information

Article

Interoperability and Targeted Attacks on Terrorist Organizations Using Intelligent Tools from Network Science

Alexandros Z. Spyropoulos [1,*], Evangelos Ioannidis [2] and Ioannis Antoniou [2]

[1] Department of Physics, School of Science, Kavala's Campus, International Hellenic University (IHU), 57001 Thessaloniki, Greece
[2] Department of Mathematics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece; ioannidek@math.auth.gr (E.I.); iantonio@math.auth.gr (I.A.)
* Correspondence: daspyro@physics.ihu.gr

Abstract: The **early intervention** of law enforcement authorities to **prevent** an impending terrorist attack is of utmost importance to ensuring **economic**, **financial**, and **social stability**. From our previously published research, the key individuals who play a vital role in terrorist organizations can be **timely revealed**. The problem now is to identify which **attack strategy** (**node removal**) is the most damaging to terrorist networks, making them **fragmented** and therefore, **unable to operate under real-world conditions**. We examine several **attack strategies** on **4 real terrorist networks**. Each node removal strategy is based on: (i) randomness (random node removal), (ii) high strength centrality, (iii) high betweenness centrality, (iv) high clustering coefficient centrality, (v) high **recalculated** strength centrality, (vi) high **recalculated** betweenness centrality, (vii) high **recalculated** clustering coefficient centrality. The damage of each attack strategy is evaluated in terms of **Interoperability**, which is defined based on the **size** of the **giant component**. We also examine a **greedy algorithm**, which removes the node corresponding to the maximal decrease of Interoperability at each step. Our analysis revealed that removing nodes based on high **recalculated** betweenness centrality is **the most harmful**. In this way, the Interoperability of the communication network drops dramatically, even if **only two** nodes are removed. This valuable insight can help law enforcement authorities in developing more effective **intervention strategies** for the **early prevention** of impending terrorist attacks. Results were obtained based on real data on **social ties** between terrorists (**physical face-to-face social interactions**).

Keywords: terrorist networks; network analysis; centrality; attacks; giant component; interoperability; fragmentation; intelligence

check for updates

Citation: Spyropoulos, A.Z.; Ioannidis, E.; Antoniou, I. Interoperability and Targeted Attacks on Terrorist Organizations Using Intelligent Tools from Network Science. *Information* **2023**, *14*, 580. https://doi.org/10.3390/info14100580

Academic Editors: Leandros Maglaras and Rami Puzis

Received: 27 July 2023
Revised: 18 October 2023
Accepted: 19 October 2023
Published: 21 October 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Terrorism continues to be a persistent and intricate threat to global stability, compelling modern states to allocate substantial resources toward devising effective counter-terrorism measures. Law enforcement agencies face critical questions that demand immediate and accurate answers—chief among them is the research question this paper aims to address: *which intervention strategy would be the most effective to prevent a possible terrorist activity?* While scholars from various disciplines have offered varying solutions to this complex issue, our study takes an innovative approach by employing intelligent tools from network science. These tools, such as real-time recalculated network centrality measures, provide a nuanced understanding of the fluid and dynamic nature of terrorist organizations. By leveraging these intelligent tools, this paper seeks to offer law enforcement authorities targeted, adaptive, and empirically validated counterterrorism strategies that are effective in real-world scenarios.

Terrorism is a complex phenomenon that has attracted global attention, especially after the 9/11 attack [1,2]. Despite the recent research activity in the field, there is still a significant knowledge gap, about the relationship between terrorism and psychiatric disorders,

radicalization processes, and the effectiveness of preventative measures [3–5]. Today's terrorism research is mainly focused on transnational and homegrown terrorism [1,2,6]. The term "radicalization" is frequent in the counter-terrorism terminology. However, it presents interpretive ambiguities and questions the balance between addressing violent extremism and promoting societal cohesion [3]. The groupthink phenomenon adds further complexity, challenging rational choice theory in the sense that certain social groups may adopt terrorism due to irrational decision-making [4]. In response to these complexities, counter-terrorism strategies should be comprehensive and evidence-based [3,5,6]. In this context, the role of social media platforms in promoting societal cohesion and preventing the spread of extremist ideologies cannot be ignored [2]. Concerning Islamic terrorism, although invoking Islam, does not imply a direct connection with the religion itself. This kind of terrorism needs an exploration of the criminological, psychological, and social dimensions of radicalization [7–13]. The application of various criminological theories, including strain theory, social control, and differential association, provides valuable insights into radicalization [11,14]. However, the lack of empirical data is challenging [9]. Several nations, such as Australia, have already adopted policy measures to counter radicalization [8]. Lessons from crime prevention policy and practice inform these measures [15]. However, these efforts can create 'suspect communities' and civil rights abuses [8]. Addressing radicalization within the context of Islamic terrorism requires an integrated, multifaceted approach that considers psychological, criminological, and social perspectives [9]. Future research should focus on gathering more empirical data, aiming to develop evidence-based interventions that respect human rights and societal diversity [8,9,16].

Network Theory has already been applied successfully in studying terrorism [17–25]. In this context, terrorist organizations are mathematically modeled as networks of nodes (actors or groups of actors) and edges (relationships) [26,27]. Several applications of network theory to terrorism have advanced significantly the existing knowledge in this field [28–30]. The predictive power of social network analysis and novel classification methods are highlighted [31–33].

The fusion of network science, machine learning, data mining, and link analysis has led to innovative methodologies for evaluating, predicting, and countering terrorist networks [31,32]. New methods have been proposed to identify crucial players within terrorist networks and predict potential activities [34,35]. The increasing use of social media requires new approaches for analyzing and identifying influential nodes in terrorist networks [35]. Understanding the role of social ties is vital for preventing possible future terrorist activities [36,37]. Our previously published research on four real-world terrorist networks revealed the distinct social roles of individuals in terrorist organizations [38] and uncovered successfully some early signs of impending terrorist attacks [39]. The fusion of social network analysis and machine learning methods provides valuable insights into the structure, operation, and dynamics of terrorist networks [37,40–47].

In counterterrorism and law enforcement, our team contributed two groundbreaking papers. "Entropy and Network Centralities as Intelligent Tools for the Investigation of Terrorist Organizations" [48] and "Investigation of Terrorist Organizations Using Intelligent Tools: A Dynamic Network Analysis with Weighted Links" [49] both leverage mathematical tools to unlock the obscured behaviors and structure of terrorist organizations. The first paper utilizes entropy and network theory to discern the diverse roles within a terrorist organization and detect early signs of impending attacks. By mapping physical contacts within four real-world terrorist networks, the research uncovers distinctive roles linked to specific centrality values, and intriguingly, the imminent threat of an attack correlates with the evolutionary pattern of these centralities' entropies. This illuminates an invaluable tool for law enforcement, empowering them to not only identify pivotal figures within terrorist cells but also predict an imminent attack through monitoring the evolution of the centralities' entropies [48]. In a parallel vein, the second paper champions an innovative, quantitative, and unbiased methodology based on network theory to explore the distinct roles within terrorist organizations. Challenging the conventionally biased or subjective

witness statements, it employs select global indices, such as density, small worldness, centralization, average centrality, and standard deviation of centrality, offering insights into the organizational structure and potential activity of terrorist groups. These indices, tested on four real-world terrorist networks, reveal the organization's distinct roles and indicate possible impending activities [49].

Concerning network attacks related to terrorist organizations, three key papers were found in the relevant literature, namely: (a) [41] where a model for assessing network robustness with non-real data was studied, (b) [46] where attacks on the air transportation network of a terrorist organization were studied, and (c) [47] where attacks on the online social network of ISIS foreign fighters was studied.

Even though significant work has been conducted in this field, there is still no "action plan" for the early prevention of imminent terrorist attacks, tested with real data of social ties, which can be applied by law enforcement authorities in real-world conditions. As a result, the research purpose of this paper is to address the following research question: **Which attack strategy (node removal) is the most damaging to terrorist networks, making them fragmented, and therefore unable to operate under real-world conditions?**

The rest of the paper is organized as follows. In Section 2, we present the methodology, the datasets, and the proposed network attack strategies. In Section 3, we present the results of our analysis, and we discuss them in Section 4. Finally, in Section 5 we summarize the key conclusions of our work.

2. Methodology, Attack Strategies and Datasets

Law Enforcement Authorities *presuppose* that *any terrorist organization is a connected network* (there is *always* a path between *every* pair of nodes). If the terrorist organization has isolated nodes ("lone wolves") or isolated groups of nodes, then these distinct terrorist threats are treated as *different* terrorist organizations [50–55].

Interoperability, a fundamental concept in systems design, is the capacity of distinct systems, devices, or components to exchange and effectively utilize information in a cooperative manner [56]. According to the Institute of Electrical and Electronics Engineers (IEEE), interoperability is explicitly defined as "the ability of two or more systems or components to exchange information and to use the information exchanged" [57,58]. This definition implies that for systems to be interoperable, they must not only be capable of exchanging data but also interpreting and using that data in a meaningful way. Clear and unambiguous descriptions of characteristics and abilities are essential to ensure that the data is computationally interpretable [56]. The concept of interoperability extends beyond pure system functionality and includes aspects of cooperative behavior and shared understanding. For instance, NATO defines "interoperability" as the ability of Allies to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives [59]. In this context, interoperability entails the ability for forces, units, and/or systems to operate together, share common doctrine and procedures, and leverage each other's infrastructure and bases. Therefore, it transcends the scope of mere data exchange and becomes a facilitator of shared understanding and collaborative action. Ultimately, interoperability enables large scale systems to function smoothly, reducing duplication, enabling resource pooling, and creating synergies, leading to improved efficiency and effectiveness [59]. It is therefore a critical characteristic in large-scale systems design and management, impacting both system performance and cooperative ability.

In Network Theory, the Giant Component of a network is the largest connected component, containing a significant fraction of nodes of the entire network [60]. We denote the size of the giant component with C. For a connected network of N nodes, the size of the giant component is equal to N, i.e., $C = N$. The size of the giant component can reflect quantitatively the above Law Enforcement Assumption in the following sense. If C is decreasing significantly after removing—"neutralizing" a few intelligently selected nodes, then the terrorist network is considered fragmented, and therefore unable to operate

under real-world conditions. We define the **Interoperability** I_r of a terrorist network, after sequentially removing r nodes, as:

$$I_r = \frac{C_r}{C_0}$$

where:

C_0 is the initial *size* of the giant component, without any attack (node removal)

C_r is the size of the giant component after r sequential attacks (removals of nodes)

The above definition of Interoperability is actually the normalized index (taking values from 0 to 1) of the giant component size C_r, with respect to the initial-maximal size C_0. In this way, we can effectively compare several attack strategies (node removals) on terrorist networks with different giant component sizes.

We examine several attack strategies for sequentially removing nodes, based on different centrality criteria, reflecting distinct social roles in terrorist networks [48]:

(i) randomness (random node removal, averaging the results of 1000 interactions),
(ii) high strength centrality (participators),
(iii) high betweenness centrality (mediators),
(iv) high clustering coefficient centrality (team leaders),
(v) high *recalculated* strength centrality,
(vi) high *recalculated* betweenness centrality,
(vii) high *recalculated* clustering coefficient centrality

We also examine a greedy algorithm [61–64], which removes the node corresponding to the maximal decrease of Interoperability at each step.

The delineation of specific roles among the members within an organization is an integral part of the definition of a terrorist organization, according to common legal standards adopted by European Union member states [65,66]. These standards include four criteria for characterizing a group of individuals as a criminal organization: (a) An association of three or more individuals. (b) The presence of a structured organization with a hierarchy is characterized by clear differentiation in roles, including leadership, team leadership, and functional team members. (c) Engagement in criminal acts is subject to imprisonment. (d) Sustained duration of criminal activity. While law enforcement authorities typically find it straightforward to detect the execution of particular criminal deeds (condition c), recognize associations among persons (condition a), and observe the temporal evolution of criminal behavior (condition d), the verification of distinct roles within a criminal organization (condition b) often proves to be a complex and challenging task [50–55,67].

Centralities represent metrics that reflect the significance of each node, arising from the topology of links [17,18,23,48,68–72]. The prominence of nodes is determined by ranking them based on their centrality values. There are over a hundred such indicators that locally pertain to each individual node [17,18]. In this paper, the proposed strategies **(ii)–(iv)** pertain to the sequential removal of nodes with the highest values in strength centrality, betweenness centrality, and clustering coefficient. The mathematical definitions of these indicators are provided subsequently:

The degree of node i in a network of order N, is the number of connections of the node i and takes values from 0 to $N-1$. The value 0 indicates the absence of links and there are no self-loops. The normalized degree is the degree of centrality [48,60,73]:

$$DEG_\kappa = \frac{\sum_{\lambda=1}^{N} a_{\kappa\lambda}}{N-1},$$

where:

$a_{\kappa\lambda}$ is the $\kappa\lambda$—element of the adjacency matrix [17,18,60] of the network.

In the case of weighted networks, the weighted degree is known as strength [17,18,60]: $DEG_\kappa^{[w]} = \frac{\sum_{\lambda=1}^{N} w_{\kappa\lambda}}{N-1}$.

Betweenness centrality is a well-known index from Network Theory, which captures the role of *"mediator"*, allowing information to pass from one part of the network to the other. In other words, Betweenness centrality measures the ability of a node to act as a *"bridge"* between different network modules [18,48,74]. The betweenness centrality B_κ of node κ is defined as the sum of proportions of all shortest weighted paths (geodesics) between pairs of other nodes (except node κ) that pass through node κ:

$$B_\kappa = \frac{1}{(N-1)(N-2)} \cdot \sum_{\substack{\lambda=1 \\ \lambda \neq \kappa}}^{N} \sum_{\substack{\mu=1 \\ \mu \neq \kappa}}^{N} \frac{\sigma_{\lambda(\kappa)\mu}}{\sigma_{\lambda\mu}}$$

where $\sigma_{\lambda(\kappa)\mu}$ is the number of shortest weighted paths (geodesics) between nodes λ and μ (with $\kappa \neq \lambda$ and $\kappa \neq \mu$) that pass through node κ, while $\sigma_{\lambda\mu}$ is the total of shortest weighted paths (geodesics) between nodes λ and μ. The shortest weighted paths (geodesics) are identified on the transformed weight matrix: $-\ln(w_{\kappa\lambda})$ [75]. Term $\frac{1}{(N-1)(N-2)}$ normalizes the betweenness index in order to take values in the interval $[0, 1]$.

The neighborhood density of a node indicates the extent to which its first neighbors are linked to each other. The neighborhood density of node i, also known as the clustering coefficient of node κ is calculated from the formula [18,48]:

$$clu_\kappa = \frac{2E_\kappa}{\sqsubset_\kappa(\sqsubset_\kappa - 1)},$$

where E_κ is the number of links between the first neighbors of node κ and $\sqsubset_\kappa$ is the number of first neighbors of node κ.

The distinct social roles of nodes of the network according to the selected relevant criteria are assessed by the values of the corresponding centralities. For example, in the cooperation network of the employees of a company, the nodes with high degrees are the popular employees or the employees with many responsibilities. Betweenness centrality identifies the employees who act as mediators between different employees. The team players or teamworking nodes are the employees with a high clustering coefficient [48].

Greedy algorithms operate on the principle of finding a locally optimal solution at each step, with the aspiration that these local optima will collectively yield a global optimum. At each iteration, the choice that seems most advantageous at that specific moment is selected, without accounting for its long-term implications [61–64]. In the context of our study, the greedy algorithm functions by removing the node that results in the maximum possible decrease in Interoperability I_r at each step, irrespective of the future consequences of this choice.

For example, for the first node to be removed $(r = 1)$, the greedy algorithm will remove node κ, if the removal of this node minimizes Interoperability I_1. To be more specific, we provide below a brief description of how the greedy algorithm works (Table 1).

Taking into account Table 1, the output of the greedy algorithm is the set $\mathcal{V}_r$ of the r sequentially removed nodes, which is actually an *ordered* list, where the order matters. In addition, we acquired the corresponding *ordered* list $\{I_r\}_{r=0,1,2,\ldots}$ of the Interoperability values of the network. The above procedure starts on a fully connected network, and it is iteratively applied, until the network becomes completely fragmented, i.e., no connections exist (all nodes are isolated, $I_r = 0$). It is crucial to highlight that greedy algorithms do not always produce a globally optimal solution [61,63,76].

For strategies **(ii)–(iv)**, the calculation of nodes' centralities is realized only once at the beginning. On the contrary, for strategies **(v)–(vii)** with recalculation, the calculation of nodes' centralities is realized again after each attack-removal, due to the change of the network structure. We investigate several attack strategies on four real terrorist networks, which are briefly presented in Table 2.

Table 1. Brief description of the greedy algorithm.

Initial Values $r = 0$ $I_r = I_0 = 1$ $\mathcal{V}_s = \mathcal{V}$ $\mathcal{V}_r = \varnothing$	r is the number of removed nodes I_r is the Interoperability of the network after sequentially removing r nodes. Initially, for $r = 0$, we have $I_r = I_0 = 1$ $\mathcal{V}$ is the set of nodes-vertices of the network $\mathcal{V}_s$ is the set of *surviving* nodes-vertices $\mathcal{V}_r$ is the set of *removed* nodes-vertices
Iterative Loop While $I_r \neq 0$: • $r \longleftarrow r + 1$ • Remove node κ, if $I_r(\kappa) = \min_{\mu \in \mathcal{V}_s}\{I_r(\mu)\}$ • $\mathcal{V}_s \longleftarrow \mathcal{V}_s - \{\kappa\}$ • $\mathcal{V}_r \longleftarrow \mathcal{V}_r + \{\kappa\}$ • $I_r \longleftarrow I_r(\kappa)$	$I_r(\mu)$ is the Interoperability after sequentially removing r nodes, where the r-th node, is node μ: $I_r(\mu) = \frac{C_r(\mu)}{C_0}$ where: C_0 is the initial size of the giant component, without any node removal. $C_r(\mu)$ is the size of the giant component after sequentially removing r nodes, where the r-th node, is node μ.

Acquiring data on physical, face-to-face, social interactions among terrorists is a formidable challenge. This is because this kind of data are almost always classified or inappropriate for academic research [50–55]. Unlike most studies in this area, which rely on data from social media interactions [77–91], our work is grounded on real-world social ties among terrorists, namely physical face-to-face interactions. This kind of data is more reliable because social media interactions can be used for deliberately sharing false realities, aiming to mislead law enforcement agencies [92–96]. Also, physical, face-to-face, social interactions among terrorists are valuable for law enforcement agencies, aiming to "neutralize" key influential terrorists. On the contrary, data on social media interactions cannot be utilized for such operations [51–55]. Of course, there is always some possibility of unobserved or hidden nodes and connections, unknown even to law enforcement agencies. This case is out of the scope of this first exploratory work. Despite these limitations, it is crucial to derive insights based on the available data, as would be the practice in law enforcement operations. This study utilizes data drawn from two open-access databases: the John Jay and ARTIS Transnational Terrorism Database (JJATT) from John Jay College of Criminal Justice [97] and the Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University [98]. The datasets comprise information on four distinct terrorist organizations originating from different countries. These organizations exhibit the following shared attributes: (a) radical Islamic ideologies primarily drive their members, (b) their period of activity spans from the mid-1980s to the mid-2000s, (c) the datasets represent networks of physical contacts, and (d) the data includes a temporal element. The data are presented via coded identifiers representing individual organization members; the real names corresponding to these codes are unknown to the researchers. The first organization under consideration is the "Jamaah Islamiah Section of Indonesia" [99], which was under surveillance by the Indonesian police from 1985 to 2007 [100]. Its most notable act of terrorism occurred in 2004, with a major bombing of the Australian embassy in Jakarta, causing significant casualties [101]. The data illustrate the interactions of 27 organization members across 11 distinct periods [99]. The second organization is the "Hamburg Cell," monitored by U.S. and German intelligence services from 1985 to 2006 [102]. Members of this organization are believed to have played a significant role in orchestrating the 9/11 terrorist attacks [103]. The dataset documents the activities of 34 organization members over 15 time periods [102]. The third organization, "Al-Qaeda Section of Madrid," was under the watch of Spanish security services from 1985 to 2006 [104]. The organization's most devastating attack was carried out in 2003 when an explosive device was detonated on a train, resulting in numerous casualties [105]. The data details the activities of 54 organization members across 14 time periods [104]. The fourth organization, "Jamaah Islamiah Section of the Philippines," was under surveillance

by the Philippine security services from 1985 to 2006 [106]. This organization demonstrated high activity levels, with many bombings, the largest of which occurred in 2000 [53]. Notably, an attempt to carry out a substantial terrorist attack in 2005 was thwarted by a timely intervention from the security services [107]. The dataset reveals the activities of 16 organization members over 14 consecutive periods [106].

The early intervention of law enforcement authorities *to* prevent an impending terrorist attack is of utmost importance to ensuring economic, financial, and social stability. From our previously published research, the time of an impending terrorist attack can be timely revealed. More specifically, the violent fluctuations of betweenness centralization are a clear early sign of an impending terrorist attack [49]. Betweenness centralization is defined as [49,74]:

$$\mathrm{B} = \frac{\sum_{\kappa=1}^{N} \left(\max_{\nu=1,2,\ldots,N} \{\mathrm{B}_\nu\} - \mathrm{B}_\kappa \right)}{N-1},$$

where:

B_κ is the betweenness centrality of node κ.

Based on this finding, we select the best time-year for a network attack, i.e., for removing nodes (Table 2).

Table 2. Brief description of the 4 real terrorist networks.

Network	Terrorist Organization	Number of Nodes	Year of Significant Terrorist Attack	Selected Year for Removing Nodes
1	"Jamaah Islamiah Section of Indonesia" [99,100]	27	2004	2003
2	"Hamburg Cell" [102,103]	34	2001	2000
3	"Al-Qaeda Section of Madrid" [104,105]	54	2003	2002
4	"Jamaah Islamiah Section of the Philippines" [106,107]	16	2004	2003

3. Results

The sequence of nodes removed per strategy for each terrorist organization is presented in Tables 2–5. The damage of each strategy is evaluated in terms of Interoperability I_r. The results are presented for the 4 terrorist networks (Figures 1–4), illustrating the Interoperability I_r, after removing $r = 0, 1, 2, \ldots$ nodes, sequentially. The comprehensive numerical results, along with the calculations for the centrality measures, greedy algorithms, and betweenness centralization, are provided in the Supplementary Material (Tables S1–S4). We also present a set of illustrative figures to visualize the changes in network structures based on recalculated betweenness, as per attack strategy (**vi**). (Figures 5–8). The animated GIFs for all examined strategies are provided in the Supplementary Material (S5–S8). Data analysis was manually programmed using the R programming language to ensure full customization in addressing the specific problem under investigation. Subsequent relevant computations and result interpretation were automated through a prototype software developed in R (v. 4.3.1).

In Table 3, we present the sequential removal of nodes in the network of the terrorist organization "Jamaah Islamiah Section of Indonesia". The several strategies for node removal are based on selected centrality metrics, namely strength, betweenness, clustering coefficient, and the corresponding recalculated versions of them. We also test a greedy algorithm which removes the node corresponding to the maximal decrease of Interoperability I_r at each step. The coded node identifiers (e.g., X1579) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

Table 3. This table shows the sequential removal of nodes in the network of the terrorist organization 'Jamaah Islamiah Section of Indonesia'. The several strategies for node removal are based on selected centrality metrics, including a greedy algorithm. The coded node identifiers (e.g., X1579) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

Sequential Node Removal in "Jamaah Islamiah Section of Indonesia"							
	Strength Centrality	**Betweenness Centrality**	**Clustering Coefficient Centrality**	**Strength Centrality Recalculated**	**Betweenness Centrality Recalculated**	**Clustering Coefficient Centrality Recalculated**	**Greedy Algorithm**
Attack	Node	Node	Node	Node	Node	Node	Node
0	0	0	0	0	0	0	0
1	X1579	X1556	X1504	X1579	X1556	X1506	X1561
2	X177	X1561	X1563	X1595	X1580	X801	X1580
3	X1595	X1590	X1570	X1590	X1590	X1574	X1579
4	X1590	X1553	X1574	X1582	X1579	X1570	X1553
5	X1553	X1580	X801	X177	X1582	X1563	X577
6	X1556	X1579	X1506	X1580	X177	X1504	X1509
7	X1562	X1595	X177	X1562	X1595	X177	X177
8	X1580	X1562	X1553	X1556	X1562	X1561	X800
9	X1582	X1509	X1561	X1558	X1506	X1556	X1504
10	X1504	X1582	X1579	X1563	X801	X1558	X1507
11	X1561	X577	X1556	X1570	X1558	X1534	X1556
12	X1563	X177	X1562	X1553	X1534	X802	X1562
13	X1574	X1504	X1582	X1506	X802	X598	X1563
14	X577	X1563	X1595	X801	X598	X1595	X1570
15	X1570	X800	X1580	X1534	X1574	X1590	X1574
16	X598	X1507	X577	X802	X1570	X1582	X1582
17	X801	X1570	X800	X598	X1563	X1580	X1590
18	X1506	X1574	X1507	X1574	X1561	X1579	X1595
19	X800	X598	X1509	X1561	X1553	X1562	
20	X1509	X802	X1590	X1509	X1509	X1553	
21	X1534	X1534	X598	X1507	X1507	X1509	
22	X1558	X1558	X802	X1504	X1504	X1507	
23	X1507	X801	X1534	X800	X800	X800	
24	X802	X1506	X1558	X577	X577	X577	

Table 4. This table shows the sequential removal of nodes in the network of the terrorist organization 'Hamburg Cell'. The several strategies for node removal are based on selected centrality metrics, including a greedy algorithm. The coded node identifiers (e.g., X1017) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

Sequential Node Removal in "Hamburg Cell"							
	Strength Centrality	**Betweenness Centrality**	**Clustering Coefficient Centrality**	**Strength Centrality Recalculated**	**Betweenness Centrality Recalculated**	**Clustering Coefficient Centrality Recalculated**	**Greedy Algorithm**
Attack	Node	Node	Node	Node	Node	Node	Node
0	0	0	0	0	0	0	0
1	X64	X65	X1030	X64	X65	X1035	X65
2	X62	X60	X1032	X62	X64	X1032	X60
3	X1005	X61	X1035	X1005	X61	X1030	X61
4	X60	X62	X1017	X65	X62	X63	X1005
5	X61	X64	X1016	X61	X1005	X66	X63
6	X65	X1005	X66	X60	X60	X1017	X64
7	X66	X58	X63	X57	X66	X1016	X62
8	X57	X1017	X58	X63	X57	X60	X57
9	X63	X650	X60	X1017	X1039	X58	X58

Table 4. *Cont.*

Sequential Node Removal in "Hamburg Cell"							
	Strength Centrality	**Betweenness Centrality**	**Clustering Coefficient Centrality**	**Strength Centrality Recalculated**	**Betweenness Centrality Recalculated**	**Clustering Coefficient Centrality Recalculated**	**Greedy Algorithm**
10	X1016	X1016	X62	X1032	X1035	X62	X66
11	X1017	X57	X1005	X1012	X1034	X1005	X650
12	X1012	X66	X64	X1016	X1033	X650	X1011
13	X58	X1012	X61	X1039	X1032	X64	X1012
14	X1032	X1035	X1012	X1035	X1031	X1039	X1016
15	X650	X63	X65	X1034	X1030	X1034	
16	X1030	X1011	X57	X1033	X1017	X1033	
17	X1011	X1015	X650	X1031	X1016	X1031	
18	X1015	X1030	X1011	X1030	X1015	X1015	
19	X1034	X1031	X1015	X1015	X1012	X1012	
20	X1035	X1032	X1031	X1011	X1011	X1011	
21	X1039	X1033	X1033	X650	X650	X65	
22	X1031	X1034	X1034	X66	X63	X61	
23	X1033	X1039	X1039	X58	X58	X57	

Table 5. This table shows the sequential removal of nodes in the network of the terrorist organization 'Al-Qaeda Section of Madrid'. The several strategies for node removal are based on selected centrality metrics, including a greedy algorithm. The coded node identifiers (e.g., X3136) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

Sequential Node Removal in "Al-Qaeda Section of Madrid"							
	Strength Centrality	**Betweenness Centrality**	**Clustering Coefficient Centrality**	**Strength Centrality Recalculated**	**Betweenness Centrality Recalculated**	**Clustering Coefficient Centrality Recalculated**	**Greedy Algorithm**
Attack	Node	Node	Node	Node	Node	Node	Node
0	0	0	0	0	0	0	0
1	X3136	X3132	X3135	X3136	X3132	X3165	X3141
2	X3132	X3141	X3142	X3132	X3136	X3156	X3134
3	X3157	X3137	X3156	X3141	X3161	X3142	X3179
4	X3138	X3162	X3165	X3157	X3141	X3135	X3135
5	X3142	X3159	X3143	X3160	X3159	X3143	X3138
6	X3134	X3136	X3157	X3138	X3157	X3157	X3132
7	X3143	X3161	X3140	X3161	X3138	X3140	X3136
8	X3156	X3134	X3138	X3180	X3160	X3138	X3137
9	X3179	X3160	X3161	X3165	X3165	X3161	X3140
10	X3140	X3179	X3137	X3143	X3153	X3136	X3162
11	X3141	X3143	X3132	X3159	X3180	X3159	X3142
12	X3161	X3157	X3179	X3153	X3179	X3160	X3153
13	X3135	X3138	X3136	X3179	X3162	X3153	X3143
14	X3137	X3135	X3134	X3162	X3156	X3180	X3156
15	X3160	X3140	X3141	X3156	X3143	X3179	X3160
16	X3153	X3142	X3162	X3142	X3142	X3162	
17	X3162	X3156	X3180	X3140	X3140	X3141	
18	X3180	X3180	X3153	X3137	X3137	X3137	
19	X3165	X3153	X3160	X3134	X3134	X3134	
20	X3159	X3165	X3159	X3135	X3135	X3132	

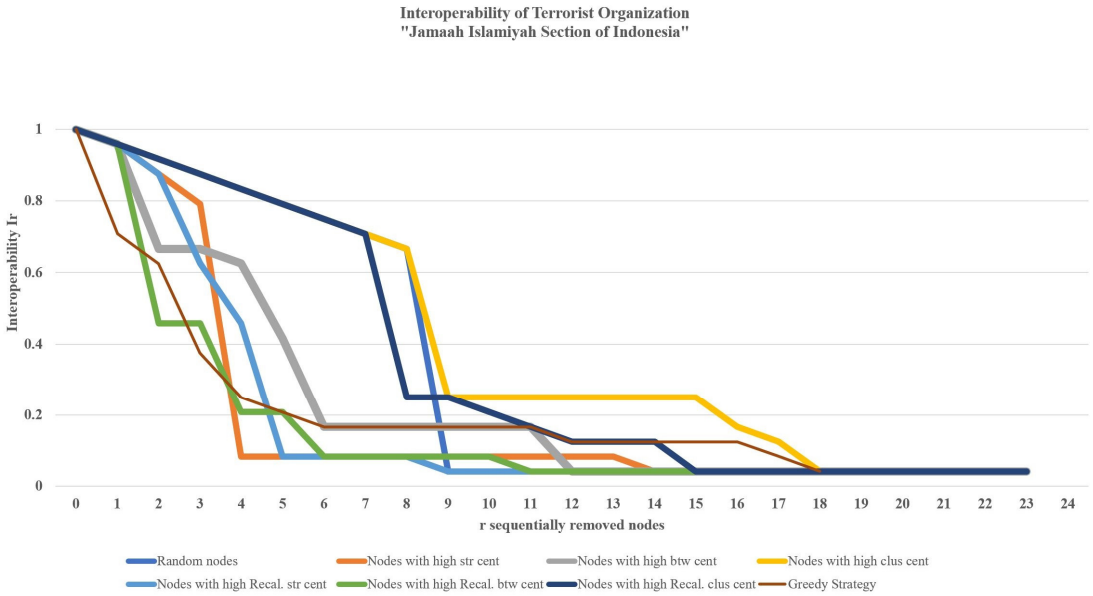

Figure 1. Interoperability I_r of terrorist network "Jamaah Islamiah Section of Indonesia" [99], after sequentially removing $r = 0, 1, 2, ..., 23$ nodes. The selected year for testing the eight attack strategies is 2003, as indicated in Table 1. Removing nodes based on recalculated betweenness is the most harmful, resulting in rapid network fragmentation. The interoperability drops significantly, even if only two nodes are removed ($I_2 < 0.5$).

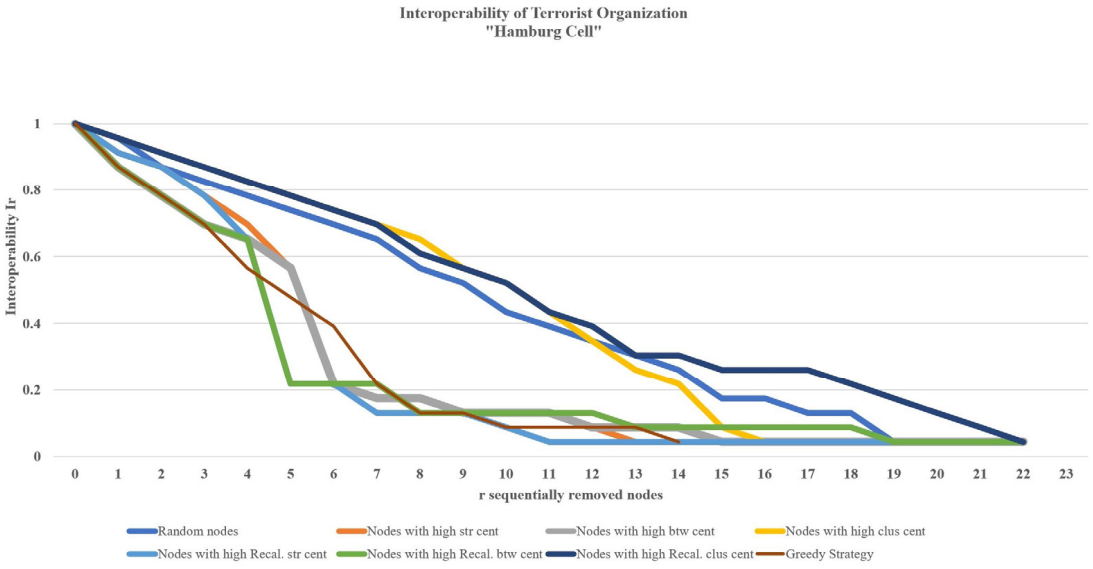

Figure 2. Interoperability I_r of terrorist network "Hamburg Cell" [102], after sequentially removing $r = 0, 1, 2, ..., 22$ nodes. The selected year for testing the eight attack strategies is 2000, as also indicated in Table 2. Removing nodes based on recalculated betweenness is the most harmful, resulting in rapid network fragmentation. The interoperability drops significantly if five nodes are removed ($I_5 = 0.2$).

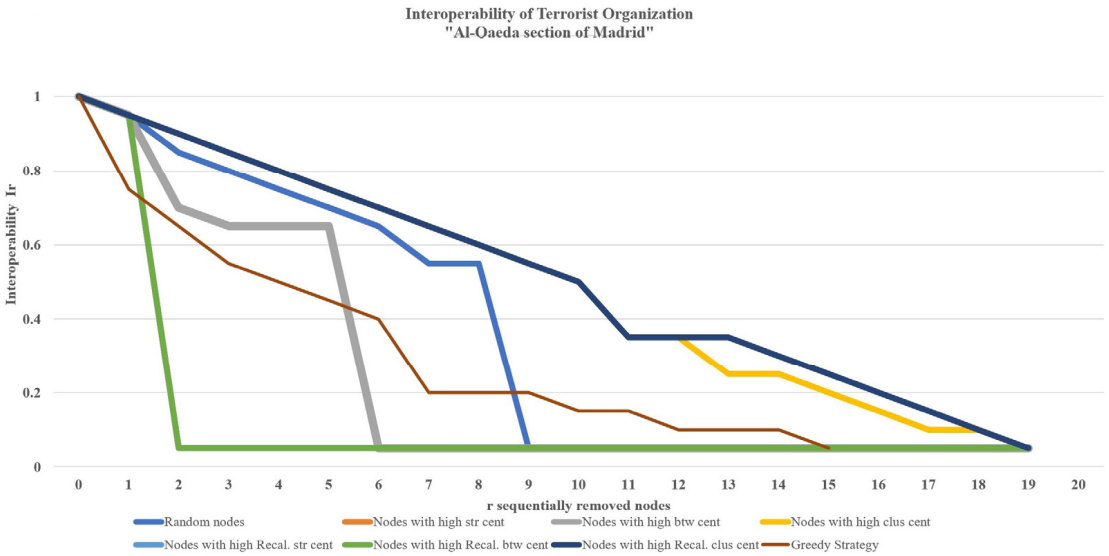

Figure 3. Interoperability I_r of terrorist network "Al-Qaeda Section of Madrid" [104], after sequentially removing $r = 0, 1, 2, ..., 19$ nodes. The selected year for testing the eight attack strategies is 2002, as also indicated in Table 2. Removing nodes based on recalculated betweenness or recalculated strength is equally the most harmful strategy (the two-color labels overlap in the diagram), resulting in rapid network fragmentation. The interoperability drops almost to zero, even if only *two* nodes are removed ($I_2 \approx 0$).

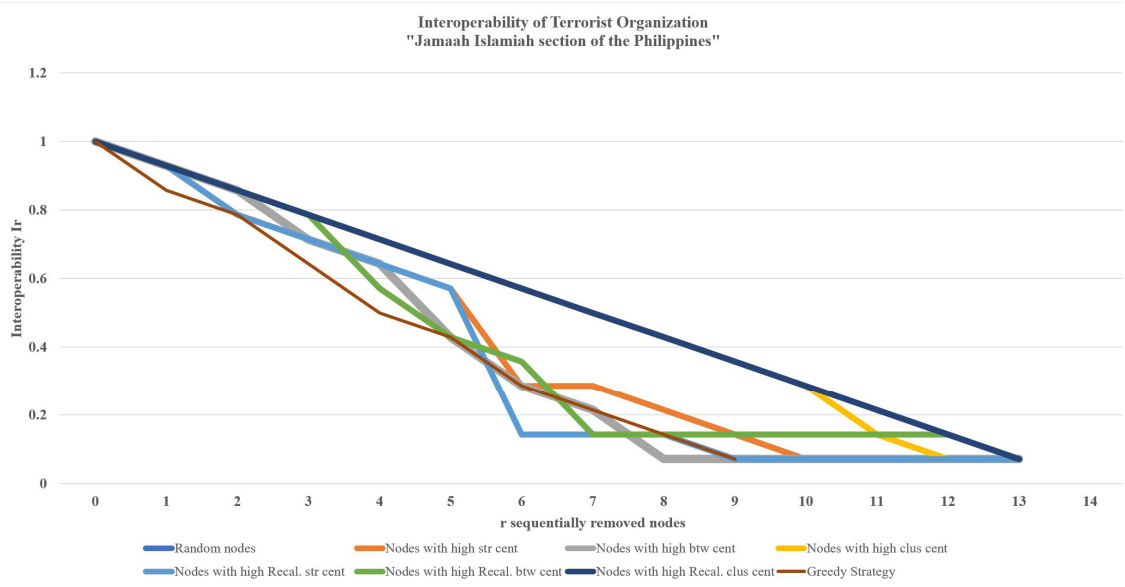

Figure 4. Interoperability I_r of terrorist network "Jamaah Islamiah Section of the Philippines" [106], after sequentially removing $r = 0, 1, 2, ..., 13$ nodes. The selected year for testing the eight attack strategies is 2003, as also indicated in Table 1. Removing nodes based on recalculated betweenness is equally or more harmful, compared to other strategies. The similar results of the eight different strategies are understandable due to the small size of the network, which is only 16 nodes, as also indicated in Table 1. It is worth mentioning that the removal of nodes based on recalculated clustering coefficient decreases the Interoperability I_r linearly with the number of removed nodes r.

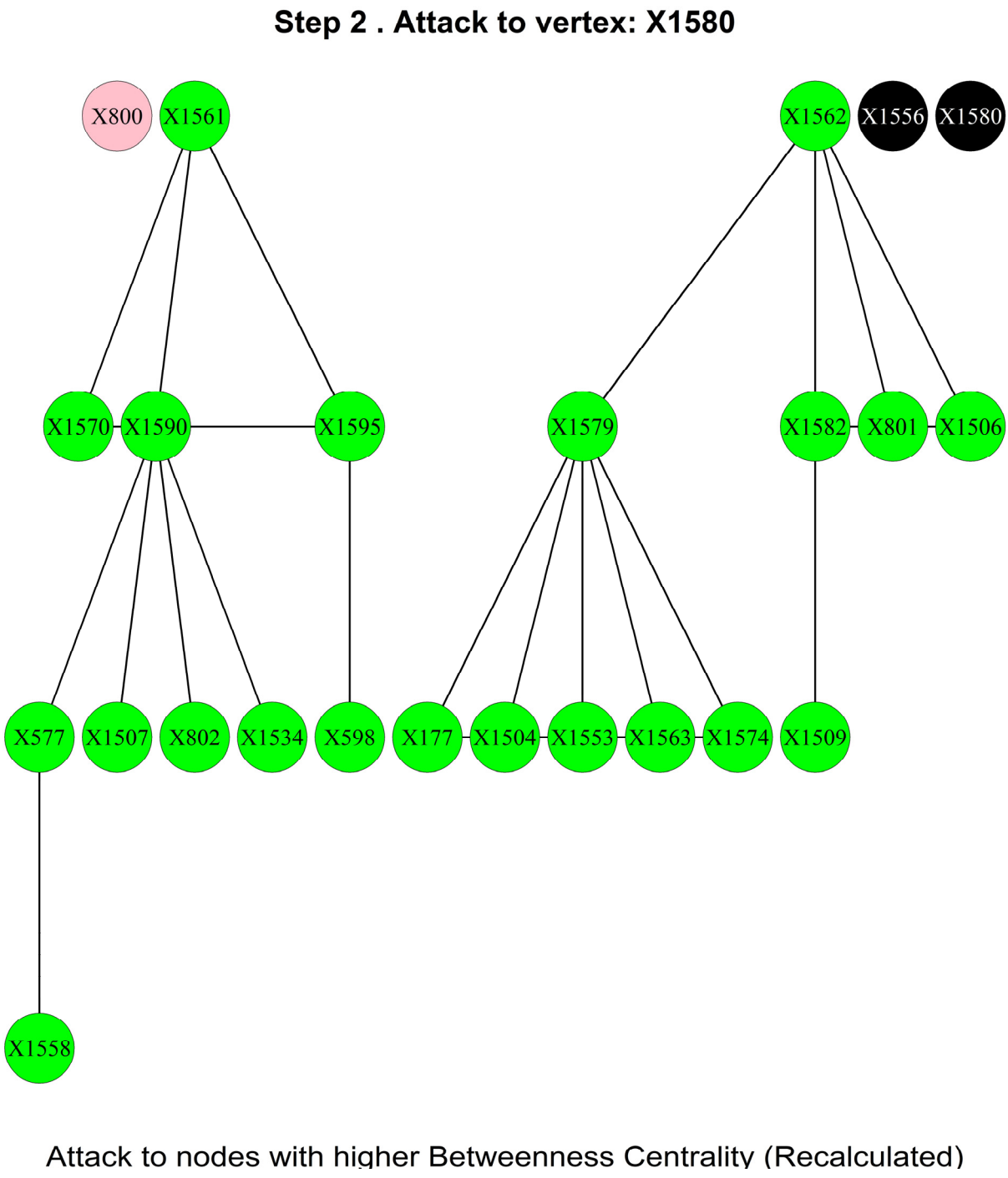

Figure 5. Image of the terrorist network "Jamaah Islamiah Section of Indonesia [99]", showing the network structure after the removal of two specific nodes based on recalculated betweenness (attack strategy **(vi)**). Removed nodes are indicated with Black color. Nodes that are still connected to the network are indicated with Green color. Nodes that become isolated, due to network attacks, are indicated with Pink color.

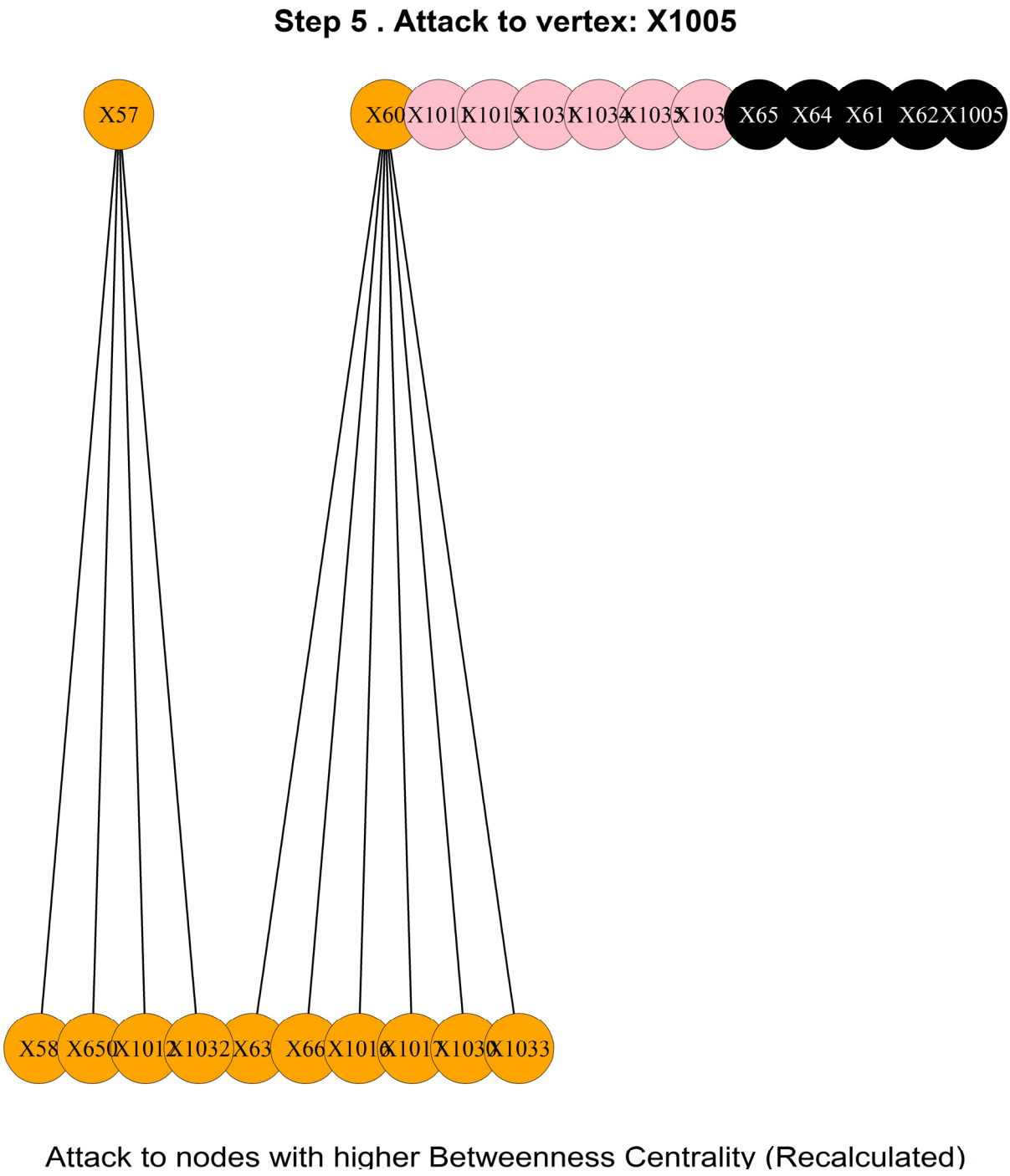

Figure 6. Image of the terrorist network "Hamburg Cell" [102], showing the network structure after the removal of five specific nodes based on recalculated betweenness (attack strategy **(vi)**). Removed nodes are indicated with Black color. Nodes that are still connected to the network are indicated with Orange color. Nodes that become isolated, due to network attacks, are indicated with Pink color.

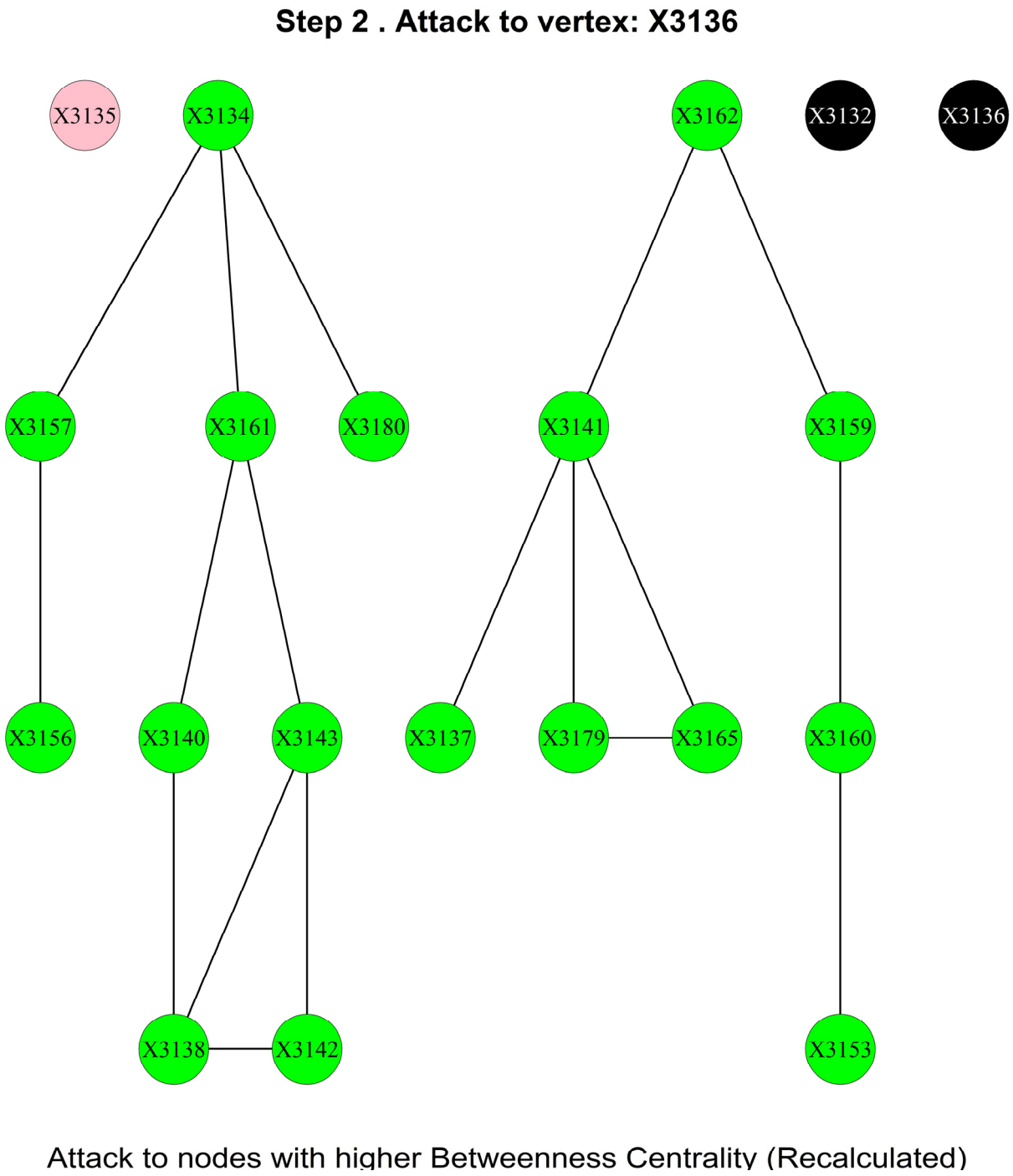

Figure 7. Image of the terrorist network "Al-Qaeda Section of Madrid" [104], showing the network structure after the removal of two specific nodes based on recalculated betweenness (attack strategy **(vi)**). Removed nodes are indicated with Black color. Nodes that are still connected to the network are indicated with Yellow color. Nodes that become isolated, due to network attacks, are indicated with Pink color.

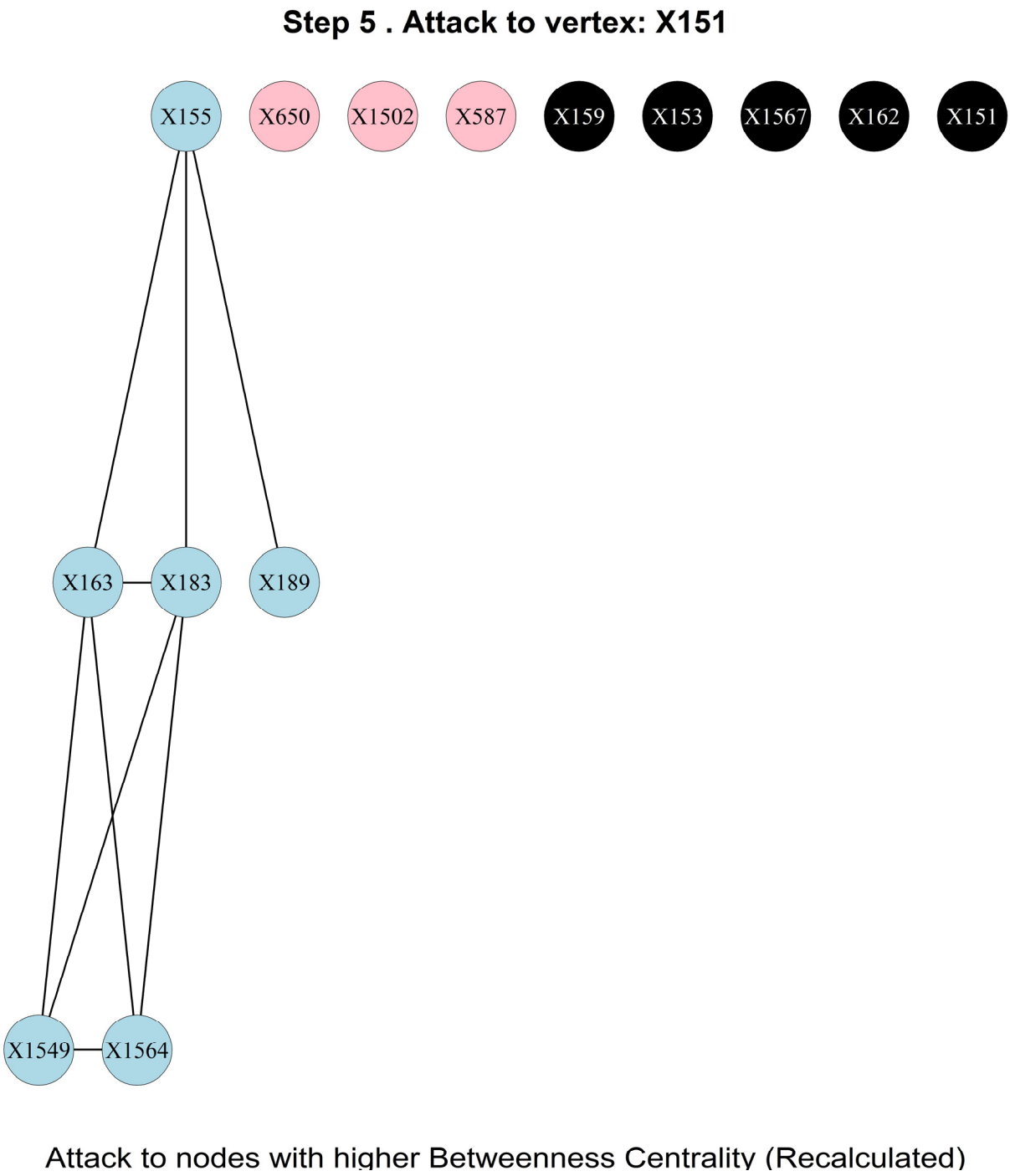

Figure 8. Image of the terrorist network "Jamaah Islamiah Section of Philippines" [106], showing the network structure after the removal of five specific nodes based on recalculated betweenness (attack strategy **(vi)**). Removed nodes are indicated with Black color. Nodes that are still connected to the network are indicated with a Light Blue color. Nodes that become isolated, due to network attacks, are indicated with Pink color.

While the sequence of removing nodes differs significantly between the different strategies, some nodes appear frequently in the early stages of removal across multiple strategies, suggesting their key role within the network (X1580, X1579).

In Table 4, we present the sequential removal of nodes in the network of the terrorist organization "Hamburg Cell". The several strategies for node removal are based on selected centrality metrics, namely strength, betweenness, clustering coefficient, and the

corresponding recalculated versions of them. We also test a greedy algorithm which removes the node corresponding to the maximal decrease of Interoperability I_r at each step. The coded node identifiers (e.g., X64) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

While the sequence of removing nodes differs significantly between the different strategies, some nodes appear frequently in the early stages of removal across multiple strategies, suggesting their key role within the network (X65, X1005).

In Table 5, we present the sequential removal of nodes in the network of the terrorist organization "Al-Qaeda Section of Madrid". The several strategies for node removal are based on selected centrality metrics, namely strength, betweenness, clustering coefficient, and the corresponding recalculated versions of them. We also test a greedy algorithm which removes the node corresponding to the maximal decrease of Interoperability I_r at each step. The coded node identifiers (e.g., X3136) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

While the sequence of removing nodes differs significantly between the different strategies, some nodes appear frequently in the early stages of removal across multiple strategies, suggesting their key role within the network (X3132, X3141).

In Table 6, we present the sequential removal of nodes in the network of the terrorist organization "Jamaah Islamiah Section of the Philippines". The several strategies for node removal are based on selected centrality metrics, namely strength, betweenness, clustering coefficient, and the corresponding recalculated versions of them. We also test a greedy algorithm which removes the node corresponding to the maximal decrease of Interoperability I_r at each step. The coded node identifiers (e.g., X153) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

Table 6. This table shows the sequential removal of nodes in the network of the terrorist organization 'Jamaah Islamiah Section of the Philippines'. The several strategies for node removal are based on selected centrality metrics, including a greedy algorithm. The coded node identifiers (e.g., X1567) correspond to unique members of the organization and are consistent with the encoding practices of the JJATT and CASOS databases.

Sequential Node Removal in "Jamaah Islamiah Section of the Philippines"							
	Strength Centrality	**Betweenness Centrality**	**Clustering Coefficient Centrality**	**Strength Centrality Recalculated**	**Betweenness Centrality Recalculated**	**Clustering Coefficient Centrality Recalculated**	**Greedy Algorithm**
Attack	Node	Node	Node	Node	Node	Node	Node
0	0	0	0	0	0	0	0
1	X153	X159	X189	X153	X159	X1564	X162
2	X162	X151	X650	X162	X153	X1549	X151
3	X163	X162	X1502	X1567	X1567	X1502	X153
4	X1567	X1567	X1549	X163	X162	X650	X155
5	X183	X153	X1564	X183	X151	X189	X159
6	X151	X155	X183	X151	X183	X159	X1567
7	X155	X163	X163	X159	X163	X1567	X163
8	X1549	X183	X155	X1564	X587	X183	X183
9	X1564	X189	X159	X189	X1564	X163	X1549
10	X159	X650	X1567	X587	X1549	X155	
11	X1502	X1502	X162	X1549	X1502	X153	
12	X189	X1549	X151	X1502	X650	X587	
13	X650	X1564	X153	X650	X189	X162	
14	X587	X587	X587	X155	X155	X151	

While the sequence of removing nodes differs significantly between the different strategies, some nodes appear frequently in the early stages of removal across multiple strategies, suggesting their key role within the network (X162, X153, X151).

A meticulous analysis of Figure 1 provides invaluable insights into the effects of node removal strategies on the network integrity of the terrorist organization, "Jamaah Islamiah Section of Indonesia," for the year 2003. The figure measures the network's Interoperability (I_r) after sequentially removing $r = 0, 1, 2, ..., 23$ nodes based on eight different attack strategies, which include Strength Centrality, Betweenness Centrality, Clustering Coefficient Centrality, and their recalculated variants, as well as a Greedy Algorithm.

One striking observation is the precipitous drop in interoperability when nodes are removed based on recalculated Betweenness Centrality. After the removal of only two nodes, the interoperability drops to a value of less than 0.5 ($I_{2,} < 0.5$), indicating rapid fragmentation of the network. This is in stark contrast to other strategies, such as Strength Centrality and Clustering Coefficient Centrality, which maintain higher levels of interoperability even after multiple node removals.

The Greedy Algorithm also results in a significant decline in interoperability, but not as rapidly as the recalculated Betweenness Centrality. It is evident that by the 9th attack, the interoperability falls to 0.1667, corroborating the efficacy of this algorithmic approach in dismantling the network.

Interestingly, the Betweenness Centrality strategy shows a steep decline in interoperability after the second node removal, reaching a value of 0.6667. However, this strategy is not as effective as its recalculated counterpart, further emphasizing the potency of recalculated metrics in disrupting the network.

In summary, Figure 1 strongly confirms the findings of this study that recalculated Betweenness Centrality is the most effective strategy for causing rapid network fragmentation, thereby incapacitating the terrorist organization. These insights could be pivotal for law enforcement agencies aiming to employ scientific tools in the fight against terrorism, allowing for more efficient and targeted interventions.

The analysis of Figure 2 offers a comprehensive understanding of the impact of various node removal strategies on the terrorist network known as the "Hamburg Cell" for the year 2000. This network's interoperability (I_r) was measured after sequentially removing $r = 0, 1, 2, ..., 23$ nodes based on eight different attack strategies.

One key observation is the catastrophic drop in interoperability when nodes are removed based on recalculated Betweenness Centrality. If five nodes are removed using this strategy, the interoperability of the network plummets to a mere 0.2 ($I_5 = 0.2$), indicating a swift fragmentation of the network. This sharp decline underlines the effectiveness of recalculated Betweenness Centrality in disrupting network integrity.

The Greedy Algorithm Strategy also shows promise in dismantling the network. By the 10th attack, interoperability drops to 0.0869, demonstrating its efficacy in network disruption, albeit not as rapidly as the recalculated Betweenness Centrality.

Contrastingly, other strategies like Strength Centrality and Clustering Coefficient Centrality show a slower rate of decline in network interoperability. For instance, after five nodes are removed using Strength Centrality, the interoperability is still at a relatively high level of 0.7391, suggesting that this strategy is less effective in immediate network fragmentation.

Notably, strategies like Betweenness Centrality also cause a significant decline in interoperability but not as dramatically as its recalculated counterpart. By the fifth attack, interoperability reaches 0.5652, which is significantly higher than the 0.2174 observed when using recalculated Betweenness Centrality.

In summary, Figure 2 provides compelling evidence that recalculated Betweenness Centrality is the most potent strategy for rapid network fragmentation in the case of the "Hamburg Cell." This information could be invaluable for law enforcement agencies using scientific approaches to disrupt the organizational structures of terrorist networks.

The analysis of Figure 3 provides an in-depth understanding of the impact of different node removal strategies on the terrorist network "Al-Qaeda Section of Madrid" for the year 2002. This network's interoperability (I_r) was measured after sequentially removing $r = 0, 1, 2, ..., 23$ nodes based on eight different attack strategies.

The most striking observation is the near-complete collapse of the network's interoperability when nodes are removed based on either recalculated Betweenness Centrality or recalculated Strength Centrality. According to the data, both strategies are equally effective in causing rapid network fragmentation. After removing just two nodes, the interoperability drops almost to zero ($I_2 \approx 0$), indicating extreme vulnerability in the network's structure to these particular attack strategies.

The Greedy Strategy also shows promise but is not as effective as the recalculated centrality metrics. By the tenth attack, interoperability drops to 0.15, which, while significant, is not as devastating as the almost zero interoperability caused by recalculated Betweenness and Strength Centrality.

Other strategies like Strength Centrality, Betweenness Centrality, and Clustering Coefficient Centrality also cause a decline in network interoperability but not as dramatically. For instance, after removing five nodes using Strength Centrality, the interoperability still stands at a relatively high 0.7. This suggests that these strategies are not as effective in causing immediate network fragmentation.

In summary, Figure 3 reveals that recalculated Betweenness Centrality and recalculated Strength Centrality are the most potent strategies for inducing rapid fragmentation in the case of the "Al-Qaeda Section of Madrid." This is a critical insight for law enforcement agencies and researchers who aim to disrupt such networks using scientific tools.

The analysis of Figure 4 sheds light on the resilience and vulnerabilities of the "Jamaah Islamiah Section of the Philippines" terrorist network for the year 2003. Given that this network is relatively small, consisting of only 16 nodes, the impact of node removal across different strategies tends to be similar. This is reflected in the relatively close values of interoperability (I_r) across the eight attack strategies as nodes are sequentially removed.

Notably, the removal of nodes based on recalculated Betweenness Centrality appears to be equally or more harmful compared to other strategies. This is indicative of the effectiveness of using recalculated betweenness as a strategy for causing rapid network fragmentation. For instance, after removing 6 nodes based on recalculated Betweenness Centrality, the interoperability plummets to a mere 0.1429, compared to 0.5714 when nodes are removed randomly.

It is worth noting that the removal of nodes based on recalculated Clustering Coefficient Centrality results in a linear decrease in interoperability with the number of nodes removed. This is a unique characteristic in this particular dataset and could be attributed to the small network size.

In summary, Figure 4 suggests that despite the small size of the "Jamaah Islamiah Section of the Philippines" network, certain attack strategies, especially those based on recalculated betweenness, can be highly effective in fragmenting the network. The small network size makes most strategies somewhat effective, but recalculated betweenness stands out as particularly potent. The linear decrease in interoperability when using a recalculated Clustering Coefficient is also an interesting behavior that may warrant further investigation, especially in the context of small networks.

In scrutinizing the data presented in Figure 5, one observes a remarkable pattern of network degradation when implementing the attack strategy based on recalculated betweenness centrality. The series of nodes sequentially removed—starting from X1556 and proceeding through to X577 [Table 3]—indicates a tactical dismantling of the "Jamaah Islamiah Section of Indonesia" terrorist network. Upon the removal of the first two nodes, X1556 and X1580, a significant drop in the Interoperability of the network is already discernible. The network structure undergoes a palpable fragmentation, as evidenced by the increasing number of nodes turning pink, signifying their isolation from the main component. As the removal progresses to the 15th step, the network has been

rendered largely non-operational. The nodes indicated in black, which have been removed, were clearly pivotal to the network's operational integrity. This particular attack strategy, focusing on recalculated betweenness centrality, appears to be highly effective in disrupting the network's capacity to function as a coherent unit. The insights gleaned from this figure stand as a testament to the potential efficacy of this approach in real-world counter-terrorism operations.

In Figure 6, the efficacy of the attack strategy based on recalculated betweenness centrality is further confirmed when applied to the "Hamburg Cell" terrorist network. The sequential removal of nodes, commencing with X65 and extending to X58 [Table 4], showcases a well-calibrated disruption of the network architecture. The nodes designated in black, which have been excised, are instrumental in maintaining the network's structural integrity. Shortly after the removal of the initial nodes, X65 and X64, there was a noticeable decline in the network's Interoperability. The network's primary component begins to disintegrate, as indicated by the escalating number of nodes turning pink, symbolizing their subsequent isolation. Furthermore, the nodes that remain connected are highlighted in orange, and their dwindling number signifies the degradation of the network's cohesion. By the time the fifteenth node is removed, the network has been substantially weakened, corroborating the effectiveness of this particular node-removal strategy based on recalculated betweenness centrality.

In Figure 7, the analytical focus shifts to the "Al-Qaeda Section of Madrid" terrorist network, where the application of the node-removal strategy based on recalculated betweenness centrality yields equally compelling results. Starting with the removal of node X3132 and progressing through to X3135 [Table 5], the network experiences a significant structural disintegration. Nodes marked in black, which have been removed, demonstrate their crucial roles in maintaining the network's functional coherence. As early as the removal of the first two nodes, X3132 and X3136, a discernible decrease in the network's Interoperability is evident. The network becomes increasingly fragmented, with a rise in nodes turning pink, signifying their isolation from the main component. The remaining connected nodes, denoted in yellow, also decline in number, attesting to the weakening of the network's overall structure. By the sixteenth step of node removal, the network is largely ineffectual, corroborating the potency of the strategy focusing on recalculated betweenness centrality.

In Figure 8, the subject of analysis is the "Jamaah Islamiah Section of the Philippines" terrorist network. Here again, the application of the node-removal strategy based on recalculated betweenness centrality proves to be notably efficacious. The data series commences with the removal of node X159 and continues through to node X155 [Table 6]. As nodes marked in black are systematically excised from the network, their essential roles in sustaining the network's functional integrity become evident. Notably, after the removal of just the first two nodes, X159 and X153, the network's Interoperability already shows a marked decrease. The process of fragmentation is visually captured by the increasing number of nodes turning pink, indicating their isolation from the main component. Conversely, the nodes that remain connected to the network, represented in light blue, diminish in number as the attack progresses, further confirming the effectiveness of this particular node-removal strategy. By the completion of the twelfth step, the network is substantially incapacitated, largely affirming the merits of focusing on recalculated betweenness centrality as an attack strategy.

These findings are in harmony with those from the "Jamaah Islamiah Section of Indonesia", "Hamburg Cell", and "Al-Qaeda Section of Madrid" networks, further bolstering the argument for the universal efficacy of this approach.

4. Discussion

The goal of this work is to examine the vulnerability of four terrorist networks under random and targeted attacks (node removal), namely: the Jamaah Islamiah Section in Indonesia, the Hamburg Cell, the Al-Qaeda Section of Madrid, and the Jamaah Islamiah

Section in the Philippines. By comparing the Interoperability scores in response to various node removal strategies, the following discussion provides actionable insights into the comparative efficacy of these methods. We focus on how these strategies can destabilize the network, ultimately offering valuable perspectives for counterterrorism initiatives.

From Figures 1 and 5, and Table 3 of the Jamaah Islamiah Section of Indonesia we observe the following. Initially, the procedure begins with the maximal possible Interoperability score equal to 1, denoting a fully (100%) functional network. A rapid decline of Interoperability is observed in all strategies. Attacking nodes randomly results in a moderate, consistent drop of Interoperability with a final score of 0.0417 after 24 episodes. Attacking nodes based on strength centrality results in a dramatic drop to 0.0833 by the 4th attack. Attacks based on betweenness centrality damage the network by the 2nd attack, achieving a score of 0.6667. Attacks based on clustering coefficient centrality are the least effective, as the network shows resilience, having a stable score of 0.25 after many episodes. Dynamic recalculations of centrality metrics highlight that betweenness centrality is the most effective strategy, lowering the score to 0.0417 by the twelfth attack, while recalculated strength centrality and clustering coefficient centrality are less harmful. The network is highly vulnerable to targeted attacks based on betweenness centrality, especially when betweenness centrality is recalculated dynamically, implying that counterterrorism strategies should prioritize these nodes for disruption.

Several key differences emerge when comparing the network interoperability of the Hamburg Cell organization (Figures 2 and 6 and Table 4) to that of the Jamaah Islamiah Section of Indonesia (Figures 1 and 5 and Table 3). First and foremost, the Hamburg Cell network is remarkably more resilient to random node attacks. The Interoperability score in this scenario drops only to 0.043478261 after 19–20 attacks, indicating the robustness against random attacks, which is not present in the Jamaah Islamiah network. However, this resilience seems to diminish when we focus on targeted strategies. Specifically, while attacks based on high strength centrality are initially harmful, their effectiveness lowered significantly, requiring 20 attacks to reach the critical Interoperability score. However, the highest vulnerability is observed when attacking nodes with high betweenness centrality. In this case, six attacks can reduce the Interoperability to the same low point. Clustering coefficient centrality does not perform well in both networks, namely the Hamburg Cell network and the Jamaah Islamiah Section of Indonesia. A total of 23 attacks are required to achieve the same low score of 0.043478261, rendering it the least effective of the tested strategies. Interestingly, dynamic recalculations, which generally make strategies more effective for the Jamaah Islamiah network, do not offer the same advantage against the Hamburg Cell. For instance, the recalculated strength centrality is surprisingly less effective than strength centrality, and the recalculated clustering coefficient centrality still needs to be more effective. Only the recalculated betweenness centrality maintains its extreme efficacy, reducing the score after two attacks. These results suggest that while the Hamburg Cell network is generally more resilient against random attacks, it is vulnerable to targeted attacks. In particular, even without dynamic recalculations, targeted strategies focusing on nodes with high betweenness centrality could be remarkably effective.

Analyzing Figures 3 and 7 and Table 5 concerning the Al-Qaeda Section of Madrid reveals a range of vulnerabilities and strengths regarding the network's resilience to various attack strategies. Several points of comparison with the Hamburg Cell (Figures 2 and 6, and Table 4) and the Jamaah Islamiah Section of Indonesia (Figures 1 and 5, and Table 3) can be identified. Random node attacks show that the network's Interoperability score drops to 0.05 after only 9–10 attacks. This indicates that the Al-Qaeda Section of Madrid is considerably less resilient to random attacks than the Hamburg Cell and even the Jamaah Islamiah Section of the Indonesia network. When targeting nodes based on strength centrality, the network shows an initial decrease in Interoperability but seems to stabilize at 0.05 after nine attacks. The recalculated strength centrality metrics show similar behavior, suggesting that while the network is quite robust against this strategy, it still has a significant level of vulnerability. Regarding betweenness centrality, the Al-Qaeda Section of the Madrid

network appears to be highly vulnerable. The Interoperability score falls dramatically to 0.05 after nine attacks. Notably, the high network vulnerability is present even when the metrics are recalculated, with the score remaining at 0.05 after 20 attacks. Here, recalculated betweenness or recalculated strength are equally the most harmful strategies, as indicated in the relevant diagram. This leads to rapid network fragmentation, while interoperability drops almost to zero even when only two nodes are removed. Clustering coefficient centrality is the least effective attack strategy, as it takes 20 attacks for the Interoperability score to drop to 0.05, both in "static" and recalculated forms. This confirms that generally, it is a strategy with low efficiency. In summary, the Al-Qaeda Section of Madrid presents a mixture of results concerning network resilience. While it is relatively less resilient to random node attacks, it demonstrates specific strengths and weaknesses against targeted strategies. Specifically, the greatest weak point is its high vulnerability to targeted attacks with high betweenness centrality. This result holds even when metrics are recalculated. On the other hand, it shows a better resilience against clustering coefficient centrality attacks, similar to the other networks examined. The Al-Qaeda Section of Madrid, in particular, would be significantly fragmented if the nodes of high betweenness centrality were removed, highlighting the importance of targeted strategies over random attacks.

The results concerning the Jamaah Islamiah Section of the Philippines reveals some intriguing patterns (Figures 4 and 8, and Table 5). However, it is important to note that the network size of this group is significantly smaller than other networks under consideration. This may introduce specific challenges when comparing the efficacy of various attack strategies. At the column of random node attack, where the experiment is running 1000 times, interoperability is relatively stable initially but decreases as more nodes are removed. Given the smaller network size, it is reasonable that the "correct" nodes—those significantly affecting network interoperability—are more likely to be targeted simply because fewer nodes exist. This could skew the results, making random attacks appear more effective in this particular setting than in larger networks. For Strength and Betweenness Centrality (recalculated or not) the interoperability also declines, though not always in the same manner. For instance, the impact on interoperability varies in the recalculated Strength and Betweenness Centrality attacks. This suggests that adaptive strategies may affect smaller networks differently than larger ones. In this smaller network, strategies involving Betweenness Centrality (recalculated or not) and Strength Centrality seem to impact significantly, leading to a rapid decline in interoperability. This could suggest that these strategies are particularly harmful in smaller networks, although it is tough to generalize this without additional data. The Clustering Coefficient Centrality (recalculated or not), also indicates a steady decrease in interoperability as nodes are removed. However, it does not drop as sharply as Betweenness and Strength Centrality. This could mean that this measure is less sensitive to the size of the network, but further research is needed to confirm this first impression. In summary, the size of this network could pose challenges for straightforward comparison with larger networks. Different attack strategies may yield different results depending on the network size, and smaller networks might be more vulnerable to certain types of attacks due to their limited structural complexity.

To sum up, from our findings concerning the four terrorist networks studied, it is clear that the strategy of recalculating betweenness centrality is the most effective in terms of interoperability. Although these networks manifest varying degrees of resistance to different kinds of attacks (random or targeted), the Achilles' heel seems to be the nodes with high betweenness centrality, especially when recalculated dynamically. Our analysis demonstrates the effectiveness of this strategy in 3 out of 4 networks (Figures 1–3) and is equally or more harmful in the fourth network, despite its smaller size (Figure 4, 16 nodes, Table 2). These findings concerning vulnerability on real face-to-face terrorist networks, could serve as the cornerstone for counter-terrorism, aiming to network fragmentation. The importance of context-dependent factors, such as the size of the network and its inherent resilience characteristics, should be taken into account. Particularly revealing was the remarkable effectiveness of the recalculated betweenness centrality strategy in the largest

network of our analysis (Figure 3, 54 nodes, Table 2). To optimize the effectiveness of the recalculated betweenness centrality, it is essential to update-recalculate the centrality score of each node after each removal, due to the dynamic nature of network structure. This highlights the necessity for law enforcement agencies to maintain real-time data concerning the ever-changing social ties among terrorists. Without timely updates, even a theoretically effective strategy could lose its effectiveness.

From Figures 1–4, we observe that the implementation of the greedy algorithm outperforms most of the other attack methods investigated in this study. More specifically, the greedy algorithm reduces the Interoperability quickly, resulting eventually in zero Interoperability. On the other hand, the recalculated betweenness centrality does not result eventually into zero Interoperability but achieves a greater drop of Interoperability cumulatively after a few attacks. This finding makes the recalculated betweenness centrality the best attack strategy, because the goal of law enforcement authorities is to attack only a few nodes, resulting in the greatest possible drop of Interoperability. Zeroing out interoperability by attacking many nodes is not a realistic scenario for law enforcement authorities. It is interesting to note that the greedy algorithm performs better compared to all non-recalculated centrality strategies. The dynamic aspect of recalculation, concerning the betweenness centrality strategy, is the key factor for outperforming the greedy algorithm. This finding highlights the importance of real-time monitoring and updating the relevant data concerning terrorist networks. Another drawback of the greedy algorithm is that the nodes for removal are not characterized by some specific role in the terrorist organization. On the contrary, the excellent results of recalculated betweenness centrality in all networks examined, suggest strongly that "mediators" are the best targets. Therefore, we can conclude that the role of "mediator" is the best for attack, and this is our insight provided to the law enforcement authorities.

More specifically, when examining the reduction of Interoperability (I_r) to a level below 50% ($I_r \leq 0.5$), it is observed that node removal based on recalculated betweenness centrality yields better results than the greedy algorithm (Figure 9). For instance, in the terrorist organization Jamaah Islamiah Section of Indonesia, Interoperability (I_r) values reach ≤ 0.5 after the removal of just two nodes based on recalculated betweenness centrality, while with the greedy algorithm, the value is higher at ≥ 0.6. In the case of the Hamburg Cell terrorist organization, five node removals may be required, but the Interoperability (I_r) drops to 0.21 using recalculated betweenness centrality, as opposed to 0.47 with the greedy algorithm. The most striking results are observed in the Al-Qaeda Section of Madrid. In this organization, with the removal of just two nodes, Interoperability (I_r) drops to ≤ 0.05 using recalculated betweenness centrality, whereas it remains at ≥ 0.65 with the greedy algorithm. Lastly, in the smaller terrorist organization Jamaah Islamiah Section of the Philippines, the Interoperability value is below 0.5 after the removal of five nodes for both node removal strategies.

Finally, it is worth mentioning that strategies of random node removal are the least effective because they require the elimination of numerous nodes to achieve a remarkable drop in network interoperability score. This highlights the crucial role of pre-attack network analysis in identifying the most effective points for intervention. Ignoring such research could lead to inefficient outcomes. Therefore, the tailored, data-driven, recalculated betweenness centrality approach emerges as an effective strategy and valuable tool for counterterrorism interventions.

While our study provides valuable insights into the effectiveness of various node removal strategies for network fragmentation, it is important to clarify that we are not in a position to recommend specific methods for carrying out these removals. Decisions involving arrest, detention, legal procedures, or any other form of intervention are subject to ethical, legal, and sociopolitical considerations that lie outside the scope of this analysis. These decisions require expertise in law, criminology, sociology, and ethical studies and must be made by applicable local, national, and international regulations. Our focus is

solely on the mathematical and network analysis aspects to aid counter-terrorism efforts from a theoretical standpoint.

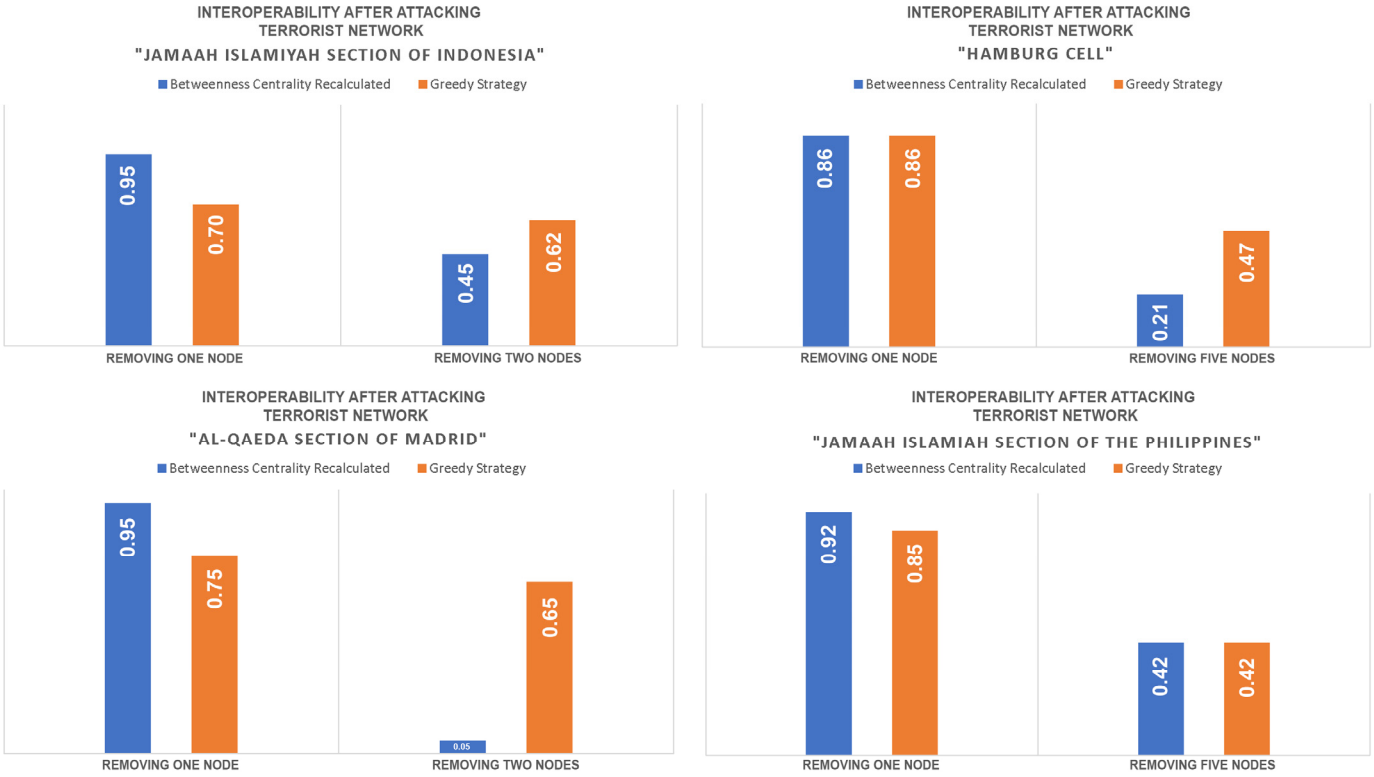

Figure 9. Comparative analysis of the impact of node removal based on recalculated betweenness centrality versus the greedy algorithm on the Interoperability (I_r) for specific terrorist organizations—Jamaah Islamiah Section of Indonesia, Hamburg Cell, Al-Qaeda Section of Madrid, and Jamaah Islamiah Section of the Philippines. The graph illustrates the reduction of Interoperability to levels below 0.5 following the removal of minimal nodes when utilizing recalculated betweenness centrality, in contrast to higher values achieved using the greedy algorithm.

Comparative Analysis with the Existing Literature

In the broader context of network science applied to counterterrorism, this study distinguishes itself in several noteworthy ways. While numerous studies have investigated targeted node removal strategies, the scope and methods often differ. For instance, research has been conducted on the effectiveness of various node removal strategies, but a majority of them rely heavily on synthetic or social media data [77–91]. In contrast, the current study leverages real-world data from face-to-face interactions within terrorist networks, adding a layer of practical relevance not universally present in the literature.

Additionally, many existing studies focus on a singular aspect of network centrality, such as degree centrality or betweenness centrality, to identify key nodes for targeted attacks [108–110]. Our research goes beyond this by examining a comprehensive set of seven different centrality metrics, thereby providing a more nuanced understanding of how different strategies impact the network's interoperability. This multi-metric approach has been explored less frequently in the existing literature [108,111–113]. The concept of 'Interoperability' as a measure for evaluating the effectiveness of node removal is also relatively unique to this study. Earlier works have primarily used measures like network efficiency [114–116]. Interoperability, as defined here, provides a more comprehensive understanding of how well parts of the network can still communicate after node removal, making it a robust metric for real-world application.

Furthermore, while some studies have employed machine learning algorithms for node classification and targeted removal [114–118], our study employs a greedy algorithm

in addition to centrality-based strategies, thus offering a more diverse range of approaches for practical implementation [119–121]. Importantly, the current study is one of the few to apply its methodology to multiple real-world terrorist networks [48,49,99,102,104,106]. This allows for a more robust validation of the strategies discussed and adds to the generalizability of the findings.

In summary, this study contributes to the existing body of knowledge by its unique focus on face-to-face interaction networks, its comprehensive approach to node centrality, and its application to multiple, real-world terrorist networks. These distinctions not only enrich the academic discourse but also offer actionable insights for law enforcement agencies.

5. Conclusions

The primary objective of this investigation is to identify the most effective attack strategy on terrorist networks, aiming to neutralize their operational ability. More specifically, we focus on attacks involving face-to-face human networks, specifically bombings, hijackings, and assassinations, rather than cyber-security. Extending our previously published research [48,49], this study examines seven different node removal strategies based on several centrality criteria in four terrorist networks. Each attack strategy is evaluated based on "Interoperability", estimated by the size of the giant component of the network. Unlike most studies in this area, which rely on data from social media interactions [77–91], our work is grounded in real-world social ties among terrorists, namely physical face-to-face interactions [48,49,99,102,104,106].

5.1. Key Findings

1. **Effectiveness of Recalculated Betweenness Centrality:** Removing nodes based on high recalculated betweenness centrality was found to be the most effective strategy in reducing Interoperability. The effectiveness of this strategy was observed universally across different-sized networks. The dynamic nature of recalculated betweenness centrality is the key factor for outperforming the greedy algorithm, highlighting the importance of updating network data, and reflecting the ever-changing nature of terrorist organizations. The above finding suggests strongly that nodes acting as "mediators" are the best targets, and this is our insight provided to the law enforcement authorities.
2. **Limitations of Random Node Removal:** Random node removal was less effective, emphasizing the importance of targeted interventions based on topological network analysis with centralities.
3. **Impact of Network Size:** While the main results hold for all four networks examined, the size of the network introduces nuances concerning the effectiveness of different strategies. This fact emphasizes the need for a tailored approach based on each network's characteristics.
4. **Critical Nodes for Counterterrorism:** Regardless of the network's structure, nodes with high betweenness centrality consistently emerged as critical points of vulnerability and thus represent optimal targets for counterterrorism efforts.

5.2. Implications and Contributions

These findings offer actionable insights for law enforcement agencies, aiding the development of more precise, real-time intervention strategies. They also underscore the necessity for ongoing data updates to reflect the dynamic nature of terrorist organizations. Furthermore, our study brings forth ethical, legal, and sociopolitical dimensions that must be considered when translating these insights into practice.

5.3. Future Directions

Given the pioneering nature of this work, future research could delve deeper into more complex models and additional centrality metrics. As the field matures, a comparative framework involving various real-world networks could provide even more nuanced insights.

In summary, this study makes a substantial contribution to the development of more effective, targeted, and globally applicable counterterrorism strategies, fulfilling a pressing need for data-driven, real-world relevant interventions in this critical domain.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/info14100580/s1, Table S1: Numerical Results for "Jamaah Islamiah Section of Indonesia"; Table S2: Numerical Results for "Hamburg Cell"; Table S3: Numerical Results for "Al-Qaeda Section of Madrid"; Table S4: Numerical Results for "Jamaah Islamiah Section of Philippines"; S5: Animated GIFs for "Jamaah Islamiah Section of Indonesia"; S6: Animated GIFs for "Hamburg Cell"; S7: Animated GIFs for "Al-Qaeda Section of Madrid"; S8: Animated GIFs for "Jamaah Islamiah Section of Philippines".

Author Contributions: Conceptualization, A.Z.S. and E.I.; methodology, A.Z.S. and E.I.; software, A.Z.S.; data curation, A.Z.S.; writing—original draft preparation, A.Z.S.; writing—review and editing, A.Z.S. and E.I.; visualization, A.Z.S.; supervision, I.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used in this study have been collected and published freely for academic-research use by the following organizations: **(1)** *John Jay & ARTIS Transnational Terrorism Database* (JJATT) http://doitapps.jjay.cuny.edu/jjatt/index.php (accessed on 31 December 2021); **(2)** *Center for Computational Analysis of Social and Organizational Systems* (CASOS) at Carnegie Mellon University http://www.casos.cs.cmu.edu/tools/datasets/external/index.php (accessed on 31 December 2021). Code numbers represent humans appeared in the dataset. The number–human correspondence is not provided to the data users.

Acknowledgments: The constructive comments of the reviewers improved significantly this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ganor, B. Trends in Modern International Terrorism. In *To Protect and To Serve: Policing in an Age of Terrorism*; Weisburd, D., Feucht, T., Hakimi, I., Mock, L., Perry, S., Eds.; Springer: New York, NY, USA, 2011; pp. 11–42. ISBN 978-0-387-73685-3.
2. Combs, C.C. *Terrorism in the Twenty-First Century*; Taylor & Francis: Abingdon, UK, 2022; ISBN 978-1-00-060984-4.
3. Richards, A. The Problem with 'Radicalization': The Remit of 'Prevent' and the Need to Refocus on Terrorism in the UK. *Int. Aff.* **2011**, *87*, 143–152. [CrossRef]
4. Tsintsadze-Maass, E.; Maass, R.W. Groupthink and Terrorist Radicalization. *Terror. Polit. Violence* **2014**, *26*, 735–758. [CrossRef]
5. Trimbur, M.; Amad, A.; Horn, M.; Thomas, P.; Fovet, T. Are Radicalization and Terrorism Associated with Psychiatric Disorders? A Systematic Review. *J. Psychiatr. Res.* **2021**, *141*, 214–222. [CrossRef]
6. Chermak, S.M. *Transnational Terrorism*; Routledge: Oxford, UK, 2019; ISBN 978-1-351-87782-4.
7. Ahmad, F.; Monaghan, J. Mapping Criminological Engagements Within Radicalization Studies. *Br. J. Criminol.* **2019**, *59*, 1288–1308. [CrossRef]
8. Kundnani, A. Radicalisation: The Journey of a Concept. *Race Cl.* **2012**, *54*, 3–25. [CrossRef]
9. Wolfowicz, M.; Litmanovitz, Y.; Weisburd, D.; Hasisi, B. What Is the State of the Quantitative Literature on Risk Factors for Radicalization and Recruitment to Terrorism? In *Understanding Recruitment to Organized Crime and Terrorism*; Weisburd, D., Savona, E.U., Hasisi, B., Calderoni, F., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 25–53. ISBN 978-3-030-36639-1.
10. Silke, A. Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalization. *Eur. J. Criminol.* **2008**, *5*, 99–123. [CrossRef]
11. Webber, D.; Kruglanski, A.W. Psychological Factors in Radicalization. In *The Handbook of the Criminology of Terrorism*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2016; pp. 33–46. ISBN 978-1-118-92398-6.
12. Stohl, C.; Stohl, M. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences. *Commun. Theory* **2007**, *17*, 93–124. [CrossRef]
13. Cherney, A. Working with Radicalised Individuals: Insights from a Secondary and Tertiary Prevention Program. *Behav. Sci. Terror. Polit. Aggress.* **2022**, *0*, 1–21. [CrossRef]
14. Cherney, A.; Putra, I.E.; Putera, V.S.; Erikha, F.; Magrie, M.F. The Push and Pull of Radicalization and Extremist Disengagement: The Application of Criminological Theory to Indonesian and Australian Cases of Radicalization. *J. Criminol.* **2021**, *54*, 407–424. [CrossRef]
15. Cherney, A. Designing and Implementing Programmes to Tackle Radicalization and Violent Extremism: Lessons from Criminology. *Dyn. Asymmetric Confl.* **2016**, *9*, 82–94. [CrossRef]

16. Rahimullah, R.H.; Larmar, S.; Abdalla, M. Radicalization and Terrorism: Research within the Australian Context. *Int. J. Criminol. Sociol.* **2013**, *2*, 180–185. [CrossRef]
17. Paolo, B.; Vigna, S. Axioms for Centrality. *Internet Math.* **2010**, *3–4*, 222–262.
18. Freeman, L.C. Centrality in Social Networks Conceptual Clarification. *Soc. Netw.* **1978**, *1*, 215–239. [CrossRef]
19. Kolaczyk, E.D.; Csárdi, G. Networked Experiments. In *Statistical Analysis of Network Data with R*; Springer International Publishing: Cham, Switzerland, 2020; pp. 187–205. ISBN 978-3-030-44129-6.
20. Kolaczyk, E.D.; Csárdi, G. Statistical Models for Network Graphs. In *Statistical Analysis of Network Data with R*; Springer International Publishing: Cham, Switzerland, 2020; pp. 87–113. ISBN 978-3-030-44129-6.
21. Kolaczyk, E.D.; Csárdi, G. Visualizing Network Data. In *Statistical Analysis of Network Data with R*; Springer International Publishing: Cham, Switzerland, 2020; pp. 29–41. ISBN 978-3-030-44129-6.
22. Kolaczyk, E.D.; Csárdi, G. Dynamic Networks. In *Statistical Analysis of Network Data with R*; Springer International Publishing: Cham, Switzerland, 2020; pp. 207–223. ISBN 978-3-030-44129-6.
23. Hughes, C.E.; Bright, D.A.; Chalmers, J. Social Network Analysis of Australian Poly-Drug Trafficking Networks: How do Drug Traffickers Manage Multiple Illicit Drugs? *Soc. Netw.* **2017**, *51*, 135–147. [CrossRef]
24. Marwell, G.; Oliver, P.E.; Prahl, R. Social Networks and Collective Action: A Theory of the Critical Mass. III. *Am. J. Sociol.* **1988**, *94*, 502–534. [CrossRef]
25. Das, K.; Samanta, S.; Pal, M. Study on Centrality Measures in Social Networks: A Survey. *Soc. Netw. Anal. Min.* **2018**, *8*, 13. [CrossRef]
26. Farooq, A.; Joyia, G.J.; Uzair, M.; Akram, U. Detection of Influential Nodes Using Social Networks Analysis Based on Network Metrics. In Proceedings of the 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 3–4 March 2018; pp. 1–6.
27. Li, G.; Hu, J.; Song, Y.; Yang, Y.; Li, H.-J. Analysis of the Terrorist Organization Alliance Network Based on Complex Network Theory. *IEEE Access* **2019**, *7*, 103854–103862. [CrossRef]
28. Fu, J.; Fan, Y.; Wang, Y.; Wang, S. Network Analysis of Terrorist Activities. *J. Syst. Sci. Complex.* **2014**, *27*, 1079–1094. [CrossRef]
29. Matusitz, J. Social Network Theory: A Comparative Analysis of the Jewish Revolt in Antiquity and the Cyber Terrorism Incident over Kosovo. *Inf. Secur. J. Glob. Perspect.* **2011**, *20*, 34–44. [CrossRef]
30. Xu, F.; Sun, D.; Li, Z.; Li, B. Exploring Structural Features of Terrorist Organization's Online Supporting Community via Social Network Modeling. In Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 13–16 December 2017; pp. 274–278.
31. Wang, T.; Krim, H. Statistical Classification of Social Networks. In Proceedings of the 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Kyoto, Japan, 25–30 March 2012; pp. 3977–3980.
32. Fu, J.; Chai, J.; Sun, D.; Wang, S. Multi-Factor Analysis of Terrorist Activities Based on Social Network. In Proceedings of the 2012 Fifth International Conference on Business Intelligence and Financial Engineering, Lanzhou, China, 18–21 August 2012; pp. 476–480.
33. Knoke, D. Emerging Trends in Social Network Analysis of Terrorism and Counterterrorism. In *Emerging Trends in the Social and Behavioral Sciences*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2015; pp. 1–15. ISBN 978-1-118-90077-2.
34. Elhajj, A.; Elsheikh, A.; Addam, O.; Alzohbi, M.; Zarour, O.; Aksaç, A.; Öztürk, O.; Özyer, T.; Ridley, M.; Alhajj, R. Estimating the Importance of Terrorists in a Terror Network. In *Mining Social Networks and Security Informatics*; Özyer, T., Erdem, Z., Rokne, J., Khoury, S., Eds.; Lecture Notes in Social Networks; Springer Netherlands: Dordrecht, The Netherlands, 2013; pp. 267–283. ISBN 978-94-007-6359-3.
35. Leuprecht, C.; Walther, O.; Skillicorn, D.B.; Ryde-Collins, H. Hezbollah's Global Tentacles: A Relational Approach to Convergence with Transnational Organized Crime. *Terror. Polit. Violence* **2017**, *29*, 902–921. [CrossRef]
36. Pilny, A.; Proulx, J.D. Using Interorganizational Communication Networks to Predict Terrorist Attacks. *Commun. Res.* **2022**, *49*, 3–32. [CrossRef]
37. Rai, A.K.; Kumar, S. Identifying the Leaders and Main Conspirators of the Attacks in Terrorist Networks. *ETRI J.* **2022**, *44*, 977–990. [CrossRef]
38. Mishra, A.K.; Rajpoot, V.; Bhardwaj, R.; Mishra, P.K.; Dwivedi, P. A Fuzzy-GA for Predicting Terrorist Networks in Social Media. In *Dark Web Pattern Recognition and Crime Analysis Using Machine Intelligence*; IGI Global: Pennsylvania, PA, USA, 2022; pp. 126–160. ISBN 978-1-66843-942-5.
39. Mithoo, P.; Kumar, M. A Role Of Link Analysis in Social Networking: A Survey. In Proceedings of the 2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Mangalore, India, 1–3 December 2022; Volume 7, pp. 272–275.
40. Iyer, S.; Killingback, T.; Sundaram, B.; Wang, Z. Attack Robustness and Centrality of Complex Networks. *PLoS ONE* **2013**, *8*, e59613. [CrossRef]
41. Zhu, W.; Liu, K.; Wang, M.; Yan, X. Enhancing Robustness of Metro Networks Using Strategic Defense. *Phys. Stat. Mech. Its Appl.* **2018**, *503*, 1081–1091. [CrossRef]
42. Piraveenan, M.; Uddin, S.; Chung, K.S.K. Measuring Topological Robustness of Networks under Sustained Targeted Attacks. In Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Istanbul, Turkey, 26–29 August 2012; pp. 38–45.

43. McMillan, C.; Felmlee, D.; Braines, D. Dynamic Patterns of Terrorist Networks: Efficiency and Security in the Evolution of Eleven Islamic Extremist Attack Networks. *J. Quant. Criminol.* **2020**, *36*, 559–581. [CrossRef]
44. Birkeland, M.S.; Heir, T. Making Connections: Exploring the Centrality of Posttraumatic Stress Symptoms and Covariates after a Terrorist Attack. *Eur. J. Psychotraumatol.* **2017**, *8*, 1333387. [CrossRef] [PubMed]
45. Asal, V.H.; Rethemeyer, R.K.; Anderson, I.; Stein, A.; Rizzo, J.; Rozea, M. The Softest of Targets: A Study on Terrorist Target Selection. *J. Appl. Secur. Res.* **2009**, *4*, 258–278. [CrossRef]
46. Zhang, L.; Zhao, Y.; Chen, D.; Zhang, X. Analysis of Network Robustness in Weighted and Unweighted Approaches: A Case Study of the Air Transport Network in the Belt and Road Region. *J. Adv. Transp.* **2021**, *2021*, e8810254. [CrossRef]
47. Jensen, M.A.; Ferguson, N.; Kane, S.; LaFree, G. Choosing Where to Fight: Do Social Networks Distinguish American ISIS Foreign Fighters from ISIS-Inspired Terrorists? *J. Confl. Resolut.* **2023**, *Vol. 0*, 00220027231164925. [CrossRef]
48. Spyropoulos, A.Z.; Bratsas, C.; Makris, G.C.; Ioannidis, E.; Tsiantos, V.; Antoniou, I. Entropy and Network Centralities as Intelligent Tools for the Investigation of Terrorist Organizations. *Entropy* **2021**, *23*, 1334. [CrossRef]
49. Spyropoulos, A.Z.; Bratsas, C.; Makris, G.C.; Ioannidis, E.; Tsiantos, V.; Antoniou, I. Investigation of Terrorist Organizations Using Intelligent Tools: A Dynamic Network Analysis with Weighted Links. *Mathematics* **2022**, *10*, 1092. [CrossRef]
50. Bongar, B.; Brown, L.M.; Beutler, L.E.; Breckenridge, J.N.; Zimbardo, P.G. *Psychology of Terrorism*; Oxford University Press: Oxford, UK, 2006; ISBN 0-19-803854-2.
51. Primoratz, I. State Terrorism and Counter-Terrorism. In *Terrorism: The Philosophical Issues*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 113–127.
52. Nester, W.R. Terrorism and Counterterrorism. In *Globalization, War, and Peace in the Twenty-First Century*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 77–94.
53. Braithwaite, A. The Logic of Public Fear in Terrorism and Counter-Terrorism. *J. Police Crim. Psychol.* **2013**, *28*, 95–101. [CrossRef]
54. Richardson, L. *The Roots of Terrorism*; Routledge: Oxford, UK, 2013; ISBN 1-135-44847-7.
55. Richardson, L. *What Terrorists Want: Understanding the Enemy, Containing the Threat*; Random House: New York, NY, USA, 2006; ISBN 1-58836-554-9.
56. Rezaei, R.; Chiew, T.K.; Lee, S.P. An Interoperability Model for Ultra Large Scale Systems. *Adv. Eng. Softw.* **2014**, *67*, 22–46. [CrossRef]
57. Geraci, A. *IEEE Standard Computer Dictionary: Compilation of IEEE Standard Computer Glossaries*; IEEE Press: Piscataway, NJ, USA, 1991; ISBN 1-55937-079-3.
58. Interoperability: Definition, Evaluation and Application. Available online: https://www.ffe.de/en/publications/interoperabilitaet-begriffsklaerung-bewertung-und-anwendung/ (accessed on 27 July 2023).
59. NATO Interoperability: Connecting Forces. Available online: https://www.nato.int/cps/en/natohq/topics_84112.htm (accessed on 27 July 2023).
60. Newman, M. *Networks*; Oxford University Press: Oxford, UK, 2018; ISBN 0-19-252749-5.
61. Vince, A. A Framework for the Greedy Algorithm. *Discrete Appl. Math.* **2002**, *121*, 247–260. [CrossRef]
62. Goyal, A.; Lu, W.; Lakshmanan, L.V.S. CELF++: Optimizing the Greedy Algorithm for Influence Maximization in Social Networks. In Proceedings of the 20th International Conference Companion on World Wide Web; Association for Computing Machinery, Hyderabad, India, 28 March–1 April 2021; pp. 47–48.
63. Edmonds, J. Matroids and the Greedy Algorithm. *Math. Program.* **1971**, *1*, 127–136. [CrossRef]
64. Heidari, M.; Asadpour, M.; Faili, H. SMG: Fast Scalable Greedy Algorithm for Influence Maximization in Social Networks. *Phys. Stat. Mech. Its Appl.* **2015**, *420*, 124–133. [CrossRef]
65. Council Of The European, European Union, Criminal Offence to Participate in a Criminal Organisation. *Off. J. Eur. Union* **1998**, *31998F0733*, 1–3.
66. The EU's Fight against Organised Crime. Available online: https://www.consilium.europa.eu/en/policies/eu-fight-against-crime/ (accessed on 10 July 2023).
67. Jackson, R.; Smyth, M.B.; Gunning, J. *Critical Terrorism Studies: A New Research Agenda*; Routledge: Oxford, UK, 2009; ISBN 978-1-134-05051-2.
68. Kolaczyk, E.D.; Csárdi, G. Network Topology Inference. In *Statistical Analysis of Network Data with R*; Springer International Publishing: Cham, Switzerland, 2020; pp. 115–140. ISBN 978-3-030-44129-6.
69. Rodríguez, J.A.; Estrada, E.; Gutiérrez, A. Functional Centrality in Graphs. *Linear Multilinear Algebra* **2007**, *55*, 293–302. [CrossRef]
70. Klein, D.J. Centrality Measure in Graphs. *J. Math. Chem.* **2010**, *47*, 1209–1223. [CrossRef]
71. Kolaczyk, E.D.; Csárdi, G. Modeling and Prediction for Processes on Network Graphs. In *Statistical Analysis of Network Data with R.*; Springer International Publishing: Cham, Switzerland, 2020; pp. 141–167. ISBN 978-3-030-44129-6.
72. Kolaczyk, E.D.; Csárdi, G. Descriptive Analysis of Network Graph Characteristics. In *Statistical Analysis of Network Data with R*; Springer International Publishing: Cham, Switzerland, 2020; pp. 43–68. ISBN 978-3-030-44129-6.
73. Wasserman, S.; Faust, K. *Social Network Analysis: Methods and Applications*; Cambridge University Press: Cambridge, UK, 1994; ISBN 978-0-521-38707-1.
74. White, D.R.; Borgatti, S.P. Betweenness Centrality Measures for Directed Graphs. *Soc. Netw.* **1994**, *16*, 335–346. [CrossRef]

75. Goñi, J.; van den Heuvel, M.P.; Avena-Koenigsberger, A.; Velez de Mendizabal, N.; Betzel, R.F.; Griffa, A.; Hagmann, P.; Corominas-Murtra, B.; Thiran, J.-P.; Sporns, O. Resting-Brain Functional Connectivity Predicted by Analytic Measures of Network Communication. *Proc. Natl. Acad. Sci. USA* **2014**, *111*, 833–838. [CrossRef]
76. Bang-Jensen, J.; Gutin, G.; Yeo, A. When the Greedy Algorithm Fails. *Discrete Optim.* **2004**, *1*, 121–127. [CrossRef]
77. Cuesta, Á.; Barrero, D.F.; R-Moreno, M.D. A Descriptive Analysis of Twitter Activity in Spanish around Boston Terror Attacks. In Proceedings of the Computational Collective Intelligence. Technologies and Applications: 5th International Conference, ICCCI 2013, Craiova, Romania, 11–13 September 2013; Proceedings 5. Springer: Berlin/Heidelberg, Germany, 2013; pp. 631–640.
78. Fischer-Preßler, D.; Schwemmer, C.; Fischbach, K. Collective Sense-Making in Times of Crisis: Connecting Terror Management Theory with Twitter User Reactions to the Berlin Terrorist Attack. *Comput. Hum. Behav.* **2019**, *100*, 138–151. [CrossRef]
79. Leenuse, M.L.; Pankaj, D.S. Detection and Prediction of Terrorist Activities and Threatening Events in Twitter-A Survey. In Proceedings of the 2023 International Conference on Control, Communication and Computing (ICCC), Thiruvananthapuram, India, 19–21 May 2023; IEEE, 2023; pp. 1–6.
80. Kusen, E.; Strembeck, M. Dynamics of Personal Responses to Terror Attacks: A Temporal Network Analysis Perspective. 2022. Available online: https://eprints.cs.univie.ac.at/7565/1/complexis22-responses.pdf (accessed on 6 June 2023).
81. Buntain, C.; Golbeck, J.; Liu, B.; LaFree, G. Evaluating Public Response to the Boston Marathon Bombing and Other Acts of Terrorism through Twitter. In Proceedings of the International AAAI Conference on Web and Social Media, Cologne, Germany, 17–20 May 2016; Volume 10, pp. 555–558.
82. Sarker, A.; Chakraborty, P.; Sha, S.S.; Khatun, M.; Hasan, M.R.; Banerjee, K. Improvised Technique for Analyzing Data and Detecting Terrorist Attack Using Machine Learning Approach Based on Twitter Data. *J. Comput. Commun.* **2020**, *8*, 50–62. [CrossRef]
83. Grobelscheg, L.; Sliwa, K.; Kušen, E.; Strembeck, M. On the Dynamics of Narratives of Crisis during Terror Attacks. In Proceedings of the 2022 Ninth International Conference on Social Networks Analysis, Management and Security (SNAMS), Milan, Italy, 29 November–1 December 2022; IEEE, 2022; pp. 1–8.
84. Ishengoma, F.R. Online Social Networks and Terrorism 2.0 in Developing Countries. *arXiv* **2014**, arXiv:14100531.
85. Schafer, V.; Truc, G.; Badouard, R.; Castex, L.; Musiani, F. Paris and Nice Terrorist Attacks: Exploring Twitter and Web Archives. *Media War Confl.* **2019**, *12*, 153–170. [CrossRef]
86. Najjar, E.; Al-augby, S. Sentiment Analysis Combination in Terrorist Detection on Twitter: A Brief Survey of Approaches and Techniques. *Res. Intell. Comput. Eng. Sel. Proc. RICE 2020* **2021**, *1254*, 231–240.
87. Garg, P.; Garg, H.; Ranga, V. Sentiment Analysis of the Uri Terror Attack Using Twitter. In Proceedings of the 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 5–6 May 2017; IEEE, 2017; pp. 17–20.
88. Giavazzi, F.; Iglhaut, F.; Lemoli, G.; Rubera, G. Terrorist Attacks, Cultural Incidents, and the Vote for Radical Parties: Analyzing Text from Twitter. *Am. J. Polit. Sci.* **2023**. [CrossRef]
89. Burnap, P.; Williams, M.L.; Sloan, L.; Rana, O.; Housley, W.; Edwards, A.; Knight, V.; Procter, R.; Voss, A. Tweeting the Terror: Modelling the Social Media Reaction to the Woolwich Terrorist Attack. *Soc. Netw. Anal. Min.* **2014**, *4*, 206. [CrossRef]
90. Simon, T.; Goldberg, A.; Aharonson-Daniel, L.; Leykin, D.; Adini, B. Twitter in the Cross Fire—The Use of Social Media in the Westgate Mall Terror Attack in Kenya. *PLoS ONE* **2014**, *9*, e104136. [CrossRef]
91. Arifin, V.; Jallow, F.B.; Lubis, A.; Bahaweres, R.B.; Rofiq, A.A. Using Deep Learning Model to Predict Terms Use by Terrorist to Pre-Plan an Attack on A Real-Time Twitter Tweets from Rapid Miner. In Proceedings of the 2022 10th International Conference on Cyber and IT Service Management (CITSM), Yogyakarta, Indonesia, 20–21 September 2022; IEEE, 2022; pp. 1–6.
92. Shu, K.; Bhattacharjee, A.; Alatawi, F.; Nazer, T.H.; Ding, K.; Karami, M.; Liu, H. Combating Disinformation in a social Media Age. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2020**, *10*, e1385. [CrossRef]
93. Aïmeur, E.; Amri, S.; Brassard, G. Fake News, Disinformation and Misinformation in Social Media: A review. *Soc. Netw. Anal. Min.* **2023**, *13*, 30. [CrossRef]
94. Nela, A.; Parruca, E. Impact of Social Media Disinformation and of Fake News Overexposure on the Actual Capacities and the Psychological Wellbeing During the COVID-19 Pandemic: A Systemic Literature Review. *Glob. Psychother.* **2023**, *3*, 126–132. [CrossRef]
95. Gottlieb, M.; Dyer, S. Information and Disinformation: Social Media in the COVID-19 Crisis. *Acad. Emerg. Med.* **2020**, *27*, 640. [CrossRef]
96. Bradshaw, S.; Howard, P.N. The Global Organization of Social Media Disinformation Campaigns. *J. Int. Aff.* **2018**, *71*, 23–32.
97. John Jay & ARTIS Transnational Terrorism Database. Available online: http://doitapps.jjay.cuny.edu/jjatt/index.php (accessed on 16 December 2021).
98. CASOS | Computational Analysis of Social and Organizational Systems (Carnegie Mellon University). Available online: http://www.casos.cs.cmu.edu/index.php (accessed on 26 June 2021).
99. John Jay & ARTIS Transnational Terrorism Database Austrailian Embassy Bombing Data Set [Data set] 2016. Available online: http://www.casos.cs.cmu.edu/index.php (accessed on 26 June 2021).
100. Jemaah Islamiyah—Wikipedia. Available online: https://en.wikipedia.org/w/index.php?title=Jemaah_Islamiyah&oldid=1025043319 (accessed on 26 June 2021).
101. Australian Embassy Bombing in Jakarta—Wikipedia. Available online: https://en.wikipedia.org/wiki/Australian_Embassy_bombing_in_Jakarta (accessed on 10 August 2021).

102. John Jay & ARTIS Transnational Terrorism Database Hamburg Cell 9/11 [Data Set] 2001. Available online: http://www.casos.cs.cmu.edu/index.php (accessed on 26 June 2021).
103. Hamburg Cell—Wikipedia. Available online: https://en.wikipedia.org/w/index.php?title=Hamburg_cell&oldid=977822420 (accessed on 10 August 2021).
104. John Jay & ARTIS Transnational Terrorism Database Madrid Train Bombing 2004 [Data Set] 2004. Available online: http://www.casos.cs.cmu.edu/index.php (accessed on 26 June 2021).
105. Madrid Train Bombings—Wikipedia. 2004. Available online: https://en.wikipedia.org/w/index.php?title=2004_Madrid_train_bombings&oldid=1037095728 (accessed on 10 August 2021).
106. John Jay & ARTIS Transnational Terrorism Database Phillippines Bombing [Data Set] 2000. Available online: http://www.casos.cs.cmu.edu/index.php (accessed on 26 June 2021).
107. Rizal Day Bombings—Wikipedia. Available online: https://en.wikipedia.org/w/index.php?title=Rizal_Day_bombings&oldid=1033689495 (accessed on 10 August 2021).
108. Cunningham, S.F.E. Dan Terrorist Network Adaptation to a Changing Environment. In *Crime and Networks*; Routledge: Oxford, UK, 2013; ISBN 978-1-315-88501-8.
109. Xu, J.; Hu, D.; Chen, H. The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad. *J. Homel. Secur. Emerg. Manag.* **2009**, *6*. [CrossRef]
110. Karthika, S.; Geetha, R.; Bose, S. Whom to Remove? Breaking the Covert Network. In Proceedings of the 2013 Fifth International Conference on Advanced Computing (ICoAC), Chennai, India, 18–20 December 2013; pp. 348–354.
111. Elmhadhbi, L.; Karray, M.-H.; Archimède, B.; Otte, J.N.; Smith, B. An Ontological Approach to Enhancing Information Sharing in Disaster Response. *Information* **2021**, *12*, 432. [CrossRef]
112. Hu, D. Analysis and Applications of Social Network Formation. Ph.D. Thesis, University of Arizona, Tucson, AZ, USA, 2009.
113. Reis, J.; Amorim, M.; Melão, N.; Cohen, Y.; Costa, J. Counterintelligence Technologies: An Exploratory Case Study of Preliminary Credibility Assessment Screening System in the Afghan National Defense and Security Forces. *Information* **2021**, *12*, 122. [CrossRef]
114. Scripps, J.; Tan, P.-N.; Esfahanian, A.-H. Exploration of Link Structure and Community-Based Node Roles in Network Analysis. In Proceedings of the Seventh IEEE International Conference on Data Mining (ICDM 2007), Omaha, NE, USA, 28–31 October 2007; pp. 649–654.
115. Ji, J.; Wu, G.; Duan, C.; Ren, Y.; Wang, Z. Greedily Remove k Links to Hide Important Individuals in Social Network. In Proceedings of the Security and Privacy in Social Networks and Big Data; Meng, W., Furnell, S., Eds.; Springer: Singapore, 2019; pp. 223–237.
116. Christopoulos, K.; Baltsou, G.; Tsichlas, K. Local Community Detection in Graph Streams with Anchors. *Information* **2023**, *14*, 332. [CrossRef]
117. Camacho, D.; Luzón, M.V.; Cambria, E. New Research Methods & Algorithms in Social Network Analysis. *Future Gener. Comput. Syst.* **2021**, *114*, 290–293. [CrossRef]
118. Ballinger, O. Insurgency as Complex Network: Image Co-Appearance and Hierarchy in the PKK. *Soc. Netw.* **2023**, *74*, 182–205. [CrossRef]
119. Choudhary, P. A Survey on Social Network Analysis for Counter-Terrorism. *Int. J. Comput. Appl.* **2015**, *112*, 24–29.
120. Carley, K. Dynamic Network Analysis for Counter-Terrorism. 2005. Available online: https://www.researchgate.net/profile/Kathleen-Carley/publication/228770516_Dynamic_network_analysis_for_counter-terrorism/links/00b7d517d66cece937000000/Dynamic-network-analysis-for-counter-terrorism.pdf (accessed on 20 June 2023).
121. Scott, J.; Carrington, P.J. The SAGE Handbook of Social Network Analysis. SAGE: Newcastle upon Tyne, UK, 2011; ISBN 978-1-4462-5011-2.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.