Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

This project was funded by the European Union's Internal Security Fund – Police

Public–Private Partnerships to Counter Terrorist Financing

Ruta Bajarunaite

Research Briefing No. 10

About Project CRAAFT

Project CRAAFT is an academic research and community-building initiative designed to build stronger, more coordinated counterterrorist financing capacity across the EU and in its neighbourhood. Project CRAAFT is funded by the European Union's Internal Security Fund – Police, and implemented by a Consortium led by RUSI Europe, along with the University of Amsterdam, Bratislava-based think tank GLOBSEC and the International Centre for Counter-Terrorism (ICCT), based in The Hague. For more information, visit <projectcraaft.eu>.

This publication was funded by the European Union's Internal Security Fund – Police. The content of this publication represents the views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published in 2022 by the Royal United Services Institute for Defence and Security Studies.

Detecting, investigating and prosecuting terrorist financing cases requires significant technical expertise and robust legal and operational frameworks, which many countries lack.[1] Furthermore, countries experience challenges with the detection of transactions through both the formal and informal financial systems, such as a lack of enhanced investigative and enforcement capabilities or difficulties in integrating financial intelligence into their counterterrorism efforts.[2] These obstacles to more effective CTF policy are transnational and require international cooperation at both the public and private levels. While the importance of public–private CTF collaboration is gaining recognition, there is still a significant lack of understanding of the challenges and opportunities of public–private partnerships (PPPs) in the fight against terrorist financing.

Defining PPPs

The use of PPPs to counter terrorism is not new. Its origins are in the counterterrorism frameworks established after 9/11. UN Security Council Resolutions 1368 (2001) and 1373 (2001) called on the international community to redouble their efforts to prevent and suppress terrorist acts through increased cooperation[3] and intensifying and accelerating the exchange of (operational) information.[4] In addition to this, in November 2003, the 9/11 Commission reported that a major focus should be placed on PPPs, as the majority of critical infrastructure is in private hands, making collaboration and information sharing vital.[5] Furthermore, it was reported that existing siloes and a lack of coordination between US law enforcement and intelligence agencies driven by hierarchical pyramids led to failures to connect the dots and chase down leads prior to the attacks.[6] After 9/11, PPPs came to be seen as a comprehensive response to the changing terrorism threat as they could prevent terrorists from exploiting gaps within the multi-layered international financial system.[7]

The utility of PPPs was further underlined in the UN Global Counter-Terrorism Strategy adopted by the UN General Assembly in 2006, where member states were encouraged to consider reaching out to the private sector for contributions to capacity-building programmes, in particular for port, maritime and civil aviation security.[8] Then in 2007 the Organization for Security and Co-operation in Europe formally acknowledged the usefulness of public–private counterterrorist efforts.[9]

The emphasis on the collaboration between public and private stakeholders is emphasised in UN Security Council Resolution 2462 (2019). The resolution encourages competent national authorities, in particular financial intelligence units, to establish effective partnerships with the private sector – including financial institutions, the financial technology industry and internet and social media companies – to identify the trends, sources and methods

1. UN Office on Drugs and Crime (UNDOC), 'Countering Terrorist Financing', 2022, <https://www.unodc.org/unodc/en/terrorism/news-and-events/terrorist-financing.html>, accessed 15 May 2022.
2. UN Security Council, 'Letter Dated 3 June 2020 from the Chair of the Security Council Committee Established Pursuant to Resolution 1373 (2001) Concerning Counter-Terrorism and the Chair of the Security Council Committee Pursuant to Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings and Entities Addressed to the President of the Security Council', S/2020/493, 3 June 2020, <https://documents-ddny.un.org/doc/UNDOC/GEN/N20/138/54/PDF/N2013854.pdf?OpenElement>, accessed 15 May 2022.
3. UN Security Council, 'Resolution 1368 (2001), Adopted by the Security Council at its 4370th Meeting on 12 September 2001', S/RES/1368 (2001), 12 September 2001, para. 4, <https://digitallibrary.un.org/record/448051>, accessed 18 June 2022.
4. UN Security Council, 'Resolution 1373 (2001), Adopted by the Security Council at its 4385th Meeting on 28 September 2001', S/RES/1371, (2001), 28 September 2001, paras 3(a)–3(c), <https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf>, accessed 18 June 2022.
5. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: National Commission on Terrorist Attacks Upon the United States, 2002), <https://www.9-11commission.gov/report/911Report.pdf>, accessed 18 June 2022.
6. Intelligence Resource Program and Federation of American Scientists, 'Statement of Zoe Baird Budinger and Jeffrey H. Smith Senate Committee on Homeland Security & Governmental Affair: Ten Years After 9/11: A Status Report on Information Sharing', 12 October 2011, <https://irp.fas.org/congress/2011_hr/101211smith.pdf>, accessed 19 June 2022.
7. Martin A Weiss, 'Terrorist Financing: The 9/11 Commission Recommendation', Congressional Research Report, 25 February 2005, <https://sgp.fas.org/crs/terror/RS21902.pdf>, accessed 19 June 2022.
8. UN General Assembly, 'Resolution Adopted by the General Assembly on 8 September 2006, 60/288. The UN Global Counter-Terrorism Strategy', A/RES/60/288, 20 September 2006, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement>, accessed 19 June 2022.
9. Organization for Security and Co-operation in Europe Ministerial Council, 'Decision No. 5/07 Public-Private Partnerships in Countering Terrorism', MC.DEC/5/07, 30 November 2007, <https://www.osce.org/files/f/documents/3/e/29569.pdf>, accessed 19 June 2022.

of terrorism financing.[10] Furthermore, it is important to ensure that PPPs are established before the need for a terrorist financing investigation arises.[11] Thus, while the importance of public and private sector cooperation is recognised, the term 'public–private partnership' often reflects a mixture of unspecified goals.[12] It is notable, that a partnership approach requires aligned goals on both sides. While the public and private sectors share a common commitment towards tackling various forms of illicit financing, their organisational mandates differ and thus require calibration for an effective partnership. Public stakeholders are specifically focused on national security and public safety matters so their efforts are targeted at protecting citizens from terrorism threats and disrupting terrorist groups' capabilities. Private stakeholders prioritise enforcing and maintaining their reputation and corporate integrity while formally conforming with CTF requirements. Nevertheless, a partnership approach creates more space for an open dialogue, where both sides shall be prepared to contribute to the common cause[13] – countering terrorism through tackling terrorist finances. While public and private stakeholders have diverse motives for countering terrorist financing, the close cooperation between sectors is mutually beneficial for a variety of reasons.

For the public sector, financial service providers can guide financial intelligence units and law enforcement agencies and support their investigations with additional transactional and counterterrorism data, which is for detecting and preventing attacks or investigating them after they have occurred.[14]

For the private sector, the close collaboration with law enforcement and intelligence agencies is significant as the public sector have the most comprehensive picture of terrorism and are often best placed to detect evolving threats.[15] In addition, the private sector needs guidance on the detection of terrorists' money flows and without the contextual insights from law enforcement or intelligence agencies this task is challenging.[16] Often terrorist financing activities involve small sums of money, which come from legitimate sources, such as wages. Additionally, there are often no clear links between the financial transaction and terrorist activity – the purchase of a plane ticket or renting a car may be assessed as ordinary financial transactions and are not suspicious in themselves.[17] Detecting these types of transactions on the basis of common risk indicators is incredibly difficult. That is why such transactions are at risk of being simply overlooked, if financial services providers do not get any relevant leads from the law enforcement authorities. Therefore, for private stakeholders it is more efficient to prioritise and investigate cases that potentially involve terrorist financing-related money flows with the support of information received from the public sector, rather than looking for a needle in a haystack. It is worth noting that overlooked transactions by financial services providers that lead to the financing of a terrorist attack cause not only loss of life but critical reputational damage for the financial services providers as well.

Emerging Issues

Properly enabled and resourced PPPs can help both sides ensure that their applied risk mitigation measures remain fit for purpose and can adapt in a timely and targeted way to emerging and evolving threats.[18] While PPPs may differ in their form, size, objectives, maturity level and scope

10. United National Security Council, 'Resolution 2462 (2019), Threats to International Peace and Security Caused by Terrorist Acts: Preventing and Combating the Financing of Terrorism', S/RES/2462 (2019), 28 March 2019, para. 22, <http://unscr.com/en/resolutions/2462>, accessed 16 May 2022.
11. Financial Action Task Force (FATF), 'Speech by FATF President at 2020 Chairmanship OSCE-Wide Counter-Terrorism Conference', 15 September 2020, <https://www.fatf-gafi.org/publications/fatfgeneral/documents/2020-osce-counter-terrorism-conference.html>, accessed 15 May 2022.
12. Benjamin Vogel, 'Potentials and Limits of Public-Private Partnerships Against Money Laundering and Terrorism Financing', *Eucrim* (No. 1, 2022), pp. 52–60.
13. *Ibid.*
14. Simon Riondet, 'The Value of Public-Private Partnerships for Financial Intelligence', *Journal of Financial Compliance* (Vol. 2, No. 2, 2018), pp. 148–54.
15. *Ibid.*
16. *Ibid.*
17. Belgian Senate, 'Senate Written Question No. 6-2214', 15 January 2019, <https://www.senate.be/www/?MIval=/Vragen/SVPrint&LEG=6&NR=2214&LANG=nl>, accessed 20 June 2022.
18. Global Counterterrorism Forum, 'Good Practices Memorandum for the Implementation of Countering the Financing of Terrorism Measures While Safeguarding Civic Space', September 2021, <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/cft_programme_coordinated_gctf_doc_cft_in_civic_space_en.pdf>, accessed 15 May 2022.

of data exchanged,[19] information sharing that includes identified terrorism financing-related vulnerabilities, risk indicators, trends, typologies or customer-related data is the cornerstone of PPPs. However, information sharing brings legislative, technological and security challenges that should be addressed in the co-creation or development phases of PPPs.

Legislative Challenges

Countries should ensure that their national legal environment enables PPPs to achieve their objectives, is proportionate to the threats posed by terrorism and respects fundamental human rights.[20] Therefore, existing legal limitations need to be addressed to unlock the full potential of PPPs in the fight against terrorist financing and enable targeted and timely information sharing.

Sharing of strategic information (such as typologies and trends) between public and private stakeholders to enhance the understanding of terrorist financing risks is possible under the existing EU legal framework, including GDPR. However, the effectiveness of PPPs can be enhanced in more ambitious and effective ways, which include tactical or operational information exchange about ongoing investigations with vetted financial institutions.[21] It is important to note that tactical information exchange is still not widely exploited by PPPs due to the lack of legal clarity as the current EU legal framework does not contain specific provisions on sharing tactical information between the public and the private sectors.[22]

Tactical information sharing requires a clear legal basis, the criteria and purposes for which operational information may be shared, the stakeholders between which it can be shared, and oversight mechanisms to ensure that information security, data privacy requirements and the integrity of criminal investigations are properly adhered to. Thus, even though under EU anti-money laundering and CTF legislation[23] sharing of operational data is possible, it has to be supplemented accordingly with local legal gateways, which detail the tactical information-sharing procedures. In this context, it is important to note that as CTF is a crucial contributor to national security, exemptions laid down in GDPR's Article 23[24] are applicable when considering tactical information exchange about data subjects. However, mapping potential legal gateways that consider safeguarding the integrity of criminal investigations is still needed to fully unlock the potential of tactical information sharing for CTF purposes.

It is worth noting that public–private sector collaboration and tactical information exchange has already proved to be successful, for example, the UK's Joint Money Laundering Intelligence Taskforce[25] (JMLIT) using existing established legal gateways[26] for information exchange. In 2017, after the London Bridge attack, the

19. Egmont Group, 'Public-Private Partnerships: Role of FIUs in PPPs', 2018, <https://egmontgroup.org/wp-content/uploads/2021/09/2018_Public-Private_Partnerships_PPPs_from_the_perspective_of_Financial_Intelligence_Units_FIUs.pdf>, accessed 15 May 2022.
20. Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017).
21. Riondet, 'The Value of Public-Private Partnerships for Financial Intelligence'.
22. *Ibid.*
23. Council of the European Union, 'Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC)', *Official Journal of the European Union* (L141/73, 5 June 2015).
24. Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', *Official Journal of the European Union* (L119/1, 4 June 2016). Article 23 of the GDPR lists the conditions under which EU Member States can restrict data subject rights as long as these restrictions are set out by legislative measure and are necessary and proportionate in a democratic society to safeguard, for example, national security, defence or public security.
25. Joint Money Laundering Intelligence Taskforce (JMLIT), 'Public-Private Information Sharing Partnerships to Tackle Money Laundering in the Finance Sector: The UK Experience', 2022, <https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/inline/4%20UK%20approach%20to%20public-private%20partnerships.pdf>, accessed 10 May 2022.
26. In their fight against terrorist financing, the JMLIT bases its operational information-sharing arrangements on Section 7 of the Crime and Courts Act 2013, use information-sharing provisions in Section 21CA of the Terrorism Act 2000 (as amended by the Criminal Finances Act 2017) for information-sharing purposes and process personal data according to Para 15(a) Schedule 1 of the Data Protection Act 2018. Additionally, JMLIT operational working group members act according to the JMLIT internal information-sharing arrangements.

National Terrorist Financial Investigation Unit, with the assistance of the UK's financial intelligence unit, initiated a rapid response and the case was brought to JMLIT within 12 hours of the attack. Within a few hours of the briefing, financial institutions were able to provide assistance in identifying the payments for van hire and establishing spending patterns, allowing further investigative strategies to be identified. This assistance was crucial in allowing investigators to conclude that the attack involved only three attackers with no broader network.[27]

In contrast to the JMLIT, operational information exchange for CTF purposes may be based on rather generic legal provisions – however, that does not undermine the effectiveness of PPPs. For example, the Dutch terrorism financing taskforce, a public–private partnership structurally set up in 2019, has put forward terrorist financing cases under the legal gateway, which was created according to the general article in the Netherlands Police Information Act.[28] When Dutch police passed names of suspected terrorists to banks, this revealed around 300 unusual payments.[29] Most of these transactions have been identified as suspicious. Additionally, after vetting the accounts related to flagged transactions, the banks encountered, among other things, a terrorism suspect who was engaged in fraud.[30] Banks have also identified how airline tickets for travellers from Syria were financed through intermediaries with different bank accounts.[31] Moreover, due to close collaboration the number and quality of reports submitted to the financial intelligence unit due to terrorist financing increased as well. While previously one in 10 reports about suspicious transactions was used for further investigations, after the taskforce has started its operations, six out of 10 reports were passed for the further investigations.[32]

Technology Challenges

Countries should use technology to facilitate the exchange of tactical information between public and private stakeholders, and ensure that sufficient analytical resources are available to support other PPP objectives, such as strategic information exchange. The effectiveness of PPPs in CTF highly depends on whether the information can be shared between public and private stakeholders in real-time in a secure way. To this end, it is important to ensure that software compatibility issues do not hamper information exchange. For example, the Dutch terrorism financing taskforce uses a platform – developed in conjunction with the Dutch FIU and several major banks – which contains profiles that help to identify transactions that may be related to terrorist financing.[33] These risk profiles are then shared with all relevant obliged entities for the purpose of identifying previous unusual transactions involving potential terrorist financing.[34] Additionally, the taskforce, together with banks, developed analytical models for detecting terrorist financing. Close collaboration between public and private sectors in the process of co-developing and testing new and innovative technology solutions and analytical tools helps drive software compatibility.

Security Challenges

Cross-institutional information exchange comes with particular security challenges. When considering information exchange for CTF, it is important to ensure that safeguards are in place against inappropriate sharing of information, and to prevent any potential information security breaches.[35] These requirements must be part of the local legal gateways, establishing the procedure and/or information-sharing arrangements between public and private sectors, and they should include

27. FATF ' Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom, Mutual Evaluation Report, December 2018', <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html>, accessed 15 May 2022.
28. Nick J Maxwell, 'Expanding the Capability of Financial Information-Sharing Partnerships', RUSI, March 2019, <https://www.future-fis.com/uploads/3/7/9/4/3794525/pr%C3%A9cis_of_ffis_paper_-_expanding_the_role_of_fisps_-_march_2019.pdf>, accessed 15 May 2022.
29. Belgian Senate, 'Senate Written Question No. 6-2214', 15 January 2019, <https://www.senate.be/www/?MIval=/Vragen/SVPrint&LEG=6&NR=2214&LANG=nl>, accessed 20 June 2022.
30. *Ibid.*
31. *Ibid.*
32. *Ibid.*
33. Egmont Group, 'Public-Private Partnerships: Role of FIUs in PPPs'.
34. *Ibid.*
35. Monetary Authority of Singapore, 'FI-FI Information-Sharing Platform for AML/CFT: Consultation Paper, P013–2021', October 2021, <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf>, accessed 16 May 2022.

requirements for both type of sectors to have systems and processes in place to prevent unauthorised access and use of exchanged data. Additionally, requirements should be set out to maintain records and audit trails of access to and provision of any information.[36] Apart from the security features that should be built into the information exchange system, access to information should be restricted and allowed only on a need-to-know basis. This would mean allowing only designated staff to access the information or to submit data based on received requests and/or ad-hoc needs.

There are also important ethical considerations around data collection and processing. Consistency with the principles of proportionality and data minimisation is of critical importance when it comes to operational information sharing. As noted above, Article 23[37] of the GDPR allows Member States to restrict the rights of data subjects, if that restriction respects fundamental rights and freedoms and is a necessary and proportionate measure to safeguard national security and public safety. However, this must be done by a legislative measure and even in exceptional situations the protection of personal data cannot be restricted in its entirety.[38] According to the proportionality principle, the content of the legislative measure cannot exceed what is strictly necessary to safeguard national security. Therefore, the restriction of the rights of data subjects could be justified provided that the restriction is limited to what is strictly necessary for safeguarding national security.

Sharing of customer-based (operational) data for CTF purposes facilitates analysis of suspect customers. When aggregated over a period of time, collected data can provide a detailed profile of a person's private life, including their politics, sexual orientation, medical conditions and financial status.[39] It is therefore crucial to strictly determine by a legislative measure under what circumstances and what type of personal data can be shared between public and private stakeholders for CFT purposes. For example, the Dutch taskforce underlines that they share information on specific customers only if their transactions are assessed to be suspicious and indicate potential terrorist financing activity.[40] Additionally, following the data minimisation principle, [41]personal data should be processed only if the purpose of the processing could not reasonably be achieved by other means. The responsibility to prove that processing financial personal data is crucial for national security lies with public and private sector stakeholders.

The exchange of operational information for CTF purposes raises questions around profiling. While financial profiling can help to identify common characteristics of terrorist financing, it carries the risk of profiling and discrimination based on, for example, race or religion. Therefore, if adequate control mechanisms are not established, such operational information exchange may lead to the debanking of entire groups – for example, disproportionately depriving Muslim charities banking access to carry out humanitarian activities.[42]

The Importance of Cross-Border Information Sharing

The EU Terrorism Situation and Trend Report 2022 (TE-SAT) indicates that terrorism remains a key threat to the EU's internal security, thus collective efforts to fight this threat should be intensified.[43] As terrorists and their networks send or receive funds from countries which are scattered not only throughout the EU but on a global scale, it is important to enable better cross-border terrorist-related financial flows tracking.[44] According

36. *Ibid.*
37. Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)'.
38. European Data Protection Board, 'Guidelines 10/2020 on Restrictions Under Article 23 GDPR', Version 2.0, 13 October 2021, p. 6, <https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf>, accessed 19 June 2022.
39. Amnesty International, 'Europe: Dangerously Disproportionate: The Ever-Expanding National Security State in Europe', 17 January 2017, < https://www.amnesty.org/en/documents/eur01/5342/2017/en/>, accessed 19 June 2022.
40. Belgian Senate, 'Senate Written Question No. 6-2214'.
41. Recital 39 of the Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)'.
42. Marieke de Goede, 'The Chain of Security', *Review of International Studies* (Vol. 44, No. 1, 2018), pp. 24–42.
43. Europol, *European Union Terrorism Situation and Trend Report 2022* (The Hague: European Union Agency for Law Enforcement Cooperation, 2022).
44. Riondet, 'The Value of Public-Private Partnerships for Financial Intelligence'.

to TE-SAT, terrorist organisations use national and transnational banks for transfers to accounts in and outside the EU.[45] They commonly use money transfer services, such as MoneyGram and Western Union, or informal value transfer systems, such as hawala, as well.[46] Since terrorists tend to use online payment services that are provided in different EU countries, the relevant financial transaction data may be fragmented and distributed throughout the EU and thus not readily accessible by counterterrorism authorities.[47] The majority of terrorist financing-related money flows are transnational, meaning the private and public sectors often have fragmented information. To piece this information back together requires substantial time and effort and can be undermined by a lack of cooperation between public and private sectors.[48] Therefore, cross-border cooperation and information exchange opportunities should be further explored, and potential legal gateways considered for the collaborative fight against terrorist financing to be really effective.

One of the examples that may be considered in this context is the EU–US Terrorist Finance Tracking Program Agreement, which regulates the transfer of bulk data from the Designated Provider in Europe to US authorities (US Department of the Treasury) to support the prevention, investigation, detection or prosecution of terrorism or terrorist financing.[49] This type of legal framework paves the way for the cross-border collaboration for CTF purposes between two different authorities, but it does not consider the private sector's role in it.

Conclusion

PPPs are fundamental in the effective fight against terrorist financing. They provide opportunities for a targeted and coordinated approach to the detection and disruption of terrorism financing networks and offer intelligence-led methods that deny terrorists illicit profits, material support and resources for attacks. Terrorist financing networks can only be disrupted through connecting the shared information networks of the public and private sectors. However, the appropriate balance for partnerships must be found, especially when considering operational data-sharing arrangements. Law enforcement and intelligence agencies should ensure that information-sharing arrangements with private stakeholders do not undermine their organisational integrity, personal data privacy requirements or individuals' rights. Terrorism is a global threat and it requires a collective international response. Information exchange must happen on a cross-border basis and PPPs, if constructed appropriately, can offer a solution in the fight against global terrorist financing.

Ruta Bajarunaite is an independent financial crime consultant with experience in both the public and private sectors. Her last position was at a public–private partnership in Lithuania, where she led legislative initiatives and a methodology group.

45. Europol, *European Union Terrorism Situation and Trend Report 2022.*
46. *Ibid.*
47. Riondet, 'The Value of Public-Private Partnerships for Financial Intelligence'.
48. *Ibid.*
49. Europol, 'Europol Activities in Relation to the TFTP Agreement: Information Note to the European Parliament 1 August 2010–1 April 2011', 4 August 2011, <https://www.statewatch.org/media/documents/news/2012/jun/eu-usa-tftp-europol-2012.pdf>, accessed 19 June 2022.