Islamic terrorism in Germany – The use of social network analysis to detect high-risk criminal networks

Kristin Weber ([106])

https://doi.org/10.3013/57bdcd15

Abstract

This article pays particular attention to the networks of homegrown terrorists in Germany who were engaged in conflicts and war zones in Iraq, Syria and African states by the Islamic State in Iraq and Syria (and other terrorist organisations). Based on the combination of court file and social network analysis it was possible to highlight a network of 255 people and 650 connections, the key actors and the infrastructure of the network itself. This article presents social network analysis as a possible tool for police investigations on how to identify terrorist networks as high-risk networks. Using the example of a terrorist network from Germany, it is possible to explain how terrorist networks are organised and how they can be destabilised or even disrupted. By identifying relevant key players and subgroups, their connections and positions within the network, it is possible to gain a deeper understanding of radicalisation and create more effective counterterrorism strategies.

Keywords: radicalisation, terrorism, covert networks, social network analysis, police training.

Introduction

Terrorism represents a dynamic and constantly evolving phenomenon. Security authorities and researchers continue to face major challenges in analysing and countering terrorism and radicalisation and in developing effective counterterrorism strategies. Terrorist organisations, recruitment mechanisms and narratives continually adapt to changing social and political environments. Between 2015 and 2017 ([107]), members of the Islamic State in Iraq and

([106]) The results presented are based on findings published in Weber (2023).

([107]) Terrorist acts included the following: in January 2015, attacks in Paris on Charlie Hebdo and a kosher supermarket; in November 2015, attacks in Paris on the Stade de France, bars and restaurants in the 10th arrondissement and the Bataclan theatre in the 11th arrondissement; in 2016, attacks in Brussels at Zaventem Airport and on the subway, attacks in Nice, France and at a Christmas market in Berlin, Germany; and in 2017 on Las Ramblas in Spain.

Syria (ISIS) carried out a series of terrorist attacks that profoundly affected Europe. The proclamation of the ISIS's caliphate in 2014 marked a significant turning point, sparking a wave of departures from Europe – particularly from Germany – towards war zones in Syria to join the caliphate. The Federal Office for the Protection of the Constitution estimates that over 1 060 jihadist Islamists from Germany travelled to war zones in Syria and Iraq until 2020 (the Federal Office for the Protection of the Constitution, n.d.). Many of these individuals maintained direct links to ISIS and actively engaged in combat operations. The appeal of the conflict zones and of ISIS's activities in Syria and Iraq extended far beyond Germany's borders. In 2014, approximately 1 130 individuals from France joined the conflicts in Syria and Iraq, followed by around 1 000 from Turkey, 800 from Russia, 550 from Germany, 500 from the United Kingdom and 300 each from Belgium and Sweden. From North Africa and the Middle East about 3 000 Tunisians, 2 500 Saudi Arabians, 2 090 Jordanians, 1 500 Moroccans and 890 Lebanese travelled to jihadist-held territories (cf. Salloum, 2014; Weber, 2023, pp. 31–33). Since the destruction of the caliphate in 2019, movement patterns have shifted, but ISIS has not disappeared. ISIS has retreated underground and created offshoots in different areas of the world, such as the Islamic State Khorasan Province (ISKP) in Afghanistan. Understanding the organisation's network processes, dynamics, logistics, important key players and their roles, along with detecting these covert connections, plays an important role in law enforcement and counterterrorism efforts. Strengthening investigative capacities not only requires identifying central figures and their roles but also analysing how these hidden networks operate and sustain themselves. Even after the fragmentation of ISIS in Syria, network structures and radicalisation processes continue to demand systematic research – particularly in light of ISKP's growing influence and regional expansion.

This present research ([108]) draws on a court file and social network analysis of 36 court records provided by the Federal Public Prosecutor General at the Federal Court of Justice, and other public prosecutors and the Federal Bureau of Criminal Investigation. The files offered rich insights into the radicalisation processes of the perpetrators and their network (cf. Weber, 2023, pp. 7–10).

The article highlights social network analysis as a valuable tool for law enforcement to identify and analyse underground networks, assess their risk potential and develop strategies to disrupt or destabilise them.

Data pool

This research draws on an analysis of 36 court records concerning completed legal proceedings that resulted in final convictions of the perpetrators. The dataset excludes individuals affiliated with Al-Qaeda. The analysed cases involve convictions between 2014 and 2017 for offences such as forming, participating in, or supporting a terrorist organisation abroad; preparing a serious act of violence endangering the state; establishing contacts to plan such acts; and financing terrorism ([109]). All personal identifiers of the perpetrators were anonymised to ensure confidentiality ([110]). The court files include interrogation transcripts, chat logs, telecommunications and surveillance records, arrest warrants, photographs, indictments and judgments (cf. Weber, 2023, pp. 7–10).

([108]) This research was part of the project 'X-Sonar: Extremist endeavours in social media networks: Identification, analysis and management of radicalisation processes' by the German Police University in Münster, Germany. For more information, see Weber (2023).

([109]) German Criminal Code (Strafgesetzbuch, StGB): § 129(a) StGB 'Formation of a terrorist organisation', § 129(b) StGB 'Criminal and terrorist organisations abroad', § 89(a) StGB 'Preparation of a serious act of violence endangering the state', § 89(b) 'Establishing relations for the commission of a serious act of violence endangering the state' and § 89(c) 'Financing of terrorism' (Federal Ministry of Justice, 2025). Relevant international counterterrorism frameworks include the EU Directive 2017/541 on combating terrorism (European Parliament and Council of the European Union, 2017), which harmonises legal definitions across the EU, and UN Security Council Resolutions 1373 (2001) and 2178 (2014), which establish global standards for criminalising and preventing terrorism, including the phenomenon of foreign terrorist fighters.

([110]) A comprehensive data protection framework was established and implemented throughout the X-Sonar research project and the dissertation (Weber, 2023). Measures included restricted access to case files, prohibition of third-party access, secure storage in a fireproof, lockable cabinet, the use of a coded key list for offenders and full anonymisation of offender identities. Further details are provided in Weber (2023).

The analysis identified 58 individuals (53 men and 5 women) and categorised them according to their actions.

- **Foreign terrorist fighters (*n* = 40).** These individuals travelled to war zones in Iraq, Syria or African states, received military training, and repeatedly returned to and departed from Germany.
- **Individuals intending to leave (*n* = 14).** These individuals planned to travel to war zones but were arrested or prevented from carrying out their plans.
- **Supporters (*n* = 4).** These individuals provided financial or material support (e.g. clothing) to terrorist organisations, produced propaganda and/or offered assistance to imprisoned members. They joined and supported different terrorist organisations (Jabhat al-Nusra, Jaish al-Muhajireen wal-Ansar, Jabhat al-Sham) but mostly ISIS (cf. Weber, 2023, pp. 8, 97).

All individuals investigated were affiliated with the (inter)national Salafist-jihadist milieu. The analysis shows that the individuals actively participated in Islamic seminars, Qur'an distribution campaigns and rallies organised by prominent preachers in Germany and across the EU. They also attended demonstrations, religious services, prayers and religious missionary activities. Most of them regularly frequented radical mosques and many engaged in fundraising efforts for extremist causes. Furthermore, all perpetrators were members of radical Salafist-jihadist organisations or communities based in Germany. They formed part of an international terrorist network that extended its connections to Iraq, Syria and African states (cf. Weber, 2023, pp. 156–159).

Literature review

The pioneering studies conducted by Krebs (2002), Sageman (2004), Bakker (2006), Koschade (2006), Magouirk et al. (2008), and also more recent studies by Weber and Hamachers (2020), and Weber (2023) among others exemplify the valuable use of network analysis based on open-source material and court records. Krebs (2002) conducted an analysis of open-source media to examine the communication patterns used by the al-Qaeda attackers during the World Trade Center attacks on 11 September 2001. His findings highlight the challenges of detecting covert networks and underscore the importance of identifying key actors (e.g. critical nodes, such as brokers) to effectively disrupt them. In addition, he identified not only the connections among the attackers but also the flow of information and money from other network members that supported the planning and execution of the 11 September attacks. Bakker (2006) focused on European terror networks building on Sageman's (2004) research on global terrorism. In the comparison of 172 global and 242 European terrorists he highlights their connection through kinship and friendship (Bakker, 2006). This result is also reflected in the research by Weber and Hamachers (2020) and Weber (2023).

Koschade (2006) and Magouirk et al. (2008) analysed the communication networks underlying the 2002 Bali bombings conducted by Jemaah Islamiyah. Koschade (2006) identified key players and weak points within the Jemaah Islamiyah network, demonstrating how targeting these nodes could fragment the organisation and disrupt the flow of information. He also emphasised the value of social network analysis as a tool for intelligence services. Magouirk et al. (2008) demonstrated how the network's structure shifted over time from a centralised hierarchy to a decentralised configuration, distributing critical functions across a wider set of actors.

Weber and Hamachers (2020) investigated foreign terrorist fighters from Germany by combining court record analysis and social network analysis. Their study identified three types of networks: online, offline and key-player networks, revealing the absence of a real online network and underscoring the importance of the offline sphere and active key players as critical nodes within it.

Weber (2023) applied the same methodological approach as Weber and Hamachers (2020) to examine preachers as key players and their role in the radicalisation and mobilisation of foreign terrorist fighters from Germany. She emphasised the value of social network analysis as a powerful tool for investigating underground and covert networks, particularly when using court records.

Researchers can employ this method to illuminate structures, hierarchies and key actors, and to identify strategies for weakening networks and developing effective counterterrorism measures (Mullins, 2013). However, obtaining comprehensive and reliable data, especially court records, remains a major challenge (Weber and Hamachers, 2020, p. 230).

Methodology

I employed a mixed-methods approach to analysing these files, combining qualitative content analysis by Mayring (2015), grounded theory methodology by Glaser and Strauss (1967), Strauss and Corbin's methodology (1996) and network analysis to uncover patterns and relationships (cf. Weber, 2023, pp. 90–100) ([111]).

The advantages of utilising court files are evident: experts from the police and public prosecutors meticulously collected and evaluated the data during their preliminary investigations. Consequently, they provide a wealth of detailed information, enabling in-depth individual case analyses. Combining content analysis with social network analysis proves highly beneficial in this research. It provides valuable insight into complex social processes and dynamics, such as individual radicalisation processes and group mobilisation/recruitment: why and how people became members of terrorist organisations and the international network. In addition, it allows researchers to analyse the structure of the jihadi network in Germany and its connections to members of a terrorist organisation abroad (cf. Weber, 2023, pp. 101, 106–118).

A cross-file analysis identified 255 individuals with more than 650 connections to other network actors. The analysis revealed that members of this network assumed various key roles and responsibilities to sustain and expand it (cf. Weber, 2023, pp. 263–265).

Examining the relationships (edges) between actors/individuals (nodes) within a network is the primary focus of a social network analysis (Wassermann and Faust, 1994, pp. 94–95; Weber, 2023, p. 120). A network is defined as a group of individuals who share a connection through relationships (Sageman, 2004, p. 137). The analysis treats a relationship as established when the files explicitly mention it or when the contained records provide verifiable evidence (e.g. chat records, telecommunication and observation protocols). To sum up: 'the study of networks is, in essence, the study of relationships' (Arsenault, 2011, p. 260). The size of each node reflects the strength of its connections: the larger the node, the more connections an individual has, indicating their potential significance

([111]) For more information regarding the use of content analysis and grounded theory methodology, see Weber (2023).

within the network (Figure 15.1). In any network, certain individuals play pivotal roles in its existence, maintenance, growth and overall success (cf. Weber, 2023, pp. 121–124). These roles include group or organisation leader, recruiter, preacher, propagandist, trafficker, marriage broker, recruits, organisers of a terroristic attack, terrorist attacker/assassins, supporter, contact person and exit supporter (cf. Weber, 2023, pp. 121–124).

The position of a node within the network matters too: the more central the node, the higher its importance. A node positioned at the centre of the network suggests that the individual may play a key role, potentially acting as a central figure within the network. Nodes located on the periphery can also hold significant importance. These actors function as critical nodes and fulfil different roles, such as controlling the flow of information or serving as informational hubs for subgroups distant from the centre (Figure 15.1). Such nodes facilitate the flow of information between different parts of the network and even influence its dynamics (cf. Weber, 2023, pp. 290–291). To identify critical nodes within a network, statistical measures are important.

I visualised the network with the software Gephi (Bastian et al., 2009), applying the Fruchterman–Reingold algorithm (Fruchterman and Reingold, 1991), combined with the no-overlap function. This algorithm ensures a clear arrangement of nodes, positioning those with connections closer together. This approach helps to identify distinct network structures and subgroups effectively. By using statistical centrality measures (degree, betweenness and closeness) provided by Gephi, it is possible to analyse the structure and even key players within the network (cf. Weber, 2023, pp. 121–124).

Centrality provides insights into the significance of nodes within a network, including their number of connections, the extent to which they are connected with other members, and their influence or control over the flow of information. Degree centrality represents the number of connections of a node. This number allows for determining how important a node is for the network. Betweenness centrality is a common measure used to identify potential influencers within a network. Closeness centrality gives information about how close a node is to all other nodes in the network. This measure ranges from 0 to 1. Values close to 1 indicate that nodes (individuals) are central in the network and are close to most other nodes. Values close to 0 indicate that nodes (individuals) lie far from the centre and require more steps to connect with other members of the network. Nodes with higher closeness measures are able to communicate and share information more easily because they are close to other nodes (Chau and Xu, 2007; see Medina, 2014; Fuhse, 2016; Weber and Hamachers, 2020; Weber, 2023, pp. 121–124, 290–291).

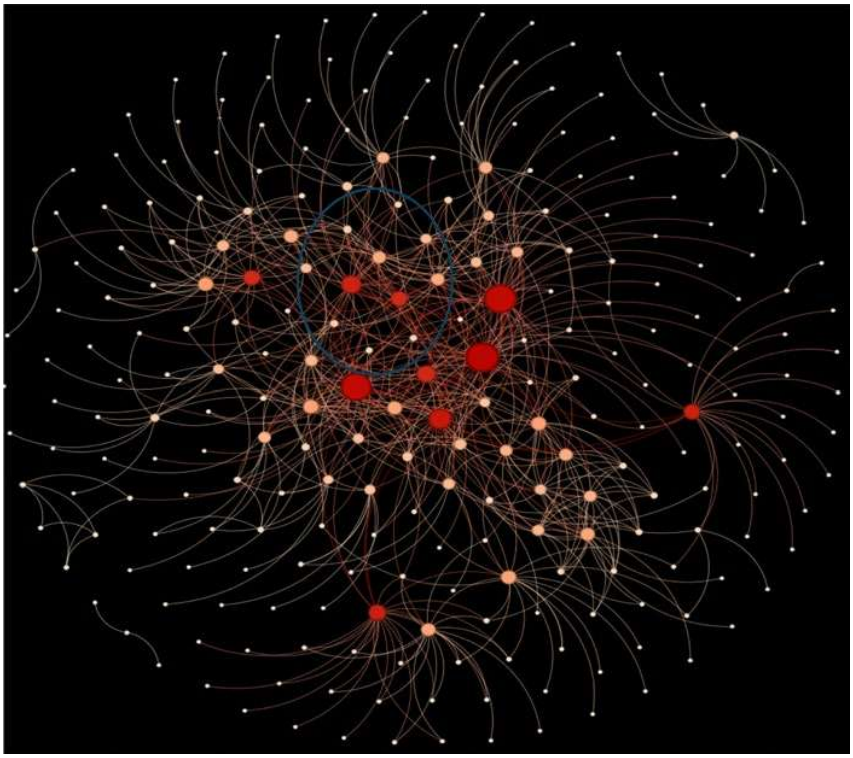

Figure 15.1. Visualised network by Gephi
NB: Fruchtermann–Reingold logarithm, no overlap.
Source: Weber, 2023.

The figure shows the complete network identified by Weber (2023). It shows a number of nodes and connections, differentiating central nodes and nodes in the periphery. Nodes with a higher degree (number of connections) are bigger than nodes with fewer connections. The blue oval highlights as an example a subgroup that will be explained next. Figure 15.1 is based on Weber (2023).

By identifying key players, such as information hubs or bridging nodes (bridges) linking peripheral and central positions, it becomes possible to strategically destabilise or disrupt the network by isolating or removing these crucial individuals. The fragmentation of the network or a slowing down in its information dynamic could result by removing important key players.

Even nodes positioned at the periphery or those without direct connections can play pivotal roles within the network. Some actors may actively cut their ties to conceal their activities, resulting in nodes that appear isolated. Peripheral nodes with long-distance connections can function as covert intermediaries, hubs, bridges or supporters, linking actors between the network's centre and its periphery.

Although this paper provides relevant insights on social network analysis and the connection between different actors in the network, it focuses on directly connected nodes and their surroundings ([112]). However, it provides a useful initial

([112]) For more information about nodes in the periphery and long-distance connections, see Weber and Hamachers (2020), Weber (2023).

heuristic for risk assessment. Focusing only on direct connections may overlook indirect relational pathways through which information, resources or influence circulate within terrorist networks. Future analyses should therefore consider higher-order connections to capture the broader structural risks embedded in indirect ties, adopting a multilevel network perspective (e.g. k-step neighbourhoods: explaining indirect range and influence of an actor). Using social network analysis combined with qualitative material, such as court records, like Weber (2023), within an interdisciplinary team (security authorities, researchers, prosecutors) can heighten the validity and the results of the analysis.

Results

To better understand the strategy of detecting and removing key players, we can take a closer look at a subnetwork of active recruiters (SR49 ([113]), SR50, SR51, SR52) as an example (blue oval, Figure 15.1, zoom: Figure 15.2) (cf. Weber, 2023, pp. 292, 297–300).

Figure 15.2. Zoom on SR49–SR52 and their connections

NB: Füh indicates leaders; P, preacher; R, recruits; and U, supporters. The filter applied is an ego network focus on SR49.

In terms of centrality measures, SR49 and SR52 score high, SR50 mediocre and SR51 low (Table 15.1).

Table 15.1. Centrality measures for SR49–SR52

Name	Degree	Betweenness	Closeness
SR49	23	1 999.00	0.40233
SR52	21	1 235.25	0.38746
SR50	15	243.442	0.34877
SR51	13	456.79	0.37774

Source: The statistical values used in this analysis are based on findings published in Weber (2023, p. 292).

([113]) SR stands for Syria returnee (foreign terrorist fighter). This abbreviation is part of the strategy to anonymise all perpetrators.

These four nodes occupy peripheral positions within the network but remain relatively easy to access (closeness). It is important to note at this point that SR49, SR50 and SR52 shared kinship ties. SR49 and SR52 demonstrate strong connectivity within the network, with degree ([114]) values of 23 and 21, respectively, indicating high levels of activity. SR49, in particular, exhibits a high betweenness centrality, highlighting his significant role as an intermediary within the network. This makes SR49 crucial for the flow of information (hub), as many connections pass through him. His strong integration into the network's core is evident through links to SR45 and P4 (see Figure15.1 and Figure15.2) (Weber, 2023, pp. 298–299). SR49 acts as a critical bridge into jihad (cf. Sageman, 2004, p. 169; Weber, 2023, p. 299).

The analysis of connections involving SR49, SR50, SR51 and SR52 reveals that SR49 maintains close links to a subnetwork of recruits. Court file analyses confirm SR49's active role as a recruiter for ISIS, directly engaging with 10 recruits. He facilitated their recruitment into violent jihad and ISIS operations by providing guidance on how and when to leave the country to join ISIS. Among these recruits were four young men (R1, R6, R7 and R9) who later died in Syria while fighting for ISIS. SR49, together with SR50 and SR52, played a crucial role in enabling these individuals to join ISIS and therefore bear direct responsibility for the deaths of these recruits (cf. Weber, 2023, pp. 289–299).

Disrupting the subnetwork formed by SR49, SR50 and SR52 could have prevented the departure of these 10 young men, or possibly more, since the exact total remains uncertain. Targeting SR49, SR50 and SR52 would likely have dismantled the network because they maintained direct links to Preacher 4 (P4). P4, as the central figure in the network, belonged to ISIS and provided multifaceted support, including facilitating departures, mediating contacts and issuing letters of recommendation ([115]). Severing the links from SR49, SR50 and SR52 to P4 would have cut the network off from crucial information (cf. Weber, 2023, pp. 292–303).

Conclusion and implications

Using a social network analysis can be beneficial for security authorities and researchers. It enables the identification, visualisation and assessment of relationships and structures within a network, helping to uncover hidden support systems, trace flows of information and resources, and improve inter-agency communication, for example, by exploring links between organised crime and the financing of terrorism.

Numerous studies have demonstrated the practical benefits of applying social network analysis in counterterrorism contexts. Krebs (2002), for example, revealed the structural vulnerabilities of the 11 September al-Qaeda network and showed how information sharing across agencies could generate a more comprehensive understanding of potential threats – an observation that remains highly relevant today. Similarly, Koschade (2006) and Magouirk et al. (2008) illustrate how the disruption of key intermediaries can significantly reduce an organisation's operational capacity. In a European context, Bakker (2006) and Sageman (2004, 2008) highlighted the decentralised but resilient structure of jihadist networks, informing strategies that prioritise disruption over dismantlement. More recent research in Germany (Weber and Hamachers, 2020; Weber, 2023) applied social network analysis to court records of foreign terrorist fighters from Germany and their connections to ISIS, revealing radicalisation and recruitment strategies, and the pivotal role of radical preachers. Collectively, these studies underscore the continued value of

([114]) Number of connections.
([115]) For more information about criminally relevant actions of P4, see Weber (2023).

social network analysis for identifying key actors, mapping hidden infrastructures and designing targeted prevention and disruption strategies in the fight against terrorism.

Social network analysis reveals the underlying social structures that shape (inter)actions among individuals within terrorist networks and provides insights into the overall behaviour and dynamics of the network. It provides a deeper understanding of how a covert network operates, identifies significant key players and reveals how different members contribute in various roles to its persistence and growth. It also exposes the structural vulnerabilities of covert networks and provides strategies to target critical points, enabling their disruption or even complete dismantling. By pinpointing and targeting key players, analysts can disconnect actors and subnetworks from the network's core and its strategically relevant members. This approach disrupts the flow, exchange and dynamics of information and can ultimately fragment the network. However, because networks are inherently dynamic and adaptive, other members may quickly replace removed actors. Future research should therefore focus on monitoring structural changes over time to detect reconfigurations after interventions and anticipate new or renewed mobilisation efforts, especially on social media ([116]).

Another benefit of applying social network analysis lies in its ability to enhance understanding of recruitment strategies and processes. Specifically, how individuals become integrated into radical milieus and, consequently, into broader networks (e.g. Weber, 2023). Such insights enable the development of more effective prevention and counterterrorism strategies. To leverage these capabilities effectively, security agencies need continuous training in social network analysis, expertise in managing big data and access to advanced analytical software tools. Recent developments in Horizon 2020 projects, such as Appraise (facilitating public and private security operators to mitigate terrorism scenarios against soft targets) ([117]) (European Commission, 2021), demonstrate how the integration of new technologies, including AI-supported network analytics and automated risk assessment frameworks, can further enhance the detection, monitoring and disruption of terrorist networks.

However, one limitation of this approach lies in the exclusive consideration of 'next neighbours' when assessing risk. Focusing only on direct connections may overlook indirect relational pathways through which information, resources or influence circulate within terrorist networks. Future analyses should therefore consider higher-order connections to capture the broader structural risks embedded in indirect ties.

References

Arsenault, A. (2011), 'Networks: The technological and the social', in Delanty, G. and Turner, S. (eds) *Handbook of Contemporary Social and Political Theory*, Routledge, London, pp. 259–269.

Appraise Consortium (2024), "Appraise achievements – Plot summaries and key results', Horizon 2020 Research and Innovation Programme (grant agreement No 101021981), https://appraise-h2020.eu/sites/default/files/2024-02/APPRAISE %20Brochure %20 %28website %29.pdf.

([116]) When using social media data for network analysis, researchers must be aware of legal restrictions and data protection regulations, including the safeguarding of personal rights and privacy.

([117]) Appraise (Horizon 2020 project, grant agreement No 101021981) develops AI-driven analytics and collaborative decision-support tools to strengthen counterterrorism capabilities and protect public spaces across Europe (cf. European Commission, 2021; Appraise Consortium, 2024).

Bakker, E. (2006), *Jihadi Terrorists in Europe – Their characteristics and the circumstances in which they joined the jihad: An exploratory study*, Netherlands Institute of International Relations Clingendael, The Hague.

Bastian, M., Heymann, S. and Jacomy, M. (2009), 'Gephi: An open-source software for exploring and manipulating networks', in: *Proceedings of the Third International AAAI Conference on Weblogs and Social Media* (ICWSM'09), AAAI Press, San Jose, pp. 361–362.

Chau, M. and Xu, J. (2007), 'Mining communities and their relationships in blogs: A study of online hate groups', *International Journal of Human-Computer Studies*, Vol. 65, No 1, https://doi.org/10.1016/j.ijhcs.2006.08.009.

European Commission (2021), 'Appraise: fAcilitating Public and Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts', European Commission website, https://cordis.europa.eu/project/id/101021981.

European Parliament and Council of the European Union (2017), Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, p. 6, ELI: http://data.europa.eu/eli/dir/2017/541/oj).

Federal Ministry of Justice (Germany) (2025), German Criminal Code (Strafgesetzbuch, StGB), https://www.gesetze-im-internet.de/stgb.

Federal Office for the Protection of the Constitution (no date), Daten und Fakten, https://www.verfassungsschutz.de/DE/themen/islamismus-und-islamistischer-terrorismus/zahlen-und-fakten/zahlen-und-fakten_node.html#doc678982bodyText4.

Fruchterman, T. M. J. and Reingold, E. M. (1991), 'Graph drawing by force-directed placement', *Software: Practice and Experience*, Vol 21, No 11, pp. 1129–1164, https://doi.org/10.1002/spe.4380211102.

Fuhse, J. (2016), *Soziale Netzwerke: Konzepte und Forschungsmethoden*, 1st Kindle edition, UVK Verlagsgesellschaft mbH, Konstanz.

Glaser, B. G. and Strauss, A. L. (1967), The Discovery of Grounded Theory, Aldine, Chicago.

Koschade, S. (2006), 'A Social Network Analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence', *Studies in Conflict and Terrorism*, Vol. 29, pp. 559–575.

Krebs, V. E. (2002), 'Mapping networks of terrorist cells', Connections, Vol. 24, No 3, pp. 43–53.

Magouirk, J., Atran, S. and Sageman, M. (2008), 'Connecting terrorist networks', *Studies in Conflict and Terrorism,* Vol. 31, No 1, pp. 1–16, https://doi.org/10.1080/10576100701759988.

Mayring, P. (2015), *Qualitative Inhaltsanalyse: Grundlagen und Techniken*, 12th edition, Beltz Verlag, Weinheim.

Medina, R. M. (2014), 'Social Network Analysis: A case study of the Islamist terrorist network', Security Journal, Vol. 27, No 1, pp. 97–121, https://doi.org/10.1057/sj.2012.21.

Mullins, S. (2013), 'Social network analysis and counter-terrorism: Measures of centrality as an investigative tool', *Behavioral Sciences of Terrorism and Political Aggression*, Vol. 5, No 2, pp. 115–136, https://doi.org/10.1080/19434472.2012.718792.

Sageman, M. (2004), *Understanding Terror Networks*, University of Pennsylvania Press, Philadelphia.

Sageman, M. (2008), *Leaderless Jihad: Terror networks in the twenty-first century, University of Pennsylvania Press, Philadelphia*.

Salloum, R. (2014), 'Rekruten für den Islamischen Staat: Die Weltkarte des Terrors', *Der Spiegel*, 28 November, https://www.spiegel.de/politik/ausland/is-islamischer-staat-zehntausende-auslaendische-kaempfer-machen-mit-a-1001193.html#bild-e3b6d3b3-0001-0004-0000-000000782535.

Strauss, A. and Corbin, J. (1996), *Grounded Theory: Grundlagen Qualitativer Forschung*, Beltz Verlag, Weinheim.

United Nations Security Council (2001), Resolution 1373 (2001), Adopted by the Security Council at its 4385th meeting, on 28 September 2001, United Nations, https://undocs.org/S/RES/1373(2001).

United Nations Security Council (2014), Resolution 2178 (2014), Adopted by the Security Council at its 7272nd meeting, on 24 September 2014, United Nations, https://undocs.org/S/RES/2178(2014).

Wasserman, S. and Faust, K. (1994), *Social Network Analysis: Methods and applications*, Cambridge University Press, Cambridge, https://doi.org/10.1017/CBO9780511815478.

Weber, K. (2023), *Islamistischer Terrorismus in Deutschland: Analyse der Täterprofile deutscher Syrienrückkehrer auf Basis von Gerichtsakten*, Springer, Berlin, https://doi.org/10.1007/978-3-658-42830-3.

Weber, K. and Hamachers, A. (2020), 'Aus dem radikalen Netzwerk in den Jihad: Radikale Prediger als Schlüsselakteure im Umfeld deutscher Syrienreisender', in: Hamachers, A., Weber, K. and Jarolimek, S. (eds), Extremistische Dynamiken im Social Web: Forschungsbefunde zu den digitalen Katalysatoren politisch und religiös motivierter Gewalt, Verlag für Polizei und Wissenschaft, Frankfurt am Main, pp. 225–270.