member states to understand terrorist trends and how these impact relevant agencies. Such an assessment would also drive the tactical and operational response though multi-agency tasking and coordinating. This, in itself, would continue to enhance trust though operational relationships.

5.2.2. Case-Based Task Forces

On a more operational level, GIRI recommends that Case-Based Task Forces be set up within the Hub, designed to react ad hoc to emerging CT challenges. Such task forces might be set up to address operational issues related to a particular terrorist group, be it al-Qa'ida or ISIL; or an issue, such as radicalisation, terrorist recruitment, to name but a few. Such task forces would promote joint execution of intelligence-led operations as well as the better sharing of personal data, as is currently being done through Europol. Task forces would follow the fusion centre model, and would be based on voluntary entry where MS with specific interests in each case could request to join. The smaller numbers of MS who share the same concerns would be more conducive to trust. Once given the requisite clearance, these functional groups would have the ability to rapidly share multilaterally and be highly connected to the relevant law enforcement and CT agencies in their respective countries. Information would therefore flow both ways and be rapidly shared within the task force. For example, a counter-ISIL group consisting of member states who have opted-in would help centralise responses and, if successful, begin to act as a benchmark for others tackling other intelligence issues and sharing. These task forces could form a joint investigative unit hosted by one of the participating nations.

5.3. Recommendation 2: SINGLE SEARCH INTERFACES

The GIRI Initiative calls for a single search interface to enable real time information exchange that would in turn encourage bilateral co-operation and trust. As discussed previously, many nations are sceptical of multilateral personal data and especially CT intelligence sharing platforms, be it within the EU or beyond. Hence, GIRI proposes a transatlantic version of Europol's Financial Intelligence Unit (FIU) model, where each nation holds its data but encrypted searching identifies information or patterns to follow-up.

Although there are suggestions that all-EU terrorist watch list could soon be set up within one of the continent's existing intelligence structures, resistance to this development could be of similar magnitude to that seen in the case of sharing PNR data.[67] Hence, a model based on the FIU, which protects source data and yet allows users to reach out to partners and follow-up on leads, could

[67] Interview, 7 March 2016.

be a welcome, workable solution. We understand Europol is currently developing an integrated model of the FIU system, based on identifying data connections through a secure portal of source anonymisations.

Such a hit-no-hit search function would begin as a standard platform for sharing basic structured data, such as PNR, criminal history, travel, financial and immigration information. This could engage a wider group of countries very quickly. The mid-term aim would be, however, to find technical solutions to create a capability for searching through unstructured data in an encrypted form.

5.4. Recommendation 3: TRANSATLANTIC CT CENTRE OF EXCELLENCE

There are a number of multilateral intelligence education courses in existence that provide useful examples for a CT Centre of Excellence (CoE). For example, the EU's Agency for Law Enforcement Training (CEPOL), in liaison with Europol, runs short courses and exchanges for border and police forces. The courses, many of which are delivered online, mainly focus on criminality, but some cover operational intelligence analysis. Meanwhile, NATO's HUMINT Centre of Excellence, based in Romania, provides another potential blueprint for the CT CoE. The CoE runs HUMINT courses and promotes best practice amongst its nine MS members. It evolved out of a recognition amongst some NATO MS that they lacked HUMINT capacity on military operations. As a result, in 2009 five MS initially joined the CoE; in 2010/11 another three followed suit, and in 2013 the US also joined, indicating the efficacy of the voluntary, ad hoc approach to intelligence training. Moreover, the Five Eyes' "Leadership in Counter Terrorism" (LinCT) programme brings together law enforcement, military and security services from these nations informally. It is a basis for enhanced social relations and the cross fertilisation of ideas, thinking and experiences that build trust.

A number of nations have been improving their training and education of their analysts and investigators. One notable step forward in professional intelligence education has been undertaken in Norway, where the Norwegian foreign intelligence service has established an intelligence university. This runs a three year course to train its operators in the theory and practice of intelligence, language, area studies, standardisation, operational analysis and techniques. One of the university's innovations has been the introduction of a short course specifically designed to inform senior politicians and decision makers about what intelligence can and cannot do, and what should be expected of intelligence agencies. In the Netherlands and Sweden there are comparable initiatives. The US also runs its National Intelligence University to accredit security personnel and allow them to study classified/top secret subjects. Other areas that have proven useful is the involvement of specialised academics in wider critical thinking on open source intelligence and security issues, such as what is the West's ISIL end game?

In order to uniformly raise capabilities and capacities of transatlantic partners, we recommend that a transatlantic CT Centre of Excellence (CoE) is eventually established. Crucially, the CoE, which would not necessarily launch as an institution but could initially coalesce around the transatlantic Core CT Hub or a focused Task Force, would bring empowered representatives from existing platforms and institutions together. Within this virtual network, best practises can be agreed, syllabuses and training material shared, and relevant courses introduced. The value of joint standardisation and training, which the CoE would design and run, would rest in bringing civilian and military, intelligence and law enforcement professionals together around CT issues and increase trust among participants and gradually their organisations. Once established, the CT CoE could work in concert or informally coordinate with the relevant EU and NATO bodies (which could also possibly provide financing) as well as the CdB's CTG. With its foundations in a shared perception of threat, and supported by strong political will, the CT CoE's primary goal would be to build trust, mutual understanding and promote standardisation.

We recommend that standardisation is a key competency of any CT CoE. In particular, common terminology is needed throughout the intelligence cycle for the understanding and prioritisation of threats, faster analysis and dissemination, and compatible standards for assessing information/ intelligence. The Brussels and Paris attacks also revealed the need for common data entry procedures, especially in terms of Arabic names. At a broader level, the CoE could provide benchmarking of MS' intelligence capabilities in order to allow entry into any core task forces such as that outlined above, whilst also encouraging best practice in intelligence oversight and liaison.

A further key competency of the CT CoE should be training. Numerous experts have identified that there needs to be strong political will to address key gaps in the current intelligence architecture, and that they must be staffed and attending by “A grade” intelligence officers if they are to be credible. CT CoE training should focus on best practises and should target collectors, analysts, and decision makers. It could also be used to address emerging technologies and the EU could contribute funding for its members.

Within the civilian sphere, the closer involvement of the private and third (voluntary) sectors should also be considered. The private sector can bring great insight into technology and the internet of things; technology itself is not a problem, but the operationalising and understanding of that technology can be. In addition, many voluntary organisations already have a close interface with hard to reach communities through their enhanced social relations over many years. This trust is a huge enabler and can assist in mitigating potential threats prior to them being exploited and indeed coming into the justice system, which in itself increases capacity and capabilities. These organisations only know what they know and if better equipped they could be valuable resources. Similarly, the CT CoE could be used to reach out to mental health services to better integrate them into CT efforts.

Via its activities, the CoE would aim to promote the enhanced security culture of partner agencies which can enhance trust and information security, identified as a key problem through this report. The integration of processes and the personal data/intelligence exchange are necessary to progress, but will only happen if the donor of that information has belief that the recipient is taking steps to protect that information. A strong security culture is hence the backbone of organisational resilience and the CoE's member states would be encouraged to promote and develop a positive organisational and security culture, which will in turn lead to a positive change in organisational-related behaviour by staff. This can result in enhanced organisational resilience and increased employee engagement; reduced risk and vulnerability; reduction in theft of materials or MS information; reduced risk of reputational or financial damage; low-cost interventions and improved organisational performance.

6. Conclusion

This paper has drawn on the vast experience of senior and tactical intelligence and law enforcement officials from across Europe and North America. It has clearly shown that the Salafist jihadist threat has evolved rapidly. Since 2014, increasing numbers of small, informal overlapping networks of violent extremists have conducted both sophisticated and crude terrorist attacks across the transatlantic space. Crucially, these networks are increasingly blending criminality with terrorist intent. And given the intent of ISIL and al-Qa'ida to target Europe and North America, this threat is likely to endure for some time to come. Moreover, the recent attacks have already exposed some nations' inability to effectively integrate their CT intelligence and law enforcement functions, and issues of capability and capacity within these functions. At the transnational level, despite the good progress made by Europol and Interpol in integrating CT law enforcement, and by the CdB in terms of CT intelligence, there is certainly potential for better liaison, both within these functions and between them. Of course, trust remains critical to increasing liaison. Building on best practises and existing networks, we have shown how a Core Transatlantic CT Hub and Case-Based Task Forces could begin to develop trust and set standards for CT intelligence liaison. It would also generate transnational multi-agency CT security and risk assessments. The better integration of hit-no-hit single search interfaces that use existing information safeguarding technologies to link existing databases is another area where CT liaison capacity, and hence operational capability, can be increased relatively easily. To further encourage standardisation, trust, best practises and political involvement, a CT Centre of Excellence – initially organic to the Core Transatlantic CT Hub – should also be considered.

These recommendations offer real-world, practical solutions to begin addressing the seams in the transatlantic security architecture that jihadists have exploited to incur over 1,000 civilian casualties since 2014. As we have shown, many of these casualties could have been prevented through best practises and better liaison. Thus, civilians across the transatlantic space have the right to demand action on these issues, and policymakers the duty to respond. Political will is crucial to the success of these proposals, but we argue that now is the time to adapt. For its part, GIRI will continue to work within its expanding network to promote this report's proposed solutions. In particular, in partnership with industry it will strive to incorporate existing technological solutions to better integrate transatlantic intelligence and law enforcement in a secure and anonymous manner. It will continue to promote trust, standardisation and collective training through continued engagement with academia and the relevant law enforcement and intelligence organisations. Finally, GIRI will aim to promote greater transparency and oversight of CT activities, and greater public awareness about how the intelligence and security agencies support public safety. Intelligence in some nations is often still viewed as part of the "deep state" and therefore not talked about in public discourse. Yet as the rule of law is central to CT efforts, governments must do more to explain the reasons for needed changes to legislation. Indeed, GIRI will continue to explore the possibility of a transatlantic summit between North American and European nations to take these and other proposals forward.

Honorary Steering Committee:

Hon. Michael Chertoff (Chair), former Secretary of US Department for Homeland Security, co-founder and Chairman of The Chertoff Group.

Hon. Carl Bildt, former Prime Minister of the Kingdom of Sweden.

John, Baron Reid of Cardowan, former Home and Defence Secretary, Member of the House of Lords.

Dr. August Hanning, former State Secretary in the Federal Interior Ministry of the Federal Republic of Germany and Director of the Federal Intelligence Service (BND).

Research Team:

Daniela Richterova, Politics and International Studies, University of Warwick.

Patrick Bury, Strategy and Security Institute, University of Exeter.

Advisors to the GIRI Initiative:

Dr. Cees Wiebes, intelligence scholar and former senior analyst at the Expertise & Analysis Department at the Office of the National Coordinator for Counter-Terrorism (NCTb) in the Netherlands.

Professor Sir David Omand GCB, Visiting Professor, Department of War Studies, King's College London and former Director of the Government Communications Headquarters (GCHQ).

Honorary Justice Jean-Louis Bruguière, Antiterrorism Expert, Council of Europe, Paris.

Jean-Baptiste Carpentier, Head of the Strategic Intelligence and Economic Security Unit, Paris.

Dr. Kjetil Anders Hatlebrekke, Associate Professor of Intelligence, The Norwegian Defence Intelligence University College, and Senior Visiting Research Fellow, Department of War Studies, King's College London.

Dr. Hans Wegmüeller, former Director of the Swiss Intelligence Service.

John Cuddihy, former Detective Chief Superintendent, Police Scotland, Visiting Practice Fellow at Coventry University.

Dr. Frank Foley, Counterterrorism and Intelligence Expert, Department of War Studies, King's College London.

Prof. Shlomo Shpiro, Director - Division of Intelligence and Homeland Security, Bar-Ilan University, Tel Aviv.

Dr. David Murphy, Lecturer in Strategy and Military History, National University of Ireland, Maynooth.

Brig. Gen. Ephraim Lapid, former senior military intelligence officer and spokesperson of the Israel Defense Forces (I.D.F).

Henry Plater-Zyberk, former UK Ministry of Defence's Conflict Studies Research Centre (CSRC), Prague.

GLOBSEC
POLICY INSTITUTE

GLOBSEC Policy Institute
Klariská 14
811 03 Bratislava
Slovak Republic

info@globsec.org
www.globsec.org

GLOBSEC
POLICY INSTITUTE

GLOBSEC Policy Institute
Klariská 14
811 03 Bratislava
Slovak Republic

info@globsec.org
www.globsec.org