The evolution of information-sharing in EU counter-terrorism post-2015: a paradigm shift?

Christine Andreeva

School of Law and Government, Dublin City University, Dublin, Ireland

ABSTRACT
Despite the instruments in place to facilitate policy and operational cooperation, until 2015 gaps in EU CT governance and operational inefficiency decreased the capacity for prevention and response. The paper will analyse the aftermath of the critical juncture brought by the attacks in Paris and Brussels (2015-2016) and its consequences for the development of EU CT information-sharing, thus enquiring the effects of securitisation on this domain. Having consulted multiple EU CT practitioners, the paper will demonstrate the increased efficiency of cross-border and inter-agency coordination in CT intelligence and police work since 2015, due to improved institutional design and legislative framework, which were able to contribute increased added value to national CT efforts. It will investigate in turn the immediate aftermath of the Paris and Brussels attacks on the institutionalisation of EU CT information exchange, and the long-term impact on practices in EU CT operational work.

Introduction
Attitudes towards information-sharing vary across EU Member States (MS), contingent on the organizational culture of law enforcement and intelligence at different operational levels. Professional jealousy and guarding of sources are characteristic to these sectors and evident within and between MS. Due to competition for information, MS hold data for their own usage, or as leverage in quid-pro-quo sharing (Interview n.23; also van Ballegooij and Bakowski, 2018, p. 27, 45; Höhn and De Kerchove, 2019, p. 26; Wensink et al., 2017, p. 70). Purportedly, the conservatism of traditional European secret services was not conducive to operational cooperation and until 2016, EU tools’ usage remained low, while decision-making power in advancing cooperation structures rested with the conservative states.

However, the November 2015 Paris attack represented a necessary critical juncture, demonstrating that MS could not deal with counter-terrorism (CT) on national level anymore. Beforehand, terrorism was a national security topic and multilateral exchange was not a practice: information-sharing was considered risky, inter-institutional competition was an impediment, and simply there was no perceived need
to share (Bures, 2018; Kaunert & Léonard, 2019; Maricut, 2016; Monar, 2015; Occhipinti, 2016; Rozée, Kaunert, & Léonard, 2013, etc.). Nevertheless, practitioners came to realize that dealing with terrorism independently was no longer realistic, as the nature of the threat had changed. As jihadist groups operating within the EU represented a new type of threat, the necessity to cooperate and the importance of information-sharing were not initially perceived – hence information gaps were not intentional, but rather resultant from fragmented intelligence data across services.

EU policy and operational entrepreneurs invested abundant efforts in convincing national practitioners of the advantages of cooperation and information-sharing in CT work. EU channels improved, various formats met more often, counterparts got to know each other, making it easier for them to coordinate. The EU has been recognized as an important channel, and national authorities have learned to use EU tools and to appreciate their added value. Some MS are still more involved than others, yet the structures necessary have been built, and practitioners’ perceptions of their usage have shifted.

The article begins by setting the scene of academic analysis in EU CT information-sharing and discussing the methodological choices made for this study. It then discusses, in turn, the institutional and practitioner-led implications of the 2015–2016 Paris-Brussels attacks on information-sharing in the EU. It wraps up by analysing the long-term consequences of these on CT practice in the Union, and reflects upon the cognitive shifts caused by this critical juncture, and their implications on the future of EU CT.

**Academic analyses of EU CT information-sharing and methodological choices made for this study**

This section will explore the scholar discussions in the domain of EU CT information exchange, and will position this article in the academic landscape of both empirical and theoretical contributions. Several scholars have delved into the idiosyncrasies underpinning information-sharing, and intelligence and police cooperation in the EU. A substantiated finding concerns the meagre intelligence-sharing at EU and multilateral levels, despite the otherwise ample amount of exchange (Den Boer, 2015; Fägersten, 2010; Gruszczak, 2016; Lander, 2004; Müller-Wille, 2004; Occhipinti, 2013; Svendsen, 2011; Walsh, 2006). Information-sharing occurs primarily at bilateral or ad hoc groupings, wherein scholars provide different explanations of the contributing factors: an obvious one is the confidentiality of information (MS risk exposing and endangering HUMINT resources), while intelligence can also become leverage for political negotiations. Intelligence is dominated by national reflexes and sovereignty concerns: interests and sensitivities rarely overlap, whereas different experiences with terrorism inform asymmetrical threat perceptions (Occhipinti, 2013). MS only exchange information when they share the threat and “otherness” of the enemy. Accountability over national security lies with MS and their services, who are unwilling to transfer responsibility to EU agencies like Europol, thus questioning their added value (Ilbiz, Kaunert, & Anagnostakis, 2017; Léonard & Kaunert, 2021; Müller-Wille, 2008; Occhipinti, 2013).
Fägersten (2010) groups European intelligence cooperation challenges in four themes:

- **Diverging preferences** – economies of scale approaches are only applied when agencies perceive that this will further their interests (or when those coincide).
- **Power asymmetries** – MS’ divergent intelligence resources and experience create asymmetric hierarchical relations, which might encourage bilateral relationships in place of multilateral ones.
- **Bureaucratic interests** – while part of the public sector, intelligence de facto operates independently, emancipated from the government’s direct control. Thus, while accountable to the government, it develops idiosyncratic institutional dynamics and internal loyalties that may trump political leadership ones.
- **Missing infrastructures** – except for technical infrastructures (e.g. databases) enabling sharing, “intelligence cooperation is facilitated by […] cooperative infrastructures. At a personal and organisational level, this means having a sufficient level of trust to allow actors to engage in cooperation” (Fägersten, 2010, p. 3). The EU’s role here can be significant: common trainings, exercises and mutual work experiences can contribute to an enhanced trust and understanding between counterparts.

The lack of confidence between partners affect the cross-border and cross-agency lack of cooperation (Bures, 2013; Fägersten, 2015; Lander, 2004; Müller-Wille, 2004; Walsh, 2006). Competition informs the mistrust between agencies horizontally, while unclear mandates and institutional design flaws are the EU-level culprits. Contention over investigative leads and financial resources, and inter-sector resentment are among the leading inter-agency issues, both within and across states. Disdain between police and intelligence in particular is a key issue in operational CT work (Bures, 2013, p. 72; Müller-Wille, 2004, pp. 17–19). The institutional design of cooperative arrangements is crucial for trust-building and approximation of divergent interests, and in overcoming cultural and strategic differences between MS. Fägersten (2010, 2015, p. 11) finds that “the overall development of the EU sets clear barriers for ambitious integration projects, particularly in contested areas such as intelligence”, nevertheless, “well-crafted arrangements have the possibility to mitigate bureaucratic resistance and thus enable cooperation even during unfavourable conditions”, which is where the EU has a role to play (Fägersten, 2010, p. 519).

Before 2015 international terrorism had little effect on EU intelligence cooperation, because “[w]hile the EU has responsibilities for some strategic decision-making, it does not play any significant operational or tactical role” (Müller-Wille, 2008, p. 69). This institutional design flaw resulted in the identity crisis of Europol and the “chicken–egg” dilemma of its added value (Bures, 2013). Europol was intended as a hub for information collection and sharing, however MS repeatedly resisted delegating such responsibilities to it, including in the aftermath of the 9/11 attacks, and 2004 Madrid bombings (Fägersten, 2010, pp. 506–507). At a time of heightened threat perception and calls for increased cooperation, MS unambiguously signalled their disinterest in an increased Europol role: they set up instead the Counter-Terrorism Group (CTG) a sub-grouping of the intergovernmental cooperation channel Club de Berne, where the majority of intelligence exchange occurs (Fägersten, 2010). One element of the problem is that “national agencies are both the main providers of intelligence to
Europol and its main customers, thus intelligence often “perceive information-sharing through Europol as an extra burden” and a duplication of their efforts, giving them no incentive to share (Bures, 2013, p. 85; Fägersten, 2010; Müller-Wille, 2004, p. 26). Another flaw of the EU CT apparatus was that databases were non-interoperable, and not cross-border accessible (Müller-Wille, 2008).

Heinrich (2006) predicted, that it would “take a new a threat, or a terrorist outrage that endangers Europeans’ shared and common interests, to change the situation”. Europe would come to learn that lesson in 2015. A 2018 editorial reported that “Europe can no longer be described as soft on terrorism” (Hegghammer, 2018). EU MS invested abundantly in CT, enhanced intelligence-sharing and “initiated a qualitative overhaul involving radical new measures that had previously been considered politically off-limits” (Hegghammer, 2018). This new model was considered successful, due to the significant decrease in attacks and casualties by 2018 – “not because plotting has decreased, but because authorities are foiling more attempts” (Hegghammer, 2018).

**Definition of core concepts and theoretical focus of this thesis**

Kuhn (1962) began the discussion of paradigm shifts during the structuralist period of social science. While his original concept dealt with natural sciences, social scientists quickly found value in it for the study of socio-political processes, and it remains one of the most reiterated concepts therein (Coleman, Skogstad, & Atkinson, 1996; Kuhn, 1962; McDonagh, 1976; Perez, 2004; Rodman, 1980; Wood, 2015, and many more). Critical junctures appeared in political science around the same time, and seemingly aimed at describing similar institutional change dynamics. It would become an influential concept for multiple social science models, such as punctuated equilibrium and historical institutionalism (Capoccia & Kelemen, 2007; Collier & Collier, 1991; Conran & Thelen, 2016; Hall & Taylor, 1996; Lowndes & Roberts, 2013; Mahoney, 2001; Pierson, 2004; Thelen, 2002). Both paradigm shifts and critical junctures made a similar causal claim: significant institutional development is not necessarily incremental or cumulative; often such change involves abrupt “jumps” instead. As both concepts originated in the same timeframe of scientific development, it is likely they were used interchangeably, as at that time neither received a detailed explanation or a conceptualization of the factors, pre-conditions, or consequences involved therein. As a result, both remained ambiguous and elusive, yet highly influential for political and social science. Still, they describe different social processes: critical junctures theorization claims that (usually due to an external event) circumstances may arise, which (temporarily) lower the threshold for political and institutional change, allowing such change to occur, whereas paradigm shifts conceptualize an (old) policy paradigm that did not fit the system anymore, being replaced by a new paradigm of perceptions and practices.

For the purposes of this article, critical junctures are defined as exogenous to the system events (in this case usually a terrorist attack), which shake up the system, often due to a change in the circumstances of the system. Such events put the system to the test and expose its inability to execute its originally defined functions. A critical juncture is usually followed by a flurry of political and functional discussions on upgrading the system’s functionality, followed further by multiple governance and legislative proposals. Usually, a critical juncture concludes by shifting the system to a new
“path” (enabled by its new instruments adopted during the critical juncture), which then becomes fixed itself, hence making it resistant to change until the next critical juncture occurs. Therefore, critical junctures are almost always followed by periods of path dependence.

Paradigm shifts (it is argued in this article) are not to be seen as synonymous with critical junctures. While critical junctures usually bring policy and institutional change, they do not necessarily shift the system’s paradigm. The system’s paradigm is characterized by the perceptions of the system’s function and use, and the practices involved therein. Thus, for example, the paradigm of EU CT used to be that the Union is only to provide a supplementary function of facilitating cooperation between the exclusively national responses to terrorism in the Union; it was then not expected to have an executive function and neither were all of its institutions and instruments. It will be argued in this article that, as a result of the critical juncture of the 2015–2016 Paris – Brussels attacks, EU CT shifted to a different paradigm, where counter-terrorism is no longer exclusively a national prerogative, but instead it necessarily involves cross-border operational cooperation and a fusion of operational resources (including both EU and national apparatuses, and practitioners across borders and professional sectors). Such a shift in perception and behaviour from both the constitutive actors of the system (EU MS) and its operational agents (CT practitioners) is conceptualized here as a paradigm shift for EU CT, and is speculated as likely to contribute to the lasting effects of the Paris-Brussels critical juncture.

Securitization is one of the more popular theoretical frames in security studies in the late twentieth and early twenty-first century, having been used by many scholars (Balzacq, 2008, 2005, 2011; Balzacq & Léonard, 2013; Bigo, 2008; Bourdieu, 1991; de Wilde, Leupold, & Schmidtke, 2016; Huysmans, Dobson, & Prokhovnik, 2006; Kaunert & Léonard, 2019; Kaunert & Yakubov, 2017; Wæver, 1995; Wittendorp, 2016). One of the more influential securitization scholars, defines securitization as

an articulated assemblage of practices whereby heuristic artefacts [...] are contextually mobilized by a securitizing actor, who works to prompt an audience to build a coherent network of implications [...], about the critical vulnerability of a referent object, that concurs with the securitizing actor’s reasons for choices and actions, by investing the referent subjects with such an aura of unprecedented threatening complexion that a customized policy must be undertaken immediately to block its development. (Balzacq, 2011, p. 3, emphasis in original)

Securitization is a process wherein state actors construct an international security issue as an existential threat to the population, with the purpose ofjustifying extraordinary government action in dealing with that issue (Buzan, Wæver, & de Wilde, 1998, p. 25). Securitization scholars posit that successfully securitized subjects receive disproportionate public attention, as compared to non-securitized topics, due to the exaggerated sense of threat. According to securitization theorists (Balzacq, 2005, p. 192), the process has three components, wherein in the absence of one or more of these elements, an attempted securitization process might fail:

− A securitising agent, the active communicator of the securitization process
− A security topic and the existential threat it potentially poses on the population
− An audience, targeted by the securitization effort.
This paper will demonstrate the EU’s opportunism in institutionalising and formulating CT governance. Securitization was palpable in the aftermath of the Paris-Brussels attacks and played a role in the domain’s reform, yet it was not deliberately designed by the EU (while it might have been pursued by its MS). However, it was skilfully applied by EU entrepreneurs to the impetus in the advancement of CT governance. Securitization in this period was the result of an increased threat, and was not perpetuated by the EU, but used by it in opportunistic and strategic ways, to add urgency and importance to legislative files, and by translating the high threat to high collective political will in advancing and reforming the Union’s CT capabilities. Finally, while driven by securitization, this EU CT critical juncture was notably different than previous ones: unlike them, it managed to change the perceptions on the Union’s role in CT and multilateral cooperation overall. As such, it provoked profound long-lasting changes and shifted the paradigm of conducting CT in the EU.

The article will demonstrate the potential effect of two factors for the development and maturation of EU CT information-sharing. The first is the perception of terrorism as an EU issue (both on political and practitioner level). While this is somewhat related to a common EU threat perception, it is still distinct, as demonstrated by the inability of the Madrid-London critical juncture to transfer the relatively high threat perception into a perception of terrorism as an EU-level issue. The second factor is the perception of EU added value in CT operational work – an integration brake before the Paris-Brussels critical juncture. This was the decisive difference brought about by the Paris-Brussels critical juncture: as MS began using EU CT capabilities in operational work, their added value was realized and further expanded by new mandates and capacities. The effects of the comprehensive CT reform have the potential to last, as they put in place the experts and structures needed for a functioning EU counter-terrorism apparatus. They have created the relationships necessary, on both political and operational level, to be considered as transformative for the policy, and they have created a political rationale and legitimacy for such coordinated EU efforts – while the EU has proven itself a useful channel for such coordination.

While these two factors may exist in previous EU CT literature, their causal potential has not been discussed thus far, because the first time that their full effect can be observed is in the aftermath of the Paris-Brussels attacks of 2015–2016. Hence, this study contributes to the EU CT academic literature in three ways: (1) through the postulation of two novel causal factors to its convergence; (2) through the discussion of new empirical material via the case study of the Paris-Brussels attacks’ aftermath and its effect on information management tools and practices; (3) through the claim that this juncture (unlike previous ones) led to a paradigm shift in EU CT information-sharing, due to the presumed long-term impact on practitioners’ perceptions.

The primary data of this study was obtained through in-depth interviews of experts, considered reliable witnesses of the inherent idiosyncrasies of the domain and its development. CT is shaped and dominated by practitioners: intelligence, police and judicial officials are the conductors of CT on national and, consequently EU level. During critical junctures before 2015, policy-makers made sweeping declarations on EU solidarity, cooperation and joined up action through EU agencies. However, as policy practitioners were not convinced of the necessity of such changes of approach, these ideas failed to become dominant or shift the paradigm. Intelligence officials have the potential to
shape CT practices and attitudes, which are not always congruent with those prescribed by political leadership, as they have a certain level of discretion rarely observed in public service. As such, they are a fundamental building block of CT’s development, they witness and participate in its reforms and standstills. As a subject of national security, CT data is difficult to obtain without a security clearance, which further made practitioners valuable in data collection. Forty diverse practitioners were interviewed between November 2018 and May 2019: 18 in national capacities, 31 in EU positions, 9 with intelligence functions, 15 with law enforcement profile, and 25 with policymaking competences.

**Post-2015 institutional developments in information-sharing**

Three sets of Council Conclusions in early 2015 renewed the EU’s mandate in CT, enabling it to legislate much more extensively: the Justice and Home Affairs (JHA) Council Conclusions, (General Secretariat of the Council of the EU, 2015b), the Foreign Affairs Council (FAC) Conclusions (General Secretariat of the Council of the EU, 2015a) and the Informal Heads of State Summit Conclusions (European Council, 2015). The framework CT strategic document was the *European Agenda on Security COM(2015) 185*, from April 2015. It offered a vision for EU coherence in various CT policy domains, while “setting out the main actions to ensure an effective EU response to terrorism and security threats” between 2015–2020 (European Commission, 2016b). Together with the Council Conclusions, it was meant to provide the Commission with a strategic mandate, through which it could justify further measures (Andreeva, 2020, p. 347, Interview n.2, 3, 4). A key legislative act, the CT Directive (*Directive (EU)2017/541 on combating terrorism*), replaced several framework documents and aimed to fill governance gaps, extending the classification of criminality of terrorist acts to include recruitment, training, travelling for terrorist purposes, facilitating and financing terrorist activities (Andreeva, 2020). These additions were necessary to impede, arrest and prosecute FTFs attempting to travel for combat training in Syria as their absence before 2017 has purportedly contributed to the ease of organization of several attacks (Andreeva, 2020, Interview n.33) (Figure 1).

**Europol’s updated mandate and new sub-structures; increased mandates for EU JHA agencies**

The first EU efforts towards online radicalization came after the Charlie Hebdo attack and involved the creation of an EU Internet Referral Unit (IRU)² at Europol, aiming to connect national practitioners and develop best practices. Since its July 2015 launch, the EU IRU has been tackling terrorist propaganda on the internet, advising MS, and acting as a platform for reporting violent content (Council of the EU, 2015b; General Secretariat of the Council, 2015a). The unit has been reported as value-adding by MS and practitioners and managed to gain an independent skillset not available at most national administrations (Interviews n.2, 6, 8, 9, 10, 13, 14, 15, 16). Less than two months after the November 2015 Paris attack, Europol’s European Counter Terrorism Centre (ECTC) was launched, intended as a channel for information-sharing and operational coordination. The Europol leadership was politically proactive as both
Figure 1. Timeline of the Paris-Brussels attacks and EU response.
sub-bodies were being prepared before they were proposed (Interview n.6). This made it possible for both institutional measures to be available when MS was looking for strategic involvement from the agency, subsequently, both were launched in exceptionally short timeframes. Both were enabled by Europol’s new mandate – Regulation (EU) 2016/794 from 11 May 2016 repealing and replacing the Europol Regulations from 2009 – a Regulation discussed since 2013, and recast by co-legislators in remarkable time (European Commission, 2017; Andreeva, 2019).

Europol’s leadership aimed to create a CT structure at the agency that mirrored national ones, without a “threatening” supranational ambition (Interview n.16, 6). The idea of a ECTC (re-)surfaced and failed to gather traction, due to MS resistance, after all previous significant attacks – 9/11, Madrid and London (Interview n.6). The fact that an old idea that previously met resistance, was recycled and eventually embraced, is a strong indication of the weight of the critical juncture brought on by the Paris (and Brussels) attacks. Currently, 80% of Europol staff have an operational function, dealing with support, analysis and prevention (Interview n.16).

In the aftermath of the Paris attack, EU agencies in aid of JHA operational work progressively gained an appreciation and increased mandates, budgets and trust from national authorities. Europol and Eurojust were engaged in CT investigations, beginning with the 2015 Bataclan attacks (Interview n.18,19). The involvement of Eurojust in investigations likely convinced MS of its added value in this domain, while (much like Europol) it helped the agency learn of the national needs where its support is most valuable.

Border security became priority for MS in the aftermath of the migrant crisis, whereas that concern has been compounded with anxieties over internal security (criminality and terrorism). Throughout the management of the migration crisis, MS became aware of the added value of Frontex, as front-line officers had access to data useful for intelligence services (Interview n.40). The upgraded Frontex, renamed the European Border and Coast Guard (EBCG), was launched on 6 October 2016, while its new mandate (adopted in November 2019) authorizes more than double the budget and staff, and provides for more extensive information-sharing with Europol and national authorities (Council of the EU, 2019; European Commission, 2018a; Europol, 2018). Most importantly, EBCG became an executive agency, empowered to deploy a Rapid Reaction Force, and recruiting a standing corps of 10,000 officers, who will be authorized to participate in operations and use force (Interview n.40; European Council on Refugees and Exiles, 2019). The most significant mandate given to an EU agency to date, it demonstrated the thinly-veiled lingering concern of national authorities over irregular migration, despite the counter-narrative of most MS governments.

The Security Union and its new commissioner

The 2016 Brussels attacks impetus enabled one of the most ambitious initiatives in internal security, the Security Union. With its legal basis in Art.67 TFEU, it upgraded the Area of Freedom, Security and Justice (AFSJ), and had its Commissioner appointed (Sir Julian King) on 19 September 2016. The Security Union established hitherto the strongest reform framework of the policy area, whereupon the Commission published regular Progress Reports, noting dossiers’ headway and timeframes. The initiative
allowed concerted and coherent policy action and follow-up on legislation, while it marked a major shift in approach through the regular use of infringement procedures against non-compliant MS, which was seen as a taboo until then (Interview n.2, 13, 8, 9, 10). The Security Union was also an innovation in terms of the holistic approach to CT and internal security – apart from traditional JHA tools, measures now include the Single Market (e.g. online content, explosives, firearms, etc.), as well as social and foreign policy domains (Interview n.13, 9). Measures on repressive security, protection of public spaces and radicalization were advanced quickly under the new Commissioner. During his first month in office, the CT Directive and the Firearms Directive were finalized and thereafter many more dossiers were pushed forward by his Cabinet, e.g. legislation on aviation security, extremist content online, explosive precursors, terrorist financing and interoperability (Interview n.13, 4).

**Inter-institutional dynamics and legislation**

Inter-institutional relations evolved in the Paris-Brussels attacks’ aftermath, due to the multitude of legislative and policy files advanced under political pressure. Through the cooperative work on high-impact legislation, EU institutions and agencies learned to work together and appreciate each other’s competence. In the process their roles and capabilities evolved too, rendering them more competent CT actors.

Before this critical juncture, security was an underestimated topic for the Commission, perceived as a national prerogative (Interview n.13). This likely followed a period of inactivity in CT, due to MS’ lack of interest in engagement. However, in the era of heightened threat, the Commission became active in all the fields where it was considered it could add value (including on operational level). Commission DGs and agencies have learned their roles and understand their position in CT better, they have found a way to communicate effectively with MS, avoiding federalist narratives. National authorities began engaging with the EU, whereas in the past “Brussels” was a faraway concept for them, as the “real work” was done at the capitals (European Council on Refugees and Exiles, 2019). Presently, MS approach the Commission proactively and flag issues or trends that need policy action. This attitude shift is significant: national authorities began understanding that the Commission can help them by obtaining expertise on the issues at stake for them (Interview n.9). Commission officials believe that they have succeeded (at least to an extent) to convince national authorities of the EU tools’ added value, leading to their increased usage (Interview n.9, 13). Furthermore, intelligence agencies began realising that the Commission advances legislation that potentially affects their work, and started engaging with the EU’s legislative triangle (Interview n.9, 13, 2, 21).

Inter-institutional tensions in the internal security apparatus are notorious. MS are generally sceptical of EU measures or legislation in this domain, they are represented in the Council by experts, who sometimes feel they do not have equivalent interlocutors in representatives from political bodies such as the EP or the Commission. The latter frequently finds itself in a brokerage position, mediating between other institutions towards constructive progress on EU-wide harmonization. In drafting legislation, the Commission often consulted primarily (and sometimes informally) the Council, presumably in pursuit of easier compromise among the often sceptical MS, with less stakeholders involved. These dynamics, combined with insufficient dialogue on divisive issues (e.g.
the security-privacy dichotomy), incurred mistrust and resentment in the EU institutional triangle. This led to a vicious cycle of omitting stakeholders from the negotiating stage, wherein these would later block progress on certain dossiers (specifically the EP) (Interview n.4, 21). Furthermore, it became a self-fulfilling prophecy: the more the Commission avoided involving the EP in the legislative procedure in the early negotiating stages for being a sceptic, the more the EP became a sceptic of the Commission’s proposals.

One of the acts that helped overcome these standstills was the High-Level Group on Interoperability. Apart from the tangible effect on the legislative dossier’s speed, the High-Level Group process, applied in other sub-fields too (radicalization, cyber security) had the welcome unintended consequence of inter-institutional cohesion. The Commission got all relevant stakeholders to sit together and iron out details on a controversial dossier, while interlocutors learned about each other’s priorities and objections. Traditional sceptics of security measures such as the EP and FRA got to voice their objections early and were content that those were considered. The Commission and MS’ experts got acquainted with these bodies’ red lines and got better at addressing them. Inter-institutional cohesion was further deepened through the reporting process of the EP’s Special Committee on Terrorism (TERR), mandated to investigate shortcomings in the EU’s CT apparatus. EP interviewees reported positive experiences from the Committee’s work, noting willingness to cooperate between stakeholders, and eagerness of the Commission to support their efforts, providing relevant information and experts (Interview n.27, 21, 26).

**Developments in information exchange after the November 2015 Paris attack**

One of the EU CT aspects that experienced the most dramatic shift as a consequence of the Paris attack was the information exchange between EU MS. It was acknowledged by interviewees that MS did not share sufficiently before the threat became ostensibly high (Interview n.23, 33, 35, 38, 31, 20, 24, 26). Databases were not used effectively (Interview n.31, 13, 28), while Europol’s state-of-the-art tools were underused (Interview n.1, 23, 24, 25). These issues made possible the information gaps that enabled the successful operation of terrorist groups on EU territory in the 2010s, and most of them were addressed in the aftermath of the Paris-Brussels attacks.

The change of attitudes began with the pursuit of Foreign Terrorist Fighters (FTFs) – European citizens who underwent training on IS territory and returned to the EU to organize terrorist acts (Interview n.2, 10, 13, 22, 23, 34, 35, 36, 38). In 2015, MS discovered that thousands of them were travelling around the EU undetected (Interview n.10). The hunt for FTFs triggered an increased use of SIS-II for discreet checks, leading to a steady annual increase in data volumes (according to eu-LISA reporting by about 30%), wherein at the time of interviews it was noted that SIS contained about 75M datapoints, which had been consulted by MS 5B times (Interview n.13). As CT structures are traditionally built on national level, it took the pursuit of FTFs and subsequent terrorist attacks for MS to realize that they could not tackle the threat nationally anymore (Interview n.16). This novel threat was more shared than ever before, and it had elements unknown to MS: the new type of terrorist had a criminal record, and operated transnationally (European Council on Refugees and Exiles, 2019).
In CT lessons learned come through attacks: they expose governance gaps and bring political will for common action. The alleged intelligence-sharing and cooperation failures during the Paris-Brussels attacks put the intelligence community under scrutiny, wherein they had to find ways to avoid further information gaps and maintain their ability to provide national security (Interview n.12). The necessity to cooperate, on EU level and internationally, became glaring and “working alone [was] no longer an option” – intelligence could not risk having undetected terrorist activity again (European Council on Refugees and Exiles, 2019). The threat could not be tackled nationally for three reasons: (1) operationally, in case something is missed on national level, to enable data discovery through other services, (2) it became politically unacceptable not to cooperate, (3) MS’ reputations were at stake, the quality of their risk assessment and ability to identify and prevent attacks were under question (European Council on Refugees and Exiles, 2019).

**Europol’s CT role increased substantially through the involvement in the Paris attacks investigation⁴ and the setup of ECTC⁵**

The proverbial window of opportunity for Europol opened when the Paris Prosecutor leading the 13 November attacks’ investigation stipulated that all the data therein was to be shared with the agency (Interview n.6). An unprecedented action, it made Europol seem like a useful channel – it helped other MS see it as a potential channel too (European Council on Refugees and Exiles, 2019). Europol formed *Taskforce Fraternité* on 7 December 2015, composed of 25 officers from France and Belgium. This was a sort of pilot for Europol’s capability to deliver holistic solutions supporting MS’ operational work, it contained all the tools necessary for sharing investigation data (European Council on Refugees and Exiles, 2019). Europol conducts background checks and cross-checks the large amounts of data contained in its databases, thus increasing investigation speed (Interview n.13, 18). However, MS only saw that after the Paris attack’s handling, which changed their perceptions of the agency’s added value (Interview n.13, 14).

This critical juncture was necessary to open national perceptions on Europol’s CT role (Interview n.14). Before 2015, Europol received little information from MS, who now share all types of data from CT investigations. Between 2009-2018, there was a ten-fold increase in the data they receive and a six-fold increase in the operations they conduct (Interview n.6). Between 2016-2018, entries in the Europol Information Systems went from 6000 to half a million (Interview n.6, 9). The agency has expanded its data collection capabilities, adapting to the increased information-sharing. Europol’s contribution has proven especially useful since the establishment of ECTC, which has an increased capacity to support operational needs (Interview n.2, 24). Until 2016, the agency had mainly a strategic and analytical capability, whereas now it has operational competences and new tools at its disposal, which clearly add value. It is particularly useful in the post-hoc stage of incidents, and when a less experienced MS is involved (for many MS the tools necessary are too expensive to develop domestically) (European Council on Refugees and Exiles, 2019).

As a result of a visible spillover process, Europol continued its evolution. It has become clearer to national authorities that the links in CT investigations will not always be evident (which allows for a bilateral approach), rather the dots to connect
often come from unrelated to the case MS (European Council on Refugees and Exiles, 2019). The “conservatism towards Brussels” and its extensions such as Europol is no longer observed in the CT community, which came to the realization that neither the EU nor Europol wants to take “the driver’s seat” in operational CT work (European Council on Refugees and Exiles, 2019). For the agency, the 2015–2016 events were crucial, as it was able to gain valuable experience and adapt to MS’ needs (Interview n.4). For the openness to Europol’s role to be achieved, MS had to first start using the tools it provides to understand their added value. Since 2016, no investigation of a terrorist attack was without an international element, and Europol was involved in all their investigations.

**Innovations in information-sharing: EU PNR adopted**

The Paris attacks were the main motivator for the ultimate adoption of the Passenger Name Records (PNR) Package (Council of the EU and European Parliament, 2016) on 21 April 2016. A legislative act previously vetoed by the EP and stuck in the EU pipelines for over a decade, was suddenly agreed in weeks under immense political pressure. The PNR package allows the collection of data on air travel passengers, provided to law enforcement authorities by airline carriers (Interview n.4, 9, 21, 35, 36, 34). Law enforcement authorities were advocating for this measure as they were struggling to track the movement of FTFs in/out and within the EU. While the events from January 2015 made a difference in advancing certain dossiers, it was ultimately the November Paris attack that “made [PNR] happen” (Interview n.4, 9). Suddenly, all legislation in this domain was a matter of high-level political discussion, which fast-tracked dossiers, as MS came to realize that low implementation and slow decision-making affected CT effectiveness.

**New legal basis for SIS-II and increased use**

The Schengen Information System (SIS-II) is the most important database for cross-border law enforcement investigations. Whereas the first generation SIS was set up in 1995 as a compensatory measure for internal border controls relaxation among Schengen signatories, a 2016 Commission evaluation found an unsatisfactory usage of the second generation database (European Commission, 2016a). One trigger for this evaluation was the failure to detain the only surviving perpetrator of the Paris attack, whereupon a police check was unable to identify a reason to detain him, despite the Belgian authorities’ awareness of his radicalization (Interview n.34, 35, 36, 38). The incident triggered a bitter political dispute and blame-shifting between France and Belgium, while eventually two systematic issues were identified: (1) insufficient information exchange between police and intelligence authorities in Belgium, and broadly in the EU, and (2) uneven SIS usage across MS, due to organizational and cultural differences (European Commission, 2016a). What followed was a record-high increase in SIS usage, wherein between 2013–2018 alerts increased by 63.5% and database accesses amplified by 381.5% (likely also due to systematic irregular migration checks). The increased use of SIS-II has proven beneficial for the database: the so-called “hits” (i.e. a cross-match of a search performed by a MS where another MS previously input an alert) have increased by 207.8%
between 2013–2018, evidencing that when more alerts are available there is a higher chance the information system adds value.

Immense political pressure pushed also the update of SIS-II’s legal basis, aiming at more effective usage (Interview n.36). Regulations (EU)2018/1860,1,2 were adopted on 28 November 2018 (Council of the EU and European Parliament, 2018a, 2018b, 2018c), introducing an obligation on MS to enter asylum return decisions in SIS, granting access to Europol and Frontex, and including more data categories (Interview n.40, 32, 34, 35, 36, 23). The legislation imposes an obligation on EU MS “to create a SIS alert for all cases related to terrorist offences” and “to inform Europol of hits [and] alerts linked to terrorism, which will help to connect the dots at the European level” (European Commission, 2018c). With the SIS reform, the Commission created derogations for some alerts’ reporting to SIS, however not for CT, seen by EU legislators as an obligation on national authorities to input alerts (Interview n.36). This is not the first EU legislative attempt to compel CT information-sharing, notably Council Decision 2005/671/JHA formally obliged authorities to share all CT data relevant to cross-border investigations, however, there was no feasible enforcement on such a clause.

**Tackling the fragmentation of data and introducing interoperability**

Various EU databases are used for divergent purposes by different national authorities. CT operational information is so sensitive that not everyone might trust one specific channel (Interview n.14). Intelligence in CT is separated on national basis but also on regional/local basis, wherein every MS (and region) has a specific way of working on terrorist cases (Interview n.19). While data input has drastically increased since 2015, national authorities still have preferences, leading to a fragmentation and compartmentalization of information (Interview n.23). The intelligence community does not go through EU platforms, but through informal channels, specifically the Club de Berne and CTG fora created by them (Interview n.19).

Whereas bilateral coordination was previously the norm, it has been recognized that multilateral cooperation was necessary to tackle the unprecedented threat. National security services are the main counter-terrorist instrument, and traditionally they avoided cooperation, to pre-empt the risk of leaks (Interview n.22, 25, 13, 14, 11). Nevertheless, as a consequence of the rising threat, MS changed their sharing habits – both in terms of volume and purpose. Through experience, some MS learned to necessarily looking for cross-border elements in terrorist plots (Interview n.19). One important realization, giving the issue of CT a European dimension, was that “you are as strong as your weakest link” (Interview n.34). Therefore, designating matters of information-sharing exclusively to MS and leaving them with a limited understanding of how to use EU tools may have significant effects on sharing practices. The EU found an effective way to harmonize and coordinate internal security responses: investing (financially and capacity-wise) in information systems (Interview n.1). Innovative information systems have significantly facilitated cross-border cooperation, and the EU has implemented several ambitious projects (European Council on Refugees and Exiles, 2019).

The most far-reaching initiative in this domain is the interoperability of EU information systems. Until 2016 any legislation on this topic was considered taboo and
politically impossible, owing to EU leaders’ unwavering position to avoid conflating and fallacious association of migration and terrorism in the context of the 2015 migrant crisis. According to EU officials (Interview n.7, 8, 9, 17, 28, 29, 30, 31), several factors affected the change of approach, including:

- The Paris attack involving two perpetrators who entered the EU during the migrant crisis with fake identification documents. In the attack’s aftermath, law enforcement (including Europol) could not access databases such as Eurodac, VIS and SIS, contributing to data compartmentalization (Interview n.4).
- The December 2016 Berlin attack, which led to political pressure by German authorities. The perpetrator had 14 fake identification documents from various MS (and criminal activities in Germany and Italy, of which both national authorities were not fully informed).

The core purpose of interoperability is connecting EU databases used by migration authorities (VIS, Eurodac) and law enforcement (SIS-II), and creating a comprehensive record of third-country nationals staying on EU territory (with or without visas), and on asylum seekers, through the establishment of new information systems (European Travel Information and Authorisation System – ETIAS, Entry/Exit System – EES and ECRIS-TCN). The interoperability framework involves a new Common Identity Repository aimed at tracing fake identification documents, while an ECRIS-TCN database is being developed to facilitate an exchange of third-country nationals’ criminal records between MS. Through a European Search Portal, law enforcement and immigration authorities at a certain clearance level will be able to see a comprehensive suspect profile, aiming to close information gaps in investigations of criminality, terrorism and irregular migration. The interoperability package will enable eu-LISA to build a Central Repository for Reporting and Statistics and a Shared Biometric Service. To empower eu-LISA to operationally manage existing databases and develop new ones, its mandate was upgraded on 12 November 2018, making it an official EU agency (European Commission, 2018b). The legislative procedure was finalized on 14 May 2019 with Regulations 2017/0351,2(COD). Considering the complexity of this legal act in its almost 350 pages (excluding supplementary legislation), its adoption within 18 months was remarkable and indicative of a solid consensus and shared prioritization, not only between co-legislators, but among all stakeholders involved.

The adoption of the interoperability package would not have been possible without the High Level Expert Group on Information Systems and Interoperability: a consultation procedure the Commission organized at the level of policy-makers, practitioners and consulting bodies (Interviews n.7, 8, 9, 17, 28, 29, 30, 31). Not only did it engage high-profile practitioners and policy officials from the 28 MS, it involved representatives from all EU institutions and relevant agencies. The Commission showed political skill in involving the potentially harshest sceptics – the European Data Protection Supervisor (EDPS), the Fundamental Right Agency (FRA) and the EP. These bodies have long criticized the Commission and Council for intransparency in the JHA legislative process, and for overlooking data protection (Interviews n.21, 26, 27, 40).
Commission avoided these criticisms by engaging all relevant stakeholders before the drafting stage, thus co-opting their support, and fostering compromise by having all concerns pre-emptively discussed, allowing for a smooth and rapid legislative procedure post-hoc.

Interoperability was discussed in 2003–2004 and in 2008–2009, yet it did not go further. Its ultimate adoption was predicated upon the underuse of data from different databases, wherein the quantity of data was not insufficient, but its usage was inefficient. By connecting information systems, EU legislators aim to close the information gaps found in migration and law enforcement.

**CTG formalization demonstrates changing attitudes towards cooperation**

The “real work” in intelligence cooperation is not done on EU level but at the intergovernmental channels of Club de Berne and its sub-grouping, the CTG (Interview n.3). These were designed bottom-up by the intelligence agencies, in an informal setting fitting to their operational coordination needs (European Commission, 2018b). CTG is the “de facto intelligence agency for the EU” and since 2015, it has built its own platform enabling multilateral cooperation (European Commission, 2018b). This permanent cooperation is “a direct reaction of the services to the Paris attack” – in its aftermath, media and political discourses zeroed in on intelligence-sharing failures, putting CTG under immense pressure (Interview n.12, 6). Some intelligence agencies were confident in their emancipated approach to CT, however the new transnational dimensions of the threat did not correspond to such isolated approaches anymore (European Commission, 2018b). Consuming exclusively their own intelligence meant that MS denied themselves the opportunity to identify possible links with other MS, and build bridges to other datapoints. One of the most significant consequences of the Paris-Brussels critical juncture, CTG’s formalization “surpassed everyone’s expectations” (Interview n.3, 12, 16, 2, 21, 4, 9). Presently, the agencies’ cooperation is structured, they have permanent representatives and liaison officers at CTG headquarters, if needed they can reach their national systems (Interview n.12). There is a common CTG database, where MS input intelligence for other MS to access and explore (European Commission, 2018b).

**Long-term impact on information-sharing**

*Increased trust practitioners learned to work together*

As previously established in academic literature (Fägersten, 2016; Müller-Wille, 2004; Svendsen, 2011; Walsh, 2006), insufficient trust across authorities is a key issue in EU CT cooperation (Interview n.1, 2, 4, 5, 7, 9, 11, 14, 17, 18, 20, 23). Lacking trust is observed at various levels – between different MS’ authorities, between national and European bodies, and within a national security apparatus (Fägersten, 2016; Müller-Wille, 2004; Svendsen, 2011; Walsh, 2006). Mistrust is explained by rivalries and competition for resources and investigative findings; further complicated by divergence and occasional incongruence in interests, whereas in some countries exchanges between agencies is discouraged (Interview n.33, 24, 25, 32). In cross-border cooperation
another significant obstacle was that many national authorities across the EU did not know how to work together and did not know each other enough to develop trust. Building trust is a slow process, practitioners need to work together for it to develop, they also must share strategic objectives, which is rarely the case (Interview n.12, 14, 17, 1).

For trust-building it is important to have strong bilateral relationships, because through them agents get acquainted with their counterparts (Interview n.11). According to interviewees, trust is built via interpersonal contacts, through cooperation on common investigations (Interview n.12, 14, 17, 1, 19, 7, 5). The resulting familiarity shapes the initial trust and sets the basis for the working relationship (Interview n.7). Regular meetings help to establish connections too: cross-border practitioners become acquainted and learn to anticipate each other’s approaches, then it becomes easier for them to work together. As MS built contacts and trust across borders and institutions, they built the habit to share (Interview n.1).

One way to fast-track that process, according to interviewees, are common trainings, both bilaterally and through the EU (Interview n.23, 7, 1, 4, 20). These practices are useful for building connections and facilitating counterparts’ understanding of each other’s way of thinking and legal/constitutional differences. EU trainings (including through CEPOL and eu-LISA) are increasingly used, as “it has become clear that [they] help to build trust” and common strategic priorities (Interview n.1, 4). Another trust-building measure praised by interviewees, is the use of liaison officers, which improves operational coordination as officers get well-acquainted and become a single point of contact with other MS, helping to build coherence (Interview n.17, 20).

These dynamics have improved trust significantly: there is better cross-border and cross-agency communication, and an enhanced understanding of mutual priorities (Interview n.2, 18, 12, 16, 25, 31). Connections have been built via the common work on CT cases, changing how practitioners think – it is no longer just a national authority they are addressing, it is a colleague they know (Fägersten, 2016; Müller-Wille, 2004; Svendsen, 2011; Walsh, 2006). The CT experts in ECTC have built confidence in Europol too, while the CTG’s relationship with Europol and the EU CTC has also improved. (Interview n.2, 9, 38).

**Enhanced information-sharing between police and intelligence**

CT is a conglomeration of sub-fields, each with its specific expertise, priorities and agenda. This makes cooperation inherently difficult, especially since on EU level it is a horizontal matter, with no central authority to coordinate efforts (Interview n.24). CT governance is decentralized: authority is dispersed across the chain of command, while it necessarily involves a fusion of police and intelligence work, and for some MS those silos do not mix (Interview n.24). For law enforcement Europol is an established channel for coordination, but there is no such channel for intelligence. If intelligence agencies want to detain someone it is a formal process; if they want to follow or use him/her, it becomes a grey zone – they could coordinate through the CTG, through the EU or not at all (Interview n.4). Police-intelligence cooperation is even more complicated on EU level, not least because intelligence work is perceived as out of scope for the EU (Interview n.16, 9, 24, 38, 4). Operational agencies with overlapping mandates are in
direct competition over investigative resources and funding (Interview n.9). Furthermore, the nexus between the sectors needs to be managed at national level first, otherwise “the EU cannot bring much added value” (Interview n.13).

The relationship between intelligence and police has been improving since 2015 (Interview n.12, 16, 4, 2). The perception that intelligence information should not be shared shifted after the Paris-Brussels attacks, as it became clear that MS need both types of data for pursuit and investigations (Interview n.35, 26). Countries that experienced terrorist acts (UK, France, Belgium, Netherlands) have established national fusion centres between law enforcement and intelligence to merge the information necessary for a full picture (Interview n.26, 38, 19, 21). The structures and channels for cooperation are now in place, and have penetrated the minds of practitioners, whereas before this juncture there was insufficient awareness of their potential uses and added value (Interview n.4). There is an increased understanding of common priorities across services, as the increased threat compelled practitioners to work together. Importantly, police and intelligence learned that they needed each other’s data as each brings a different piece of the investigative puzzle (Interview n.34, 35, 36, 11, 37, 9, 4, 20). Attacks are a catalyst for change: it took the increased threat and cross-border investigations for police and intelligence to realize that they need each other and change their approaches (Interview n.34).

**The political-operational gap**

Another issue discussed by interviewees is the political-operational gap in CT, both on national and EU levels (Interview n.2, 3, 4, 5, 11, 19, 23, 24, 31, 32, 34, 38). There is a noted chasm between political statements and operational reality: initiatives, announced or teased, seldom take account of the operational issues involved (Interview n.2, 5). Such discourses used to ensue confusion as to the role the EU was attempting to take in internal security (considered a sovereign domain for MS) and pushed practitioners “further away” from EU cooperation (Fägersten, 2016; Müller-Wille, 2004; Svendsen, 2011; Walsh, 2006). Nevertheless, improvement has been noted in this political-operational divide: with the surge of the terrorist threat, political leaders and policy-makers had a strong motivation to work with practitioners (Interview n.34). National fusion centres helped encourage dialogue and cooperation, they built communication habits between various practitioners and policy-makers. On EU level, the use of seconded experts increased, fostering cohesion between EU and national authorities. Finally, the High-Level Group format has received universal praise from policy and operational practitioners (Interview n.31).

**A long-lasting shift?**

The EU is by definition a reactive entity – as per the Treaties it is only allowed to be involved in policy areas where MS have explicitly found that it could add value to national efforts. Any field not pertaining to the Single Market is up for debate and national authorities would instinctively try to keep at the national level. MS have gotten apprehensive of the EU’s excessive bureaucracy and the unforeseen obligations that often stem from its regulation, thus to involve the Union, they need to be persuaded beyond any doubt of its instruments’ added value to national ones.
Generally, MS believe they can handle terrorism on national (if need be bilateral) level. Therefore, the bulk of EU security work takes place intergovernmentally at the Council, and there is little for the Commission to do. Furthermore, policy-making tends to get stuck after some time, then a crisis is necessary to expose governance gaps and open critical junctures (Interview n.31, 22). On one hand, the sheer shock of large-scale attacks in EU capitals, impeccably coordinated, long-organized and expensive, combined with the successful escape of the only surviving Paris attack assailant and a follow-up attack of his associates, created a juncture more powerful than those of previous attacks, and reaffirmed the validity of the punctuated equilibrium model, postulating that, unless the system experiences a shock, opening a window of opportunity for reform, that system would stay on its path, even if that path is no longer functional to its circumstances.

However, this critical juncture also produced a long-lasting bracket of reforms, impacted by (and further impacting) shifts of perception on terrorism and counter-terrorism in Europe, leading to a paradigm shift of beliefs and practices. While those would likely not have occurred without the shocks of the attacks, it is clear from EU CT history that in the absence of ideational and cognitive changes, a critical juncture has short-lasting reactive policy effects, and fails to lead to a paradigm shift. As interviewees pointed out, the attacks exposed gaps in governance and security in the EU, and subsequently, each new incident was a lesson learned informing a concrete policy or operational response. Hardly any of these responses were original: the EU had long lobbied for some of the measures. Nevertheless, it took the critical juncture and the realization of the communality of the threat to begin endorsing them, causing the realization of their usefulness, leading to more cross-border CT cooperation mediated by EU tools and mechanisms, leading to the endorsement of more measures. This virtuous feedback cycle shifted the EU CT paradigm. While national authorities learned to entrust certain tasks onto EU legislators and institutions, the latter learned to approach the former in a non-sovereignty-impinging manner, increasing mutual trust and engagement. The same effect was observed on EU level among its institutions, from the relationship between the legislative triangle of Council-Commission-Parliament to relations among EU agencies.

This shift of perceptions resulted in drastically increasing volumes of data exchange. There has been a steady increase in the use of SIS, Europol has had to develop new tools, necessary to facilitate the manifold increases of data input and common investigations (Interview n.29, 6). Practitioners got into the habit of sharing, the number of database entries has been on a consistently upward trend (Interview n.25). The proactive attitude on cross-border investigations was an “automatism created due to the attacks” (Fägersten, 2016; Müller-Wille, 2004; Svendsen, 2011; Walsh, 2006). Practitioners do not foresee mentalities shifting back and claimed that the “national reflex is gone, now the international reflex is there” (Interview n.19, also n.21, 2, 34, 35).

Except for the critical-juncture-induced surge in information-sharing, there are two important developments in EU CT that have the potential of translating to lasting convergence. Firstly, the perceptions on EU CT have changed at practitioner level: police, intelligence, and other sectors realized that they need each other and changed their reactive approaches to proactive ones (Interview n.34, 35, 36). They have built a network of contacts, they know and work well with counterparts. Multilateral cooperation has “grown organically and is not going back”, because according to practitioners “this is
Intelligence services have moved from a “need-to-know” to a “need-to-share” approach, to even a “share-to-know” one, which shifted the approach to CT work in the EU (Interview n.14, 15, 34, 35). This was an unprecedented threat for Europe and MS underestimated it, some foreseeing that they could counter terrorism on national level (Fägersten, 2016; Müller-Wille, 2004; Svendsen, 2011; Walsh, 2006). The terrorist threat can and should no longer be contained unilaterally or bilaterally by MS, nor exclusively by intelligence services (Interview n.1, 10, 14, 23, 37, 32). If CT data is represented as a puzzle, it can be assumed that a single service has several pieces, but not quite enough to visualize the full image, which is why MS need to share pieces cross-border and cross-agency to build the investigative picture.

Secondly, national authorities and practitioners have gotten to know the EU and its tools and learned that the EU is a good channel for improving bilateral and building multilateral contacts with other European or international partners. Practitioners are bound by their own practices, through which they have been trained and habitualized in the past, and are sceptical of new approaches, including cross-border cooperation, EU tools, etc. (Interview n.23). The intelligence sector is also fairly independent, which makes them not necessarily accountable to the government the same way other public servants are (Interview n.14). Therefore, CT officers need to perceive a tool as adding value in order to make appropriate use of it. Commission officials believe that they have succeeded in convincing national authorities of the EU tools’ added value in operational cooperation, leading to their increased usage (Interview n.9). Importantly, through this usage, MS were able to perceive the added value of EU channels.

**Conclusion**

While EU counter-terrorism will likely never fully integrate into a common policy, due to the significant operational, functional and sovereignty hurdles to overcome, it is well on its way to overcoming the gaps in governance that may have enabled an easier organization and execution of terrorist attacks on EU territory until 2015. The paradigm shift in EU CT was caused by a securitization-led shake-up of conceptual constructions of security policies as belonging to MS’ sovereign jurisdictions alone, and not crossing borders, thus not having to be relinquished or shared with the Union. EU policy-makers appear to be well-aware of MS’ reservations, and strategic about pushing forward important legislation in politically opportune moments, however, both European publics and national practitioners needed to be convinced of the necessity and added value of an EU role in CT. While the policy remains a hybrid, it is becoming a well-functioning one, through the clarification of mandates, proper utilization of instruments, and a necessary element in CT policy-making: a high common threat perception, induced by symmetrical political pressure across MS.

The effects of the comprehensive policy reform have the potential to last, as the latter has put in place the experts and structures needed for a functioning EU counter-terrorism apparatus. They have created the relationships necessary, on political and operational levels, to transform the policy, and have created a political rationale and legitimacy for a coordinated EU effort, while the EU has proven a useful channel for such coordination. Some of the legislation adopted during this juncture, e.g. interoperability, PNR, repressive measures towards extremist online content, firearms and explosive precursors
possession, etc., have potentially long-lasting effects too, consequential for the way CT is conducted in the EU.

While EU CT policy entrepreneurs may not have purposefully led the securitization of terrorism, they exhibited skilful opportunism in taking advantage of the high threat perception to the benefit of the construction of supranational (or at least collective) governance in CT operational work. As has been clear since 9/11, in security policies progress comes exclusively after events and EU CT policy-makers are so aware of this dynamic, that they appropriated the phrase “Never let a crisis go to waste” to their domain (Interview n.6). They know to take advantage of political will by introducing or advancing legislation. Afterwards the process takes on a natural momentum: if they can prove the added value of (and encourage the use of) the unique tools that Europol, SIS-II, Eurojust, etc. provide, then the process follows smoothly (Fägersten, 2016; Müller-Wille, 2004; Svendsen, 2011; Walsh, 2006). Pre-existing EU mechanisms and bodies were upgraded and their functions became clearer to practitioners, as impediments to their mandates and effective usage have been removed. According to practitioners, MS work together on CT much better and more effectively since 2016, and are increasingly able to avoid information gaps. It has become much more difficult to conduct organized terrorist activity in the EU. There is awareness and accountability on CT, practitioners and politicians alike learned the importance of avoiding governance gaps and are trying to bring the CT apparatus to full functionality. These dynamics would have hopefully shaped an “international intelligence community which can increasingly tackle the difficult challenge of counterterrorism with more effectiveness than individual efforts” (Lasoen, 2020, p. 13).

Notes

1. Human intelligence, e.g. spies or undercover agents.
2. Modelled after the UK’s IRU.
3. The ECTC was discussed at the 12 March 2015 JHA Council and the process was put in motion thereafter (Council of the EU, 2015b; General Secretariat of the Council, 2015a).
4. Interview n.6, 13, 14, 2, 9, 18.
5. Interview n.11, 1, 24, 2, 39, 2, 9, 24, 25.
6. The proposal, which was ultimately adopted was proposed on 2 February 2011, however there had been previous legislative proposals in 2008 that were rejected (Council of the EU, 2012).
7. These statistics are obtained through eu-LISA annual statistical data on the usage of SIS-II. As eu-LISA has a limited mandate on the use of statistics, where it is only allowed to publish annual estimates without any analytical purpose, the author has calculated these increases through the figures on annual uses of SIS published by eu-LISA (eu-LISA, 2013, 2014, 2015, 2016, 2017, 2018).
8. A new database of European Criminal Records Information System aimed at third-country nationals.
9. Interview n.12, 13, 21, 2, 3.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The author(s) reported there is no funding associated with the work featured in this article.
Notes on contributor

Christine Andreeva recently successfully defended her PhD at Dublin City University (DCU) on “EU Counter-terrorism’s Gradual Institutionalisation: Information-sharing and Cooperation in Law Enforcement and Intelligence Post-2015”. She has published articles with ERA Forum and the Bulgarian Association for European law on the topic of EU harmonisation and institutionalisation measures in counter-terrorism after 2015. Her research has aimed to demonstrate the qualitative shift in EU counter-terrorism post-2015, as compared to previous critical junctures, such as the one after the Madrid and London attacks in 2004-2005. She has presented her research at academic conferences focused on EU integration and security topics. Christine previously studied European integration with focus on EU security policies in her Master studies at the Institute of European Studies in Brussels, and worked in the European Parliament as a policy advisor to an MEP.

References

Andreeva, C. (2019, May). EU counter-terrorism policy after 2015 – the added value of harmonisation over national-based approaches. In Emerging voices – a future of Europe anthology (pp. 193–211). Dublin: Institute for International and European Affairs (IIEA). [online]. Retrieved from: https://www.iiea.com/wp-content/uploads/2019/06/Christine-Andreeva.pdf.

Andreeva, C. (2020). The EU’s counter-terrorism policy after 2015—“Europe wasn’t ready”—“but it has proven that it’s adaptable. ERA Forum, 20(3), 343–370. doi:10.1007/s12027-019-00570-0

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context. European Journal of International Relations, 11(2), 171–201. doi:10.1177/1354066105052960

Balzacq, T. (2008). The policy tools of securitization: Information exchange, EU foreign and interior policies*. JCMS: Journal of Common Market Studies, 46(1), 75–100. doi:10.1111/j.1468-5965.2007.00768.x

Balzacq, T. (2011). Understanding securitisation theory: How security problems emerge and dissolve. Oxon: Routledge.

Balzacq, T., & Léonard, S. (2013). Information-sharing and the EU counter-terrorism policy: A ‘securitisation tool’ approach. In C. Kaunert & S. Léonard (Eds.), European security, terrorism and intelligence: Tackling new security challenges in Europe, Palgrave studies in European Union politics (pp. 127–142). London: Palgrave Macmillan UK.

Bigo, D. (2008). Globalized (in) security: The field and the ban-opticon. In D. Bigo, D., & A. Tsoukala (Eds.), Terror, insecurity and liberty. Illiberal practices of liberal regimes after 9/11 (pp. 10–48). Oxon and New York: Routledge.

Bourdieu, P. (1991). Language and symbolic power. (G. Raymond and M. Adamson, Trans). Cambridge: Polity Press.

Bures, O. (2013). EU counterterrorism policy: A paper tiger? Farnham: Ashgate Publishing, Ltd.

Bures, O. (2018). ‘EU measures to combat terrorist financing’. In C. King, C. Walker, & J. Gurulé (Eds.), The Palgrave handbook of criminal and terrorism financing Law (pp. 855–881). Cham: Springer International Publishing.

Buzan, B., Wever, O., & J. de Wilde. (1998). Security: A new framework for analysis, Boulder: Lynne Riener Publishers.

Capoccia, G., & Kelemen, R. D. (2007). The study of critical junctures: Theory, narrative, and counterfactuals in Historical institutionalism. World Politics, 59(3), 341–369. doi:10.1017/S0043887100020852. 2011/06/13 edn.

Coleman, W. D., Skogstad, G. D., & Atkinson, M. M. (1996). Paradigm shifts and policy networks: Cumulative change in agriculture. Journal of Public Policy, 16(3), 273–301.

Collier, R. B., & Collier, D. (1991). Critical junctures and historical legacies. Princeton: Princeton University Press.

Conran, J., & Thelen, K. A. (2016). Institutional change, The Oxford handbook of historical institutionalism. Oxford: Oxford University Press.

Council of the EU. (2012). Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of
Homeland Security, OJ L 215, 11.8.2012, p. 5–14. [online]. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811%2801%29.

Council of the EU. (2015a, February 15). FAC meetings. Main Results. [online]. Retrieved from: https://www.consilium.europa.eu/en/meetings/fac/2015/02/09/.

Council of the EU. (2015b, March 12–13). JHA council meeting. Main results. [online]. Retrieved from: https://www.consilium.europa.eu/en/meetings/jha/2015/03/12-13/.

Council of the EU. (2019, April 1). European Border and Coast Guard: Council confirms agreement on stronger mandate. Press Release [online]. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2019/04/01/european-border-and-coast-guard-council-confirms-agreement-on-stronger-mandate/.

Council of the EU and European Parliament. (2016). Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, [online], OJ L 119, 4.5.2016, p. 132–149. Retrieved from: https://eur-lex.europa.eu/eli/dir/2016/681/oj.

Council of the EU and European Parliament. (2018a). Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, PE/34/2018/REV/1, OJ L 312, 7.12.2018, p. 1–13. [online]. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1860.

Council of the EU and European Parliament. (2018b). Regulation (EU) 2018/1861 of the European Parliament and the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, PE/34/2018/REV/1, OJ L 312, p. 56–104. [online]. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1861&from=EN.

Council of the EU and European Parliament. (2018c). Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, PE/34/2018/REV/1, OJ L 312, p. 56–104. [online]. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1862&from=EN.

de Wilde, P., Leupold, A., & Schmidtke, H. (2016). Introduction: The differentiated politicisation of European governance. West European Politics, 39(1), 3–22. doi:10.1080/01402382.2015.1081505

Den Boer, M. D. (2015). Counter-terrorism, security and intelligence in the EU: Governance challenges for collection, exchange and analysis. Intelligence and National Security, 30(2–3), 402–419. doi:10.1080/02684527.2014.988444

European Commission. (2016a). Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA, {SWD(2016) 450 final}, COM(2016) 880 final. [online]. Retrieved from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161221/report_on_evaluation_of_second_generation_sis2_en.pdf [Accessed 10 May 2019].

European Commission. (2016b, November 16). European Agenda on Security: Second report on progress towards an effective and sustainable Security Union. Press Release. [online]. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_3681.

European Commission. (2017, April 29). Commission welcomes Europol’s new mandate and cooperation agreement with Denmark. Press Release, [online]. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/fr/STATEMENT_17_1169.

European Commission. (2018a). Proposal COM(2018) 631 final, 12 September 2018, Annexes to the proposal for a Regulation of the European Parliament and the Council on the European Border
and Coast Guard and repealing Council Joint Action n°98/700/JHA, Regulation (EU) n°1052/2013 of the European Parliament and of the Council and Regulation (EU) n°2016/1624 of the European Parliament and of the Council [online]. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:631:FIN.

European Commission. (2018b). Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, PE/29/2018/REV/1, OJ L 295, p. 99–137. [online]. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1559147864586&uri=CELEX:32018R1726.

European Commission. (2018c). Security Union: New rules on reinforced Schengen Information System enter into force. Press Release. [online]. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6921.

European Council. (2015, February 12). Informal meeting of the Heads of State or Government Brussels, Statement by the members of the European Council. Press Release. [online]. Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/.

European Council on Refugees and Exiles. (2019). An EU Agreement on Reform of Frontex. [online]. Retrieved from: https://www.ecre.org/an-eu-agreement-on-reform-of-frontex/.

Europol. (2018). TE-SAT Report 2018. [online]. Retrieved from: https://www.europol.europa.eu/sites/default/files/documents/tesat_2018_1.pdf.

Fägersten, B. (2010). Bureaucratic resistance to international intelligence cooperation – The case of Europol. Intelligence and National Security, 25(4), 500–520. doi:10.1080/02684527.2010.537028

Fägersten, B. (2015). Intelligence and decision-making within the common Foreign and security policy. Swedish Institute for European Policy Studies, European Policy Analysis, 2015, 22epa. [online]. Retrieved from: https://d1wqtxts1xze7.cloudfront.net/38978720/Fagersten_EPA_2015_eng.pdf?1443797736=&response-content-disposition=inline%3B+filename%3DIntelligence_and_decision_making_within.pdf&Expires=1613698280&Signature=EUu9yDQB2b–S7rcGMj4PC0X6VU4Q9hIQxChCrC3H–i7g–f807DstAiMmzIgMNgOTHR–dFoeEd6IaggBcifv3UXWkZ7SAEcBqjNY18h6-x16zV23M2m5S0we75zIbWnvrlvBPvR7VlaHBU3Z7UtjBK1zSapsWGPtAS6yCO66wFsvs-VFbj30ERWTktiIPjhcH0cNZUZ7JK---qARHBzv9HnSd6OKIdsbh5t4t5LuAwJS3aFYWZHqgwatYrTjOEPIRJLGi2rvbWKS5ZjRS0m1w0HN1zxZWXGk0U7VUIRXDkFpFJZ14hA4MevH1nwy2antvGcW3cgW36Wbaqg__&Key-Pair-Id=APKAJLOHF5GGSLRVB4ZA.

Fägersten, B. (2016). For EU eyes only? Intelligence and European security. European Union Institute for Security Studies (EUISS). Brief Issue n. 8, 2016, pp. 1–4. [online]. Retrieved from: https://www.eui.europa.eu/sites/default/files/EUISSFiles/Brief_8_EU_Intelligence_Cooperation.pdf

General Secretariat of the Council of the EU. (2015a, April 23). Special meeting of the European Council – Statement, EUCO 18/15, CO EUR. [online]. Retrieved from: http://ec.europa.eu/dorie/fileDownload.do;jsessionid=jeSxzMm7FWkq2g1w8-L_fhXkN-Be_A75tLbPuSPQK4RGL9GsSbjJ-2142749860?docId=2098892&cardId=2098891 [Accessed 3 May 2019].

General Secretariat of the Council of the EU. (2015b). Informal meeting of Justice and Home Affairs Ministers in Riga on 29 and 30 January 2015, 5855/15. [online]. Retrieved from: http://data.consilium.europa.eu/doc/document/ST-5855-2015-INTE/en/pdf.

Gruszczał, A. (2016). Intelligence security in the European Union, building a strategic intelligence community. London: Palgrave Macmillan UK.

Hall, P. A., & Taylor, R. C. (1996). Political science and the three new institutionalisms. Political Studies, 44(5), 936–957.

Hegghammer, T. (2018, October 7). Europe to Terrorists: It’s No More Monsieur Nice Guy. Wall Street Journal. [online]. Retrieved from: https://www.wsj.com/articles/europe-to-terrorists-its-no-more-monsieur-nice-guy-1538950931.

Heinrich, J. (2006). The case for a European CIA. Europe’s World, Spring 2006, 138–139.

Höhn, C., & de Kerchove, G. (2019). The role of European intelligence in countering terrorism. In J. Dietich, & S. Sule (Eds.), Intelligence law and policy in Europe (pp. 82–120). Oxford: Hart Publishing.
Huysmans, J., Dobson, A., & Prokhovnik, R. (2006). The politics of protection: Sites of insecurity and political agency. London, New York: Routledge.

Ilbiz, E., Kaunert, C., & Anagnostakis, D. (2017). The counterterrorism agreements of Europol with third countries: Data protection and power asymmetry. Terrorism and Political Violence, 29(6), 967–984. doi:10.1080/09546553.2015.1092438

Kaunert, C., & Léonard, S. (2019). The collective securitisation of terrorism in the European Union. West European Politics, 42(2), 261–277. doi:10.1080/09546553.2018.1510194

Kaunert, C., & Yakubov, I. (2017). Securitization: Turning an approach into a framework for research on EU justice and home affairs. In A. Ripoll Servent, & F. Trauner (Eds.), The Routledge handbook of justice and home affairs research (pp. 30–40). London: Routledge.

Kuhn, T. (1962). The structure of scientific revolutions. Chicago: University of Chicago Press. ISBN: 0-226-45803-2.

Lander, S. S. (2004). International intelligence cooperation: An inside perspective. Cambridge Review of International Affairs, 17(3), 481–493. doi:10.1080/0955757042000296964

Lasoen, K. L. (2020). Plan B(ruxellles): Belgian intelligence and the terrorist attacks of 2015-16. Terrorism and Political Violence, 32(6), 1291–1309. doi:10.1080/09546553.2018.1464445

Léonard, S., & Kaunert, C. (2021). The development of Europol’s external relations: Towards supranationalism? Maastricht Journal of European and Comparative Law, 28(2), 229–244. doi:10.1177/1023263X211005162

Lowndes, V., & Roberts, M. (2013). Why institutions matter: The New institutionalism in political science. London: Macmillan International Higher Education.

Mahoney, J. (2001). Path dependent explanations of regime change. Studies in Comparative and International Development, 36(1), 111–141.

Maricut, A. (2016). With and without supranationalisation: The post-Lisbon roles of the European Council and the Council in justice and home affairs governance. Journal of European Integration, 38(5), 541–555. doi:10.1080/07036337.2016.1178253

McDonagh, E. L. (1976). Attitude changes and paradigm shifts: Social psychological foundations of the Kuhnian thesis. Social Studies of Science, 6(1), 51–76.

Monar, J. (2015). The EU as an international counter-terrorism actor: Progress and constraints. Intelligence and National Security, 30(2–3), 333–356. doi:10.1080/02684527.2014.988448

Müller-Wille, B. (2004). For our eyes only? Shaping an intelligence community within the EU. Paris: European Union Institute for Security Studies.

Müller-Wille, B. (2008). The effect of international terrorism on EU intelligence co-operation. JCMS: Journal of Common Market Studies, 46(1), 49–73. doi:10.1111/j.1468-5965.2007.00767.x

Occhipinti, J. D. (2013). Availability by stealth? EU information-sharing in transatlantic perspective. In C. Kaunert & S. Léonard (Eds.), European security, terrorism and intelligence: Tackling new security challenges in Europe, Palgrave Studies in European Union politics (pp. 143–184). London: Palgrave Macmillan UK.

Occhipinti, J. D. (2016). Still moving toward a European FBI? Re-examining the politics of EU police cooperation. In J. Argomaniz, O. Bures, & C. Kaunert (Eds.), EU Counter-Terrorism and intelligence, A critical assessment (pp. 43–67). Abingdon/New York: Taylor & Francis.

Perez, C. (2004). Technological revolutions, paradigm shifts and socio-institutional change. In E. Reinert (Ed.), Globalization, economic development and inequality: An alternative perspective (pp. 217–242). Cheltenham: Edward Elgar Publishing.

Pierson, P. (2004). Politics in time. Princeton: Princeton University Press.

Rodman, J. (1980). Paradigm change in political science: An ecological perspective. American Behavioral Scientist, 24(1), 49–78.

Rozée, S., Kaunert, C., & Léonard, S. (2013). Is Europol a comprehensive policing actor? Perspectives on European Politics and Society, 14(3), 372–387. doi:10.1080/15705854.2013.817808

Svendsen, A. D. M. (2011). On ‘a continuum with expansion’? Intelligence cooperation in Europe in the early twenty-first century. Journal of Contemporary European Research, 7(4: Special Issue), 520–538. [online]. Retrieved from: http://jcer.net/index.php/jcer/article/download/318/308.
Thelen, K. (2002). The explanatory power of historical institutionalism. In R. Mayntz (Ed.), *Akteure-Mechanismen-Modelle. Zur theoriefähigkeit makro-sozialer analysen* (pp. 91–107). Frankfurt a.M.: Campus Verlag.

van Ballegooij, W., & Bakowski, P. (2018). *The fight against terrorism. Cost of non-europe report*. Brussels: European added value unit, May 2008. [Online]. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/621817/EPRS_STU(2018)621817_EN.pdf. [Accessed 15 Jun. 2021].

Wæver, O. (1995). Securitization and desecuritization. In R. Lipschutz (Ed.), *On security* (pp. 46–87). New York: Columbia University Press.

Walsh, J. I. (2006). Intelligence-Sharing in the European Union: Institutions Are Not enough*. *JCMS: Journal of Common Market Studies*, 44(3), 625–643. doi:10.1111/j.1468-5965.2006.00638.x

Wensink, W., et al. (2017). *The European union’s policies on counter-terrorism – relevance, coherence and effectiveness*. European Parliament. [Online]. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf. [Accessed 25 Jun. 2021].

Wittendorp, S. (2016). Conducting government: Governmentality, monitoring and EU counter-terrorism. *Global Society*, 30(3), 465–483. doi:10.1080/13600826.2016.1173653

Wood, M. (2015). Puzzling and powering in policy paradigm shifts: Politicization, depoliticization and social learning. *Critical Policy Studies*, 9(1), 2–21.