Social network analysis and counterterrorism : a double-edged sword for international humanitarian law

Moncrieff, Michael Arthur; Kilibarda, Pavle; Gaggioli Gasteyger, Gloria

How to cite

MONCRIEFF, Michael Arthur, KILIBARDA, Pavle, GAGGIOLI GASTEYGER, Gloria. Social network analysis and counterterrorism : a double-edged sword for international humanitarian law. In: Journal of conflict and security law, 2024, p. 19. doi: 10.1093/jcsl/krae002

This publication URL: https://archive-ouverte.unige.ch/unige:175845

Publication DOI: 10.1093/jcsl/krae002

Journal of Conflict & Security Law, 2024, 1–19
https://doi.org/10.1093/jcsl/krae002
Article

Social network analysis and counterterrorism: a double-edged sword for international humanitarian law

Michael Moncrieff [*], Pavle Kilibarda [†], Gloria Gaggioli[‡]

[*]Michael Moncrieff, Department of International Public Law & International Organization, University of Geneva, Geneva, Switzerland; Geneva Academy of International Humanitarian Law and Human Rights, Geneva, Switzerland. Email: michael.moncrieff@unige.ch
[†]Pavle Kilibarda, Department of International Public Law & International Organization, University of Geneva, Geneva, Switzerland; Geneva Academy of International Humanitarian Law and Human Rights, Geneva, Switzerland. Email: pavle.kilibarda@unige.ch
[‡]Gloria Gaggioli, Department of International Public Law & International Organization, University of Geneva, Geneva, Switzerland; Geneva Academy of International Humanitarian Law and Human Rights, Geneva, Switzerland. Email: gloria.gaggioli@unige.ch

Abstract

The use of social network analysis (SNA) during the War on Terror has been a topic of significant political and academic discourse. SNA is an empirical method that graphically and mathematically represents interactions or relationships between nodes (eg, individuals, organizations) and the ties that connect them. The nature and degree of interdependence among nodes are believed to provide insights into the relationships and behaviour of members within a social network. The scarcity of precise and comprehensive data on the structure, functioning, and activities of terrorist groups has prompted some states to incorporate SNA into their intelligence efforts and rely on its data for counterterrorism activities, including lethal operations. However, the compatibility of SNA with international law remains underexplored. In this article, we adopt a legal-empirical approach to elucidate SNA in accessible terms and examine the challenges it presents for international law. We contend that SNA is fundamentally incompatible with international humanitarian law (IHL) targeting rules, as the data it provides do not pertain to legally relevant criteria. Nevertheless, SNA offers valuable insights for IHL by illuminating intra-group dynamics to facilitate conflict classification, identifying legally relevant characteristics in armed groups' internal networks, and determining the strength of relations between armed factions. Our findings underscore the importance of a nuanced understanding of SNA's applications and limitations in the context of international law.

Keywords: social network analysis; international humanitarian law; organized armed groups; armed conflict; terrorism.

Introduction

Modern jihadist armed groups, such as central al-Qaeda, al-Shabaab, and Boko Haram—all of which have been described as organized armed groups (OAGs) under international humanitarian law (IHL)—challenge the traditional approach to counterterrorism operations by introducing the language, concepts, and legal authority of war and armed conflict. Before the 9/11 attacks, terrorist organizations were largely seen as criminal groups—albeit particularly dangerous ones—that were properly dealt with by law enforcement and not under the conduct of hostilities paradigm. Groups designated as terrorists by one or more governments, such as the 'Red Army Faction' or the 'Red Brigades' in Europe, had been constituted as clandestine networks whose primary purpose was to engage in sporadic acts of violence intended to spread terror among the population and pressure governmental authorities to comply with their demands; they were neither conceived nor structured as paramilitary forces intended to engage in hostilities. IHL applies to situations of armed conflict: if one or more of the parties to an armed conflict is a non-state actor, then the conflict will be of a non-international character.

The existence of a non-international armed conflict requires the presence of fighting of a certain intensity and a sufficient degree of group organization, typically demonstrated by a hierarchical structure and the existence of a chain of command.[1] The applicability of IHL has significant implications for the rules on targeting and detention: for example, unlike the rules on law enforcement, IHL does not require that lethal force be employed only as a measure of last resort when confronting 'fighters' belonging to an OAG.

Whether and under what circumstances groups established for the primary purpose of engaging in acts of terrorism could meet the criteria for an 'OAG' is a complex question. The structure and functioning of terrorist groups are often opaque, decentralized, and volatile—with groups constantly splintering and reuniting—and their cells may operate across state boundaries. Rather than functioning as hierarchical organizations, contemporary jihadist groups are thus typically described as 'networks.'[2] More sophisticated empirical tools are needed to evaluate a terrorist group's intra- and inter-organizational qualities to determine whether it may be considered an OAG under international law, especially if it possesses a networked structure.[3] Not only would this be important to determine whether a given terrorist group may be considered an OAG in the first place, but it can also be both conceptually and factually challenging to ascertain who may be considered a member and who may be targeted according to the law of war.

The opaqueness of terrorist organizations—whether OAGs or not—has therefore induced states to resort to more creative means of identifying and evaluating their structure and the relations that ultimately shape it. One such popular tool is *social network analysis* (SNA), initially devised by sociologists to investigate social structures composed of various individuals and groups outside the context of armed conflict or counterterrorism. Currently, supported by vast amounts of digital metadata,[4] SNA is widely used in counterinsurgency and counterterrorism operations. Within the US military, 'the adoption of network-centric targeting and exploitation […] dominate[s] much of the use of military power and weaponry today',[5] and among Special Operations Forces, there is '[…] a continuing preference for countering threat networks as a mainstay or approach to victory'.[6]

[1] See Robert Kolb and Richard Hyde, *An Introduction to the International Law of Armed Conflicts* (Bloomsbury Publishing 2008) 74–75; Marco Sassòli, 'International Humanitarian Law' [2019] International Humanitarian Law; Gloria Gaggioli and Pavle Kilibarda, 'Counterterrorism and the Risk of Over-Classification of Situations of Violence' (2021) 103 International Review of the Red Cross 203; *Prosecutor v Duško Tadić [Decision]* [1995] United Nations International Criminal Tribunal for the former Yugoslavia IT-94-1 [70].

[2] Peter Margulies, 'Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Groups"' (2013) 89 International Law Studies 22; Eric T Jensen, 'Targeting of Persons and Property' [2015]; Geoffrey S Corn and others, *The War on Terror and the Laws of War: A Military Perspective* (OUP 86); Phil Williams, 'Transnational Criminal Networks' in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND 2001) 61; Rohan Gunaratna and Aviv Oreg, 'Al Qaeda's Organizational Structure and Its Evolution' (2010) 33 Studies in Conflict & Terrorism 1043.

[3] While debates surrounding the question of what factors constitute an armed group or membership therein abound in the literature, specifically addressing these debates is beyond the scope of this article.

[4] Vasja Badalič, 'The Metadata-Driven Killing Apparatus: Big Data Analytics, the Target Selection Process, and the Threat to International Humanitarian Law' [2023] Critical Military Studies 1, vii.

[5] Peter Mccabe (ed), *The Network Illusion: How a Network-Centric Special Operations Culture Impedes Strategic Effect* (Joint Special Operations University 2022) vii

[6] Charles Black, 'Intervening Against Systemic Level Challenges for Strategic Effect' in Peter Mccabe (ed), *The Network Illusion: How a Network-Centric Special Operations Culture Impedes Strategic Effect* (Joint Special Operations University 2022) 130

This article discusses the role that the concept of networks, in general, and SNA, in particular, have played in the War on Terror since the 9/11 terrorist attacks in political discourse and counterterrorism operations. SNA has been used as a tool to identify the organizational level and borders of designated terrorist groups, including those that are also widely considered OAGs under IHL, and to identify their members. This article aims to describe how SNA has been used to make legally relevant determinations, ascertain its precision and accuracy in this regard, and map situations and issues to which it may be applied safely and purposefully. While existing literature has explored the humanitarian impacts of SNA, such as the risk of targeting civilians, or discussed the theoretical limitations and boundaries of SNA, a crucial gap remains in understanding how these limitations translate into adverse decision making. Our article uniquely employs a first-principles approach to deconstruct the reasons behind SNA's shortcomings, illustrating the link between these limitations and the resulting humanitarian consequences. To that end, it is primarily tailored for an audience of policymakers, investigators, intelligence community members, and military and security forces who use or are considering SNA in counterterrorism operations. The discussion may also be relevant to IHL specialists interested in an important contemporary form of information gathering and analysis that impacts the implementation of and respect for the law of armed conflict. Bearing in mind the breadth and diversity of our intended audience, we describe both SNA and the relevant IHL concepts using, as far as possible, non-specialist language. Although the article primarily addresses the use of SNA in relation to OAGs that are also designated as terrorists by one or more governments or the United Nations Security Council, our conclusions regarding the advantages and disadvantages of this tool may also apply to more 'traditional' OAGs.

This article uses the term 'organized armed group' to refer to groups that meet the criteria set out in IHL and may be regarded as belligerent parties to an armed conflict. The unqualified term 'armed' or 'militant group' includes OAGs but also other armed non-state actors that are not necessarily involved in an armed conflict in the legal sense. By 'terrorist groups' or 'designated terrorist groups' we refer to groups and organizations officially designated as terrorists by the United Nations Security Council or one or more governmental authorities.

What is SNA?

SNA is the graphical and mathematical representation of dyadic interactions or relations. A social network consists of *nodes* representing individuals, groups, or other data points and *ties* representing interdependences between the nodes (eg, kinship, friendship, cooperation, communication). Figure 1 shows an example of a simple social network where arrows represent either one-way information flows (eg, actor J provides information to actor F) or two-way flows (eg, actor A and B exchange information) between 10 nodes. Such interdependences between nodes are assumed to explain something about the network members and how they behave above and beyond individual attributes or characteristics.[7] A fundamental aspect of network theory is its focus on relationships to explain individual and network outcomes.[8]

There are quantitative tools and concepts in network analysis that allow nodes or networks to be analysed and compared. For instance, the *degree* centrality of a node refers to the number of ties it has with other nodes in the network (in Figure 1, actor D has the highest degree centrality). Comparing degree centrality measures can help identify actors with

[7] Stephen P Borgatti and others, 'Network Analysis in the Social Sciences' (2009) 323 Science 892; Stephen P Borgatti and Daniel S Halgin, 'On Network Theory' (2011) 22 Organization Science 1168.

[8] Stephen P Borgatti, Daniel J Brass and Daniel S Halgin, 'Social Network Research: Confusions, Criticisms, and Controversies' in Daniel J Brass and others (eds), *Research in the Sociology of Organizations*, vol 40 (Emerald Group Publishing Limited 2014).

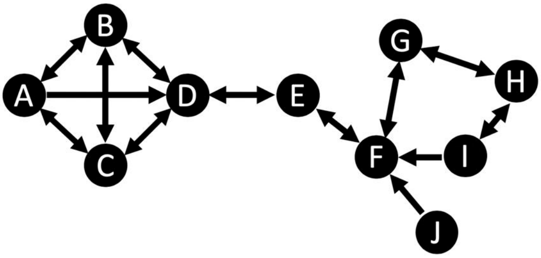

Figure 1. A simple social network.

greater influence or prominence in the network. Comparing measures of *betweenness* centrality at the node level identifies actors in a network that act as bridges or 'brokers' between subsets of nodes within the network (in Figure 1, actors E and D serve as brokers). Such bridging ties are essential for accessing novel ideas, information, and skills that might be otherwise inaccessible within one's immediate network or group.[9] Other measures examine network characteristics such as *density*, the observed number of ties divided by the total possible ties in a network, which serves as a measure of the connectedness of a network (in Figure 1, A, B, C, and D have higher density when compared to nodes F, G, H, I, and J). These metrics, among many others, allow analysts to identify individuals within militant networks with social influence or better understand militant group decision-making processes.[10]

SNA on terrorist groups has recently proliferated.[11] Most network studies use open-source data (eg, news publications, legal briefs) or law enforcement interviews to map ties between *individuals* at the *intra*organizational level or between *groups* at the *inter*organizational level.[12] Of the studies that map intraorganizational ties, most focus on mapping the relations of those individuals involved in specific terrorist attacks, armed group organization, or the networks surrounding particular individuals, that is ego networks.[13] Network analysis research is either descriptive in nature—mapping and describing the characteristic properties of specific militant networks—or analytical—testing variables that predict network properties or how network properties affect outcome variables.[14] Descriptive research predominated early attempts to understand the structure and functioning of terrorist networks.

The use of SNA by states and state practice

The USA and other countries have widely used network analysis to combat terrorism, crime networks, and terrorist groups.[15] Its application can be traced back to World War II

[9] Mark S Granovetter, 'The Strength of Weak Ties' in Samuel Leinhardt (ed), *Social Networks* (Academic Press 1977).

[10] Steven T Zech and Michael Gabbay, 'Social Network Analysis in the Study of Terrorism and Insurgency: From Organization to Politics' (2016) 18 International Studies Review 214.

[11] ibid.

[12] Marie Ouellet, 'Terrorist Networks and the Collective Criminal Career: The Relationship between Group Structure and Trajectories' (Dissertation, Simon Fraser University 2016) 11.

[13] ibid.

[14] ibid 12.

[15] Steve Ressler, 'Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research' (2006) 2 Homeland Security Affairs 10; Brian J Reed and David R Segal, 'Social Network Analysis and Counterinsurgency Operations: The Capture of Saddam Hussein' (2006) 39 Sociological Focus 251; Gareth Porter, 'How McChrystal and Petraeus Built an Indiscriminate "Killing Machine"' (*Truthout*, 26 September 2011) <https://truthout.org/articles/how-mcchrystal-and-petraeus-built-an-indiscriminate-killing-machine/> accessed 21 February 2020; Matthew Charles Ford, 'Finding the Target, Fixing the Method: Methodological Tensions in Insurgent Identification' (2012) 35 Studies in Conflict & Terrorism 113; Kate Clark, 'The Takhar Attack: Targeted Killings and the Parallel Worlds of US Intelligence and Afghanistan' (Afghanistan Analyst Network 2011) <http://

when the USA began scrutinizing foreign governments' communication and operational networks.[16] Early conceptions of networks as integral to the global terrorist phenomenon emerged with Sterling's controversial[17] book The Terror Network,[18] which influenced Reagan administration policymaker thinking.[19]

Later, scholars like Sparrow[20] and Krebs[21] argued that intelligence agencies should use network analysis to combat terrorist networks, popularizing the technique.[22] With the War on Terror, Ressler[23] noted the need for 'a new type of intelligence' incorporating social network theory and methods. The rise of information and communication technology is thought to have contributed to less hierarchical command structures and greater decentralization in modern militant groups.[24] State intelligence analysts now employ network analysis to better understand terrorist, militant, and crime networks,[25] using measures like degree centrality and betweenness centrality[26] to determine central actors and brokers whose removal might disrupt network capabilities.[27]

Network analysis played a critical role in locating Saddam Hussein in 2003[28] and was successful in assisting US counterinsurgency troops in Iraq.[29] However, in Afghanistan, leaders prioritized intelligence generated using network analysis over traditional on-the-ground intelligence techniques.[30] A reduction in intelligence resources to help target combatants outside of International Security Assistance Force-controlled areas (the NATO-led military mission in Afghanistan) resulted in an increased reliance on network analysis.[31] The military collected large amounts of data under 'signals intelligence' programmes to locate targets by tracking cell phone mobile traffic, SIM card locations, and monitoring with drone surveillance.[32] Network analysis tracked individuals who communicated with suspected militants or visited an area under drone surveillance.[33] While traditional intelligence

www.afghanistan-analysts.org/wp-content/uploads/downloads/2012/10/20110511KClark_Takhar-attack_final.pdf> accessed 21 February 2020; Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' *The Guardian* (London, 5 June 2013) <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed 20 February 2020; Ryan Lizza, 'State of Deception: Why Won't the President Rein in the Intelligence Community?' *The New Yorker* (New York, 2013) 21.

[16] Ressler ibid.

[17] Much of the book was ultimately dismissed as propaganda. For a discussion, see Edward S Herman, *The Real Terror Network: Terrorism in Fact and Propaganda* (South End Press 1982).

[18] Claire Sterling, *The Terror Network: The Secret War of International Terrorism* (Weidenfeld and Nicolson 1981).

[19] Ressler (n 15); Cynthia Stohl and Michael Stohl, 'Networks of Terror: Theoretical Assumptions and Pragmatic Consequences' (2007) 17 Communication Theory 93.

[20] Malcolm K Sparrow, 'The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects' (1991) 13 Social Networks 251.

[21] Valdis Krebs, 'Mapping Networks of Terrorist Cells' (2002) 24 Connections 43; 'Uncloaking Terrorist Networks' (*First Monday*, 1 April 2002) <https://journals.uic.edu/ojs/index.php/fm/article/download/941/863?inline=1> accessed 10 February 2020.

[22] Ressler (n 15); Stohl and Stohl (n 19).

[23] Ressler (n 15).

[24] Zech and Gabbay (n 10).

[25] Morgan Burcher and Chad Whelan, 'Social Network Analysis and Small Group "Dark" Networks: An Analysis of the London Bombers and the Problem of "Fuzzy" Boundaries' (2015) 16 Global Crime 104.

[26] ibid; Kathleen M Carley, 'Destabilization of Covert Networks' (2006) 12 Computational and Mathematical Organization Theory 51; Stuart Koschade, 'A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence' (2006) 29 Studies in Conflict & Terrorism 559.

[27] Note that other, more sophisticated approaches to removing key actors to disrupt networks are now discussed. John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Ivan R Dee, Inc 2008); Sean F Everton, 'Disrupting Dark Networks' (*Cambridge Core*, November 2012) </core/books/disrupting-dark-networks/1F2BFFEA7C036EC7CFD0ED1FFDAE21D7> accessed 20 February 2020; Nancy Roberts and Sean F Everton, 'Strategies for Combating Dark Networks' (2011) 12 Journal of Social Structure 1.

[28] Reed and Segal (n 15).

[29] Ford (n 15).

[30] ibid.

[31] ibid 123.

[32] Porter (n 15); See also, Badalič (n 4).

[33] Porter (n 15).

techniques would have involved verifying the nature of relationships, increasing demand to strike targets quickly precluded such intelligence from being gathered.[34] As Clark[35] reports, the United States Special Operation Officer in Afghanistan explained, ‘If we decide he’s [a surveyed individual] a bad person, the people with him are also bad.’ Such network-guided targeting led to the deaths of many civilians.[36] The scope of using network analysis for targeting purposes was vast. Indeed, Scahill[37] discusses how the majority (~90 per cent) of drone and night raid operations used cell data and other communications intelligence to target high-value individuals. Ford[38] discusses how too strong a focus on network analysis in Afghanistan led to intelligence officers overlooking community political processes and local social capital, which could have led to peace talks and reconciliation.

Domestically, the Obama administration expanded the National Security Agency’s phone and Internet surveillance programmes.[39] More recently, the USA used network analysis to understand which non-jihadist armed groups involved in the Syrian Resistance movement it could cooperate with to further its policy objectives by preventing the spread of Syrian chemical and biological weapons to jihadist terrorists.[40] However, this particular application of network analysis was criticized for its improper focus on central network actors while ignoring those in the periphery network.[41] Those subnetworks would later align with the Islamic State in Syria against the USA,[42] thus hindering the USA’s efforts. Other countries have also utilized network analysis for similar purposes. Mac Ginty[43] discusses its role in Sri Lanka’s military offensive against the Tamil Tigers, helping identify connections between prominent members and potentially supportive ancillary individuals. Network analysis has also been used in counterterrorism efforts as part of law enforcement operations in various states.[44]

Within the current framework of US military doctrine, the significance of SNA and the strategy of ‘countering threat networks’ remain paramount.[45] The trend towards a network-centric approach has transformed how targeting and weapons deployment are conducted across all military services.[46] In the era of digital advancement, militaries, aided by emerging technologies, continue to work to identify and target combatants operating in covert networks.[47] As noted by the former director of the CIA and NSA, ‘We kill people

[34] Clark (n 15); Ford (n 15); Porter (n 15).

[35] Clark (n 15) 30.

[36] Vasja Badalič, *The War Against Civilians: Victims of the “War on Terror” in Afghanistan and Pakistan* (Palgrave Macmillan 2019).

[37] Jeremy Scahill, *The Assassination Complex: Inside the Government’s Secret Drone Warfare Program* (Simon and Schuster 2017) 99.

[38] Ford (n 15) 126.

[39] Greenwald (n 15).

[40] Seth Lucente and Gregory Wilson, ‘Crossing the Red Line: Social Media and Social Network Analysis for Unconventional Campaign Planning’ [2013] *Special Warfare* 22.

[41] Nancy Roberts and Sean Everton, ‘Monitoring and Disrupting Dark Networks: A Bias Toward the Center and What It Costs Us’ in Alexander R Dawoody (ed), *Eradicating Terrorism from the Middle East* (Springer International Publishing 2016).

[42] ibid.

[43] Roger Mac Ginty, ‘Social Network Analysis and Counterinsurgency: A Counterproductive Strategy?’ (2010) 3 Critical Studies on Terrorism 209.

[44] Eg, Morocco, the Netherlands, Spain, the UK, and the USA. Eg, see Paul AC Duijn and Peter PHM Klerks, ‘Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement’ in Anthony J Masys (ed), *Networks and Network Analysis for Defence and Security* (Springer International Publishing 2014); Ian Grant, ‘Soca to Use Data Mining to Fight Fraud’ *ComputerWeekly.com* (4 October 2007) <https://www.computerweekly.com/news/2240083278/Soca-to-use-data-mining-to-fight-fraud> accessed 20 February 2020; Marieke de Goede, ‘Fighting the Network: A Critique of the Network as a Security Technology’ (2012) 13 Distinktion: Journal of Social Theory 215, 227.

[45] Black (n 6); Daniel T Cunningham, ‘The Co-Evolution of Social Networks in Insurgent Warfare’ (Naval Postgraduate School 2021).

[46] Black (n 6) viii.

[47] Badalič (n 4).

based on metadata.'[48] The need to manage and understand the vast amounts of metadata in modern warfare[49] thus makes SNA a crucial and evolving tool. This notion is highlighted by the expanded scope of network engagement strategies employed by the US Army[50] and Marine Corps,[51] which extend network-based activities beyond merely addressing 'threat' networks to engaging with 'friendly,' 'neutral,' and 'unknown' networks.

Social networks and international humanitarian law

IHL is a branch of international law governing the conduct of belligerent parties in an armed conflict. It does so by providing rules on the conduct of hostilities, the means and methods of warfare, and the protection of persons not engaged in hostilities.[52] IHL foresees that the only legitimate objective of the belligerent parties to an armed conflict is to weaken the enemy's military forces, and it limits their behaviour following the principles of military necessity and humanity.[53] The primary sources of IHL today are the four Geneva Conventions of 1949, their two Additional Protocols of 1977, the Hague Conventions of 1899 and 1907, and several treaties prohibiting or restricting the use of certain types of weapons, and customary international law.

The applicability of IHL requires the existence of an armed conflict. An armed conflict between a state and a non-state actor—an OAG in legal terminology—is a non-international armed conflict. A non-international armed conflict occurs when there exists fighting of a certain *intensity* against an armed group that is sufficiently *organized*.[54] These criteria were initially developed for use by the International Criminal Tribunal for the Former Yugoslavia (ICTY) and have since been applied by other bodies such as the ICRC and the International Criminal Court (ICC) with very little modification.[55] The challenge to ascertain the existence of a non-international armed conflict lies chiefly in determining whether and when a situation of internal disturbances and tensions, such as widespread rioting or the fight against organized crime, may be said to have reached the threshold of an armed conflict. The elaboration of the criteria of intensity and organization has long been the focus of legal scholarship, which has developed certain indicators; however, several important points remain contentious.

Terrorism is not, *per se*, an armed conflict phenomenon: neither may all terrorist groups be considered OAGs under the law, nor are all OAGs to be described as terrorists. The organizational peculiarities of terrorist groups, which often function as decentralized networks of cells with a high degree of autonomy, make them very different from the

[48] Interview with Michael Hayden—former director of the CIA and NSA, 'The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA' (7 April 2014) <https://youtu.be/kV2HDM86XgI>.

[49] Badalič (n 4).

[50] 'Network Engagement' (Department of the Army 2017) Army Techniques Publication ATP 5-0.6 <https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3696_ATP%205-0x6%20FINAL%20WEB.pdf> accessed 28 September 2023.

[51] 'MAGTF Network Engagement Activities' (US Marine Corps 2017) MCTP 3-02a <https://www.marines.mil/Portals/1/Publications/MCTP%203-02A%20MAGTF%20Network%20Engagement%20Activities.pdf?ver=2017-07- 11-112932-560>.

[52] See Liesbeth Zegveld and Frits Kalshoven, *Constraints on the Waging of War: An Introduction to International Humanitarian Law* (International Committee of the Red Cross 2001); Kolb and Hyde (n 1); Sassòli (n 1).

[53] This principle was first spelled out in the St. Petersburg Declaration relating to Explosive Projectiles of 1868.

[54] *Prosecutor v Tadić* (n 1) [70]. The two criteria were further developed in *Prosecutor v Fatmir Limaj, Haradin Bala and Isak Musliu [Judgment]* [2005] United Nations International Criminal Tribunal for the Former Yugoslavia IT-03-66-T [84] and *Prosecutor v Ramush Haradinaj, Idriz Balaj and Lahi Brahimaj* [2008] United Nations International Criminal Tribunal for the Former Yugoslavia IT-04-84-T [32ff].

[55] See *Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949. Commentary of 2020: art 3—Conflicts of a Non-International Character* (ICRC 2020) [421ff] and *The Prosecutor v Thomas Lubanga Dyilo [Judgment]* [2012] International Criminal Court ICC-01/04-01/06 [531ff].

hierarchical, military-like structure of more traditional OAGs.[56] There exist concerns regarding the capabilities of networked groups to even apply IHL in the absence of a proper chain of command.[57] The high degree of violence projected by certain terrorist groups, coupled with their opaque functioning and transnational reach, has nevertheless led to a greater willingness to consider them OAGs. Thus, a number of situations of violence involving jihadist armed groups such as al-Qaeda or ISIS have been described as armed conflicts.[58]

There are two broad ways that SNA could be of use from an IHL perspective. First, the law's applicability requires the involvement of an armed group that is sufficiently well-organized to be considered an OAG. The law does not precisely define the requisite level or type of organization (we discuss the matter of organization further below). Still, it must allow the group to conduct hostilities and engage in a continuum of attacks, as well as possess some kind of accountability mechanism that ensures sufficient control over the acts of its members so that those acts may be considered as the group's own.[59] Volatile and disorganized groups, or very fluid and decentralized networks, cannot be regarded as OAGs, irrespective of the violence they project. SNA could help understand a group's evolution, dynamics, and whether it may be considered an 'organized' armed group under the law.

Secondly, international terrorist groups often organize into networks united by a common ideology, goals, and a varying degree of mutual support and cooperation. The legal implications of such coalitions are unclear and the subject of ongoing debate in the legal community. Regardless of the state of IHL on the matter, it is vital to understand interorganizational dynamics, support relationships, and degrees of cooperation, for which SNA may be instrumental. However, SNA is inappropriate in other respects, particularly when it comes to delimiting a group and determining membership within it. The relations analysed by SNA could be highly pronounced but of a quality that is not relevant to the rules of IHL, putting civilians at risk and compromising the integrity of counterterrorism operations.

The limitations of SNA at the intraorganizational level for targeting

The bedrock principle of IHL governing the conduct of hostilities is that of distinction. While combatants and fighters may be lawfully targeted unless they have surrendered or been rendered *hors de combat* by injury or illness, civilians are protected from attack except when they are directly participating in hostilities.[60] The term 'fighter' is employed in the context of non-international armed conflicts to describe armed group members who may be lawfully targeted under IHL. However, international treaties do not specify exactly *who* is a fighter.

This ambiguity has led certain states and scholars to conclude that, by analogy with international armed conflicts—where the members of a state's armed forces are considered combatants[61]—*all* members of an OAG may also be labelled as fighters.[62] This could

[56] Margulies (n 2); Jensen (n 2); Williams (n 2); Gunaratna and Oreg (n 2).

[57] Gaggioli and Kilibarda (n 1); see in general about this requirement Cordula Droege, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 International Review of the Red Cross 533; Tilman Rodenhäuser, 'Armed Groups, Rebel Coalitions, and Transnational Groups: The Degree of Organization Required from Non-State Armed Groups to Become Party to a Non-International Armed Conflict' in Terry D Gill and others (eds), *Yearbook of International Humanitarian Law Volume 19*, (TMC Asser Press 2018).

[58] Gaggioli and Kilibarda (n 1).

[59] ibid.

[60] Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Publishing 2019).

[61] Additional Protocol I, art 43(2); this excludes medical and religious personnel.

[62] Stephen E Preston and Robert S Taylor, 'Department of Defense Law of War Manual' *General Counsel of the Department of Defense* (Washington 2016); Kenneth Watkin, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance' (2010) 42 Journal of International

include non-combat roles such as communication officers, cooks, and recruiters. Mainstream scholars do not share this broad view of being a 'fighter'[63] nor does the International Committee of the Red Cross.[64] The latter argues instead for a functional approach to membership, with the decisive criterion being an individual's 'continuous combat function' in the group.[65] Although the 'continuous combat function' approach has not been universally accepted,[66] it appears to be gaining ground and becoming a mainstream position in IHL; it has yet to be addressed in an international judicial setting, and may be tackled by the International Criminal Court in its forthcoming judgment in the *Al Hassan* case, where the accused is being prosecuted for crimes committed as a 'member' of Ansar Eddine/al-Qeada while working as a *de facto* police chief in Timbuktu and remaining unaffiliated with the group's military wing.[67] If the ICRC's approach were accepted, individuals who perform non-combat roles for the group may be liable for punishment under domestic criminal law, but they may not be lawfully targeted as long as they do not directly participate in hostilities.

We will now consider the limitations of using network analysis for the targeted killing of individual members of terrorist networks[68] by pinpointing the inappropriateness of a network approach at the intraorganizational (individual) level to define the boundaries and determine membership in OAGs under a functional approach. The first issue in this regard lies in the boundary specification problem. Currently, analysts need to decide the boundaries of a group for the purposes of analysis. Decisions regarding whom to include or exclude may obfuscate group membership and exaggerate or underestimate an OAG's membership. The second issue is the problem of tie ambiguity. Individuals with significant social links to militant groups may nevertheless not fulfil any combat function, a reality that network analysts may misinterpret. Even if the proper legal standard for targeting were not functional, SNA would still be an inadequate tool for target selection. Laying bare these practical hurdles of SNA, it becomes apparent why network analysis is inappropriate for targeting decisions regardless of the approach taken within international law.

The problems of boundary specification and tie ambiguity for determining membership in an armed group

When analysing a social network, it is important to specify its boundaries, namely, to determine who, and according to which rules, is to be included in the analysis. No set practice exists to make such determinations.[69] From an armed group perspective, it essentially concerns how to decide the group's membership. As discussed earlier, membership in an OAG

Law and Politics 57; R Patrick Huston, 'A Practical Perspective on Attacking Armed Groups' (2018) 51 Vanderbilt Journal of Transnational Law 919.

[63] Nils Melzer, *Targeted Killing in International Law* (OUP 2008); Sassòli (n 1); Gloria Gaggioli, 'Targeting Individuals Belonging to an Armed Group' (2018) 51 Vanderbilt Journal of Transnational Law 17.

[64] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (International Committee of the Red Cross 2009).

[65] ibid 33.

[66] See Watkin (n 55) and Michael N Schmitt, 'The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis' (2010) 1 Harvard National Security Journal 5. A significant criticism was also raised in Sandesh Sivakumaran, *The Law of Non-International Armed Conflict* (OUP 2012) 360–62.

[67] The case information sheet in *The Prosecutor v Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud* is available here: <https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/al-hassanEng.pdf> accessed 24 August 2023. For a discussion, see Katharine Fortin, 'Al Hassan Symposium—Rebel Governance Under the Spotlight: The ICC Al Hassan Case' *Articles of War* (25 July 2023) <https://lieber.westpoint.edu/rebel-governance-spotlight-icc-al-hassan-case/> (accessed 24 August 2023). Admittedly, the notion of membership for the purposes of individual criminal responsibility may be different from the notion of membership for the purposes of targeting, wherefore it behooves observers to carefully analyse the Court's reasoning once the judgment has been issued.

[68] Burcher and Whelan (n 25).

[69] Edward O Laumann, Peter V Marsden and David Prensky, 'The Boundary Specification Problem in Network Analysis' in Linton C Freeman, Douglas R White and Kimball Romney (eds), *Applied Network Analysis: A Methodological Introduction* (Sage 1983).

is not defined in international law and is not an appropriate consideration when making targeting decisions. Even if no boundary specification issue existed in SNA, it would still not help operational decision making. Even for questions where membership is a legally relevant factor—such as determining group structure and dynamics for conflict classification purposes—it is unclear whether SNA is a sufficiently precise tool to ascertain it.

The research by Laumann and others[70] on boundary specification is particularly important for understanding if social network theory could be used to define the boundaries of membership in an OAG. These authors note two different approaches for determining the limits of a group in network analysis. The *realist strategy* takes an emic (insider) approach and focuses on the conception of 'natural' boundaries perceived by group members. One of the challenges of a realist strategy for dark network boundary specification, like those of militant or terrorist groups, is that members may not have a shared conception of the group or, for security/efficiency tradeoff reasons, know the extent of the group's composition.[71] The *nominal strategy* takes an etic (outsider) approach. It focuses on the theoretical questions the researcher explores, often using the type of social interactions or frequency of interactions to delineate groups within a more extensive network. This approach can be misleading when determining the boundaries of militant groups. Take, for example, a suicide bomber who joins an armed group and, with great haste, attacks before any sustained frequency of group interaction occurs. In this circumstance, using the interaction frequency to establish the boundaries of an armed group would fail to include him as a member. However, even according to the more restrictive 'functional approach', he might possess a continuous combat function and constitute a lawful target under international law.

Different armed group researchers have approached the question of how to define a social network's boundaries differently depending on their research goals. For instance, some scholars include only those directly involved in an attack in their analysis, while others include additional peripheral members.[72] Scholars have noted that systematic differences in inclusion and membership criteria in militant network analysis make it difficult to reconstruct and reanalyse many studies.[73] This debate recalls the controversy regarding membership in IHL discussed earlier. Thus, the social network cannot tell you what the group *is* or *is not* in essence, nor who are the actual members of a group. Outside observers are likely to disagree to what extent a set of individuals are part of a group. Different interpretations can result from differences in context (eg, political versus apolitical setting) or perceiver knowledge (eg, not being privy to emic information, misinterpreting the degree of cooperative intent among a set of agents, or misunderstanding internal conflicts of interest).

The difficulties that 'fuzzy boundaries'[74] present can lead political leaders to misinterpret or misreport the extent of terrorist networks, whether for political gain or because of misunderstanding. In the early years of the War on Terror, the US government reported that the size of the al-Qaeda network was globally expansive to justify its transnational military response.[75] Coalition allies of the USA were also incentivized to expand the boundaries of the network so they could benefit from arms, training, and military aid.[76] To demonstrate military success, the US government was later incentivized to limit the scale and scope of

[70] ibid.

[71] Marie Ouellet and Martin Bouchard, 'The 40 Members of the Toronto 18: Group Boundaries and the Analysis of Illicit Networks' (2018) 39 Deviant Behavior 1467.

[72] Ouellet (n 12).

[73] Alexander Gutfraind and Michael Genkin, 'A Graph Database Framework for Covert Network Analysis: An Application to the Islamic State Network in Europe' (2017) 51 Social Networks 178.

[74] Burcher and Whelan (n 25).

[75] Stohl and Stohl (n 19).

[76] ibid.

the al-Qaeda terrorist network and applied a more restrictive boundary condition to limit those linked as members of al-Qaeda.[77] Indeed, networks can be restricted or 'infinitely extensible'[78] depending on the analyst's goals, which should serve as a cautionary tale for using SNA haphazardly to define the boundaries of militant networks. Unfortunately, network analysis does not provide an easy solution to the problems associated with determining an OAG for legal purposes or functional membership within that group without including further information or establishing rule-based boundary conditions.

The fuzzy boundaries problem is made worse by the dynamic membership nature of some militant groups. Sageman[79] noted that the evolution of connections within terrorist networks is too rapid and too nuanced for network diagrams to keep up in a way that would be useful as a battlefield tool. Instead, network analysis is more helpful in drawing post hoc conclusions about terrorist networks once more information is available. Indeed, researchers have found significant turnover and volatility in militant networks[80] and changes in network configurations and leadership roles.[81] Such findings suggest that neglecting such change, as many network studies do, is worrisome, for it poses significant problems with analysis and interpretation.[82] Network modelling studies further suggest that militant networks regularly restructure themselves to avoid government interdiction.[83] If militant networks have such dynamic membership and structural properties, it may be difficult to correctly determine functional membership in an OAG using network analysis.

Tie relationships in covert networks are ambiguous and misleading

If we are to maintain a distinction between combatants/fighters and civilians as IHL requires, then the nature of the relationship between two or more nodes is of utmost importance. Given their 'dark' nature, mapping ties between nodes accurately in covert networks can be a challenge for analysts, making it difficult to discern who is a member of the group, who has a fighting function, and who is simply an outsider interacting with its members. Individuals interact in many different ways depending not only if a relationship is present or not, as indicated by SNA, but also on the nature of the relationship.[84] Even within one category of tie, say kin-relations, a family member may be close or distant, accepting of a family member's behaviour or appalled by their actions. Conflating different relationship types is common among studies on terrorist networks[85] and in the broader social network literature.[86] Some militant network researchers code the strength of relationships while neglecting clear distinctions between the type of relationship[87]. In contrast, others code the kind of relationship without indicating the strength of these relationships.[88] The lumping of different types of relationships (eg, friendship, kinship, and organizational roles) into a *uniplex*—single tie—the relationship can lead to an arbitrary focus on certain relations

[77] ibid.

[78] Martin Coward, 'Against Network Thinking: A Critique of Pathological Sovereignty' (2018) 24 European Journal of International Relations 440.

[79] Cited in Chris Wilson, 'Searching for Saddam' [2010] *Slate* <http://www.slate.com/articles/news_and_politics/searching_for_saddam/2010/02/searching_for_saddam.html?via=gdpr-consent> accessed 20 February 2020.

[80] Rachel Stevenson and Nick Crossley, 'Change in Covert Social Movement Networks: The "Inner Circle" of the Provisional Irish Republican Army' (2014) 13 Social Movement Studies 70.

[81] Jasper L de Bie and others, 'Changing Organizational Structures of Jihadist Networks in the Netherlands' (2017) 48 Social Networks 270.

[82] Stevenson and Crossley (n 80).

[83] Walter Enders and Xuejuan Su, 'Rational Terrorists and Optimal Network Structure' (2007) 51 Journal of Conflict Resolution 33.

[84] Luke M Gerdes, 'Dark Dimensions: Classifying Relationships among Clandestine Actors' in Luke M Gerdes (ed), *Illuminating Dark Networks* (CUP 2015).

[85] ibid.

[86] Borgatti, Brass and Halgin (n 8).

[87] Marc Sageman, *Leaderless Jihad Terror Networks in the Twenty-First Century* (University of Pennsylvania Press 2008).

[88] Everton (n 27).

over others and thus contribute to a biased interpretation of the network and its actors.[89] Network researchers recognize that militant networks are likely to be multiplex, that is constituted of individuals who collaborate for militant ends but are also connected by other means, such as kinship, friendship, or business partnerships.[90] Such pre-existing social ties are likely to help facilitate militant mobilization and recruitment,[91] but they do not necessarily indicate the exercise of a fighting role as required for targeting.

To make matters more complex, some scholars code the presence of a relationship if two individuals attend a shared event (eg, attending the same university, visiting the same mosque). However, in large settings, such as a public university, there is a significant chance that meaningful relationships are rarely formed or absent altogether.[92] If two individuals attend the same mosque, it is not guaranteed that they share the same ideologies or motivations for attending, which is also problematic with such categorization.[93] When analysing social networks, the conflation of different types of relationships may cause an individual with a non-functional role in the terrorist organization (eg, a widely shared mutual friend) to display a high degree of centrality. An analyst might misinterpret that the individual is integral to group operations despite their non-functional involvement.[94]

Missing data pose significant challenges for network analysis.[95] False negatives—whether specific nodes or relations are unknown to the analyst—or false positives—whether perceived relationships are accurate—can significantly impact the interpretation of network metrics, including density and centrality.[96] Making data issues worse is that militant group members may try to deceive their adversaries by using multiple phones, SIM cards, aliases, email addresses, or more elaborate counter-intelligence efforts.[97] For instance, militant group members are known to swap SIM cards during meetings to avoid being successfully tracked by intelligence teams.[98] Militants may be left unaware that they are being traced using SIM card data and unwittingly share their phones with friends or family,[99] complicating matters when ties are established using metadata.

Williams[100] notes that the vagueness of ties in terrorism research often makes analysts exaggerate connectivity among individuals. Vaguely defined ties are likely responsible for the overinflated importance of al-Qaeda's presumed role in global jihadist terrorism. While many violent Islamist terrorist groups are likely to have links to al-Qaeda in some form, these ties are often 'diffuse, ethereal, and lacking in substance'.[101] Given the sparsity of information sources when assessing terrorist networks, even well-informed intelligence analysts may face challenges piecing together relationships when working with classified data.[102] While such relationship conflation may only affect scholars working with publicly available datasets, some evidence suggests that intelligence analysts in the US military faced

[89] Gerdes (n 84); Gutfraind and Genkin (n 73).

[90] Not relevant under IHL, see DPH Guidance p 33ff.

[91] Marc Sageman, *Understanding Terror Networks* (University of Pennsylvania Press 2004).

[92] Gerdes (n 84).

[93] It should be added that, in case of doubt as to an individual's status in the conduct of hostilities context, humanitarian law requires belligerent parties to presume that the individual in question is a civilian. The presence of lawful targets within a civilian population similarly does not deprive that population of its civilian character. See art 50 of Additional Protocol I to the Geneva Conventions.

[94] Gerdes (n 84) 29.

[95] Gueorgi Kossinets, 'Effects of Missing Data in Social Networks' (2006) 28 Social Networks 247.

[96] Burcher and Whelan (n 25); Gutfraind and Genkin (n 73).

[97] Burcher and Whelan (n 25).

[98] Scahill (n 37) 226.

[99] ibid 225.

[100] MG Clive Williams, 'The Question of "Links" Between Al Qaeda and Southeast Asia' in Kumar Ramakrishna and See Seng Tan (eds), *After Bali* (World Scientific Publishing Co and Institute of Defence and Strategic Studies 2003).

[101] Gerdes (n 84) 24.

[102] ibid.

similar difficulties.[103] In part, poorly defined network ties or confusion in relationship types may contribute to the incorrect targeting of civilians in drone strikes and night raids.[104] As Krebs[105] cautiously notes, being an 'alter of a terrorist does not prove guilt', but it should 'invite investigation'.

It is clear that relational ties established using only metadata, single information sources, or hearsay, rather than reliable intelligence and ethnographic data, contribute to poor decision-making.[106] This problem is exacerbated when the time horizon of the decision-making process is brief, and the resulting actions taken are irreversible. In Iraq and Afghanistan, the USA's reliance on an intelligence doctrine known as *find*, *fix*, *finish*, *exploit*, *analyse* (F3EA) reduced the time between intelligence gathering following a military operation, social network data analysis, and subsequent strikes on new targets.[107] Numerous intelligence data sources supported F3EA in Iraq, which helped to reduce decision-making errors.[108] However, a reduction in rich intelligence sources combined with the hasty F3EA decision-making process in Afghanistan contributed to fatal targeting mistakes.[109]

It should be added that our conclusions in this section are not only valid if one were to opt for a functional approach to targeting. As mentioned above, the most common alternative approach is 'status-based', whereby, analogously with the members of a state's armed forces, all members of an OAG may be lawfully targeted, with the exception of medical and religious personnel.[110] This framework is usually advocated as the most straightforward, and normally perceived as the most permissive when making targeting decisions. Even so, SNA and the nature of ties between nodes that it takes into account do not illuminate the question of membership in an OAG. Although it makes sense that group members would have a high level of social interaction with each other, there is nothing to suggest that such relations may not be established with individuals who are not members of the group, and, therefore, civilians. Family members, prisoners, enslaved individuals, and non-member supporters may spend much time interacting with the group's members or even be housed in the same quarters, thus enjoying strong network links without having the requisite 'status' to become lawful targets under IHL. Regardless of the applicable legal framework, lethal operations must be based on data of the highest degree of precision and reliability, which SNA alone can ultimately not provide.

Network ties do not equal command or control

Prolonged armed engagements, often in the context of asymmetrical conflicts pitting OAGs against state forces, require a sufficient degree of unit cohesion and stability to preserve the group's existence, functioning, and attainment of its goals. As discussed earlier, 'traditional' OAGs have a hierarchical structure and a relatively well-defined chain of command, allowing superiors to exercise adequate command and control over subordinate group members.[111] A hierarchical structural model is more appropriate as OAGs need to be able to implement the rules of international law by possessing at least a rudimentary accountability mechanism.[112]

[103] Ford (n 15); Badalič (n 36).

[104] Badalič (n 36).

[105] Krebs (n 21).

[106] Ford (n 15); Badalič (n 36); Scahill (n 37).

[107] Ford (n 15) 119.

[108] ibid 122.

[109] ibid; Badalič (n 36).

[110] This doctrine has been defended in various legal literature, including, eg, Michael N Schmitt, 'The Status of Opposition Fighters in a Non-International Armed Conflict' (2012) 88 International Law Studies 119 and E Corrie Westbrook Mack and Shane R. Reeves, 'Tethering the Law of Armed Conflict to Operational Practice: "Organized Armed Group" Membership in the Age of ISIS' (2018) 36:3 Berkeley Journal of International Law 334.

[111] Jensen (n 2).

[112] Gaggioli and Kilibarda (n 1).

Given the conflation between relationships, among other challenges, it can be difficult to draw firm conclusions about the control-and-command structure of a networked organization and if any large-scale coordination exists. In sizable networks, as the number of nodes increases, reaching consensus faces a collective action problem, for it becomes less likely that all members will share a common conception of goals and strategies.[113] Zech and Gabbay[114] note that the current literature often does not adequately distinguish communication ties from ties of authority, obfuscating interpretation. Such ambiguity makes it difficult to apply network analysis purposefully under international law. The legal focus is not on the density or frequency of intragroup networks but on the group's overall command-and-control capabilities and the function of individual members. When analysing intergroup ties, network density may be a proxy for a movement's cohesiveness.[115] However, density metrics at the individual level may indicate little about individuals' cohesiveness or willingness to cohere for militant action in the face of adversity.[116] An analysis of the 'Toronto 18'—18 members of a terrorist group who planned to carry out attacks in Canada—discovered that an additional 22 individuals regularly interacted with the group but were not an active part of the group's violent objectives.[117] Determining who might be in charge of operations can be difficult. Network nodes identified as bridges because of their high level of connectedness may not be leaders or those in control but relatively low-level individuals such as drivers or guides who maintain extensive contacts because of their roles.[118] A study found that being in a central network position does not necessarily imply that someone is a broker or leader. Instead, those individuals may be highly social actors otherwise deemed unfit for leadership because of social inadequacies (ie, marginalized supporters who are merely tolerated and lack any influence or power).[119]

The 'London bombers' are one example of a group of attackers who shared ideological goals with al-Qaeda and who authorities initially suspected had a solid link to the al-Qaeda network but carried out their plans without any connection to more extensive organized networks.[120] Similarly, in an analysis of suicide bombers, scholars did not find evidence that suicide bomber 'hubs' received direct orders from those outside their respective hub, nor were they guided by grand strategic motivations.[121] As Stohl and Stohl[122] argue, 'for a network approach to be useful, we cannot think of the network as a clear command-and-control structure with some links giving orders to the others. Rather, a terrorist network is at the nexus of multiple groups and constituencies that are linked in significant but non-hierarchical ways and can only be understood in context'.

Practical issues of network analysis at the intraorganizational level

Expressing relationships as linked nodes has drawbacks because it cannot account for the nuances in how people are truly connected.[123] As our discussion about the problems associated with tie inaccuracy illustrates, it can be difficult to understand relationships without

[113] Richard Matthew and George Shambaugh, 'The Limits of Terrorism: A Network Perspective' (2005) 7 International Studies Review 617.

[114] Zech and Gabbay (n 10).

[115] ibid.

[116] ibid.

[117] Ouellet and Bouchard (n 71).

[118] 'Untangling the Social Web' *The Economist* (London, 4 September 2010) <https://www.economist.com/technology-quarterly/2010/09/04/untangling-the-social-web> accessed 25 February 2020.

[119] de Bie and others (n 81).

[120] Aidan Kirby, 'The London Bombers as "Self-Starters": A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques' (2007) 30 Studies in Conflict & Terrorism 415.

[121] Ami Pedahzur and Arie Perliger, 'The Changing Nature of Suicide Attacks: A Social Network Perspective' (2006) 84 Social Forces 1987.

[122] Stohl and Stohl (n 19) 107.

[123] Wilson (n 79).

having on-the-ground knowledge of militant group members. When traditional forms of intelligence are lacking, it becomes challenging to crosscheck relational data contributing to errors in decision making.[124] Researchers have shown that strict reliance on government data sources (eg, government reports, prosecution and law enforcement data), compared, for instance, to interviews with informants who have first-hand knowledge about the internal workings of a militant group, can obscure the degree to which individuals are connected with the operations of the network.[125] While it is true that ignoring noncombatant affiliates can mask the full scope of covert groups,[126] incorrectly classifying individuals as members when they are not can lead to unethical and illegal decisions.[127]

As Ford[128] reports, when the US military shifted from using network analysis as an analytical tool to use it as evidence for conducting targeted raids or killings, analysts regularly failed to comprehend the broader social milieu. Analysts became more attentive to the form of the network and what it might say about the hostile intentions of individuals making up the network nodes than to their social and political aims. This narrow focus limited the analysts' understanding of communities' political dynamics and social capital. Ford argues that failing to understand the political and social ecology by relying too much on network analysis undermined counterinsurgency efforts to win over the local population and hindered the process of reconciliation with the Taliban.[129] Other scholars posit that too strong a focus on network analysis ignores the social milieu that influences an individual's decision to become an active member in a conflict, thereby overlooking possible contextual interventions in favour of violent and destructive interdiction.[130] We concur with Ford and other scholars that overemphasizing SNA can lead to an incomplete understanding of the political and social context. Indeed, this narrow focus can hinder efforts to engage local populations and overlook opportunities for contextual interventions, ultimately affecting the success of counterinsurgency and reconciliation strategies.

On a practical level, targeting specific individuals within a network is known to have drawbacks. Zech[131] found that the targeted killing of terrorist leaders in Spain shortly after the 9/11 attacks allowed for the later emergence of a new network that would go on to conduct the Madrid train bombings in 2004. Other scholars found that targeted killings of terrorist leaders empower lower level terrorist group members that have less restraint against targeting civilians.[132] Furthermore, empirical evidence suggests that militant networks recover rapidly after decapitations and are typically resilient to such strategies.[133] For these and additional reasons, scholars have argued that decapitation may not always be the most desirable strategic option.[134]

[124] Badalič (n 36) 34.

[125] Ouellet and Bouchard (n 71).

[126] ibid.

[127] Badalič (n 36).

[128] Ford (n 15).

[129] ibid 126.

[130] Coward (n 78).

[131] Steven T Zech, 'Decapitation, Disruption, and Unintended Consequences in Counterterrorism: Lessons from Islamist Terror Networks in Spain' (2016) 32 Defense & Security Analysis 177.

[132] Max Abrahms and Jochen Mierau, 'Leadership Matters: The Effects of Targeted Killings on Militant Group Tactics' (2017) 29 Terrorism and Political Violence 830.

[133] René M Bakker, Jörg Raab and H Brinton Milward, 'A Preliminary Theory of Dark Network Resilience' (2012) 31 Journal of Policy Analysis and Management 33; Carley (n 26); Kathleen Carley and others, 'Destabilizing Dynamic Covert Networks' in *Proceedings of the 8th International Command and Control Research and Technology Symposium* (2003), Washington, DC <http://www.casos.cs.cmu.edu/publications/papers/carley_2003_networks.pdf> accessed 10 March 2020.

[134] Everton (n 27); Roberts and Everton (n 41); Zech (n 131).

Exploring the benefits of SNA and its application to armed groups under international law

Boundary specification problems, ambiguous tie relationships, and unclear command-and-control relationships are limitations that significantly constrain the utility and application of network analysis for understanding group boundaries, membership, and to applying targeted killing practices. Despite these limitations, it is impossible to ignore its usefulness for understanding militant groups' functioning, structure, and evolution. Therefore, in the following sections, we discuss the benefits of using network analysis to inform the classification of situations of violence and to understand inter-group relationships.

Using SNA to inform the classification of situations of violence

As discussed earlier, a non-international armed conflict exists whenever 'there is […] protracted armed violence between governmental authorities and organized armed group or between such groups within a State'.[135] Therefore, the groups involved in the fighting have to possess a requisite level of organization. The International Criminal Tribunal for the former Yugoslavia (hereafter, 'the tribunal') has used the following indicative factors for determining if an armed group is sufficiently organized: '(1) the presence of a command structure; (2) the ability to carry out operations in an organized manner; (3) the group's level of logistics; (4) the group's 'level of discipline and its ability to implement the basic obligations of Common Article 3'; and (5) the group's ability to speak with one voice.'[136] Although the tribunal never explained why it resorted to these specific factors, they correspond much more closely to the functioning of a hierarchical group rather than a networked one.[137]

As evidenced throughout this article, network analysis can help analysts understand how organizations and groups function and can use structural characteristics to predict specific outcomes. As such, it is uniquely suited to help inform decisions about violence classification. Network analysis could assist in at least two ways: (i) establishing a more nuanced and objective threshold to judge the 'organization' criteria of armed groups, especially bearing in mind the need to ascertain its capacity to engage in a continuum of attacks and have accountability mechanisms and (ii) using network structure to predict the degree of violence and longevity of an emerging violent organization, which would help inform decisions about the 'intensity' criteria of protracted armed violence.

One could imagine using a command-and-control approach to establish a more objective threshold for armed group organization.[138] By analysing command-and-control ties, it might be possible to monitor situations of rising conflict and measure the proportion of individuals engaging in violence as part of a 'loosely coupled movement' where individuals follow *strategic* control but lack *operational* control, compared to the proportion of individuals in a 'coupled network', in which both strategic and operational control influences individuals. Once a certain threshold of command-and-control ties is reached, the militant collective could be considered an *organized* armed group rather than a loosely defined movement. The command-and-control threshold could be set to reflect the group's capacity for continuous engagement in the conduct of hostilities and to maintain internal discipline. While such an approach would need to be significantly developed and refined, it may be

[135] *Prosecutor v Tadić* (n 1) [70].

[136] Rodenhäuser (n 57).

[137] Gaggioli and Kilibarda (n 1).

[138] For a detailed description, see Brian A Jackson, 'Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda' (2006) 29 Studies in Conflict & Terrorism 241.

possible to clarify the organizational requirements set forth by IHL using network analysis as a more objective standard than a subjective set of indicative factors.

Despite the ability of network analysis to address how network structure might contribute to specific outcomes that are important for classifying situations of violence (eg, lethality, longevity), research of this type is still in its infancy.[139] An exception is research by Helfstein and Wright[140] who studied how the structure of networks affects the severity of attacks. While they found no significant effect of network attributes on the severity of attacks, their limited sample size and reliance on the number of causalities as their dependent variable may have limited their results. Perliger[141] also examined how structural characteristics of terrorist networks were related to group duration and the number of attacks during the group's existence (ie, productivity and durability). Perliger found that more successful networks are structured in a way that effectively balanced cohesiveness with flexibility (neither too security focused nor too efficient). They also tended to include a high portion of overlapping cliques. Future research addressing how an organization affects the capacity to engage in a continuum of attacks could be used to make judgments about the likely long-term intensity of conflicts, thus helping policymakers confront situations of violence in ways that are effective and proportional. Indeed, future studies may help with the early identification of potentially violent militant organizations within vast social networks,[142] which could facilitate state intervention and humanitarian assistance before the onset of large-scale violence.

Using SNA at the interorganizational level to determine support relationships

An analyst faces fewer theoretical and practical difficulties performing network analysis at the interorganizational level. For security reasons, tie relationships within covert militant groups are necessarily secret, ambiguous to interpretation, and sometimes intentionally misleading. In contrast, the pursuit of sociopolitical goals requires that armed groups publicly convey, at least to some degree, their existence, aims, adversaries, and allies.[143] Analysts can therefore be more certain about the nature and strength of ties *between* militant groups thanks to increased political visibility compared to *within* armed groups. The number of actors within a militant group is also typically unknown, complicating the identification of nodes. Groups within a given conflict are more apparent to analysts, and the nature of the conflict itself (eg, geographical region, declared members of opposing alliances) can help to reduce uncertainty regarding the boundary conditions of the analysis.

Legal researchers have also recognized this state of affairs, with several scholars trying to develop different theories of armed group 'coalitions'.[144] The legal rationale for the focus on coalitions is to facilitate conflict classification. By becoming a 'coalition member' or an associated force of an existing OAG, the group under scrutiny joins an existing conflict and no longer needs to project a certain intensity of violence on its own. OAG coalitions are

[139] Zech and Gabbay (n 10).

[140] Scott Helfstein and Dominick Wright, 'Covert or Convenient? Evolution of Terror Attack Networks' (2011) 55 Journal of Conflict Resolution 785.

[141] Arie Perliger, 'Terrorist Networks' Productivity and Durability: A Comparative Multi-Level Analysis' (2014) 8 Perspectives on Terrorism 17.

[142] Muhammet Serkan Çinar, Burkay Genç and Hayri Sever, 'Identifying Criminal Organizations from Their Social Network Structures' (2019) 27 Turkish Journal of Electrical Engineering & Computer Sciences 421.

[143] Zech and Gabbay (n 10).

[144] Nathalie Weizmann, 'Associated Forces and Co Belligerency' (2015) 24 Just Security; Ashley Deeks, 'Common Article 3 and Linkages Between Non-State Armed Groups' (*Lawfare*, 4 October 2017) <https://www.lawfareblog.com/common-article-3-and-linkages-between-non-state-armed-groups> accessed 14 October 2022; Vaios Koutroulis, 'Classifying Contemporary Conflicts: The Challenge of Coalitions of Non-State Armed Groups and/or States' in *Legal Challenges for Protecting and Assisting in Current Armed Conflicts* (College of Europe / ICRC 2019); Marten Zwanenburg, 'Addressing the Threat Posed by Coalitions of Non-State Armed Groups: A State Perspective', *Legal Challenges for Protecting and Assisting in Current Armed Conflicts* (College of Europe / ICRC 2019).

typically conceptualized by analogy with co-belligerency and State coalitions in international armed conflicts. Still, it is questionable whether such analogies are appropriate when discussing OAGs, and 'traditional' IHL does not foresee them.[145]

Interorganizational network analysis may, nevertheless, be useful for non-international armed conflicts to understand support relationships and answer questions about the nature of group interactions. Questions, such as, what effect does the intervening group have on the adversary by assisting the supported party? Is this effect moderated by (i) the nature of the support (eg, state/armed group, armed group/armed group), (ii) the type of support (eg, information, financial, arms), or (iii) the intensity of the support (eg, repeated, one-time)? A network perspective could help to answer such empirical questions by integrating relevant node attributes (eg, the relative strength of actors, political affiliations, ease of arms procurement, fighting capabilities, command structure, leadership abilities)[146] with tie indicators of conflictual or competitive relationships within a single conflict to measure the degree to which a supporting party positively affects the supported party and negatively affects the adversary. The lessons learned could then provide more objective standards for evaluating future interactions between intervening powers and supported parties. Predicting the likelihood of support relationships forming or dissolving and how these relationships affect the probable outcomes of a conflict would be valuable information for States and humanitarian organizations, even if they are not directly relevant for conflict classification. Using link prediction,[147] among other network analyses, future network research on militant groups may help to predict which support relationships are likely to form and how they affect conflict outcomes. The application of network analysis is particularly relevant for determining support relationships in complex battlefield environments. In such environments, it could help to clarify the nature and the strength of support relationships by combining various sources of support with the frequencies of interactions into a single assessment. It might also be possible to consider the evolution of relationship ties over time to see how support changes as a non-international armed conflict progresses.

Conclusion

SNA is a powerful tool with the potential to generate valuable insights for international law scholars and enhance IHL compliance when applied responsibly. However, using SNA for targeting in non-international armed conflicts is inherently flawed, as it fails to accurately identify lawful targets and risks putting people protected from attack under IHL at risk. Contemporary jihadist armed groups, often dubbed 'dark networks', complicate SNA's effectiveness, as many members remain unaware of the group's extended structure and function. High centrality members may not hold a combat role, while combatants could linger on the network's periphery. Consequently, SNA may jeopardize the safety of uninvolved individuals who share strong ties with group members.

Despite such limitations, SNA remains valuable in other legal domains, such as law enforcement and criminal justice. Governments often criminalize terrorist group membership, and SNA has proven effective in combating organized crime in countries like the UK and the Netherlands. Furthermore, SNA can still play a role in IHL by shedding light on intragroup dynamics for conflict classification and revealing the strength of relations between armed group coalitions. However, it is crucial to recognize the unsettled nature of these

[145] Again, this issue may be addressed in the forthcoming *Al Hassan* judgment at the ICC, as the prosecution relied on a notion of 'aggregated intensity' to describe the situation in Mali as an armed conflict at the time of the accused's alleged crimes. See Fortin (n 57).

[146] See, for instance, the group variables included in the Non-State Actors in Armed Conflict Dataset (NSA) David E Cunningham, Kristian Skrede Gleditsch and Idean Salehyan, 'Non-State Actors in Civil Wars: A New Dataset' (2013) 30 Conflict Management and Peace Science 516.

[147] David Liben-Nowell and Jon Kleinberg, 'The Link Prediction Problem for Social Networks' (2007) 58 Journal of the American Society for Information Science and Technology 1019.

coalitions in IHL, meaning SNA's results may not always carry legal significance. To address the legal implications of armed group coalitions, we call for initiating a dialogue within the IHL community to establish clear frameworks for their classification and treatment under international law. We encourage the development of guidelines and best practices for applying SNA in international humanitarian law to ensure its responsible and ethical implementation. To enhance the accuracy and relevance of SNA within IHL contexts, we advocate for interdisciplinary collaborations between international legal scholars and social scientists to refine SNA methodologies. We urge policymakers and military decision makers to exercise caution when using SNA for targeting purposes, emphasizing the importance of corroborating information and a comprehensive understanding of the individuals and groups involved in armed conflicts.

Acknowledgements

The authors express gratitude to Ilya Sobol for his insightful feedback on earlier drafts of the article and extend thanks to a previous anonymous reviewer at the journal Critical Studies on Terrorism for their detailed and valuable recommendations. We also extend our deepest gratitude to the anonymous reviewers at the Journal of Conflict and Security Law for their thoughtful comments, which greatly helped strengthen and improve the article.

Funding

This work was supported by The Swiss National Science Foundation (Grant No. 176781).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.