Interdisciplinary Description of Complex Systems 3(1), 27-43, 2005

ABOUT MODELLING OF COMPLEX NETWORKS WITH APPLICATIONS TO TERRORIST GROUP MODELLING

Dražen Penzar[1,*], Armano Srbljinović[2]

[1]Soko Z. I.
Zagreb, Croatia

[2]Croatian MoD's Institute for R&D of Defence Systems
Zagreb, Croatia

Regular paper *Received*: 12 May 2005. *Accepted*: 30. September 2005.

SUMMARY

Based on available data on various organisations and networks, the article explores some key properties of the structure of a terrorist organisation. Analytical focus is on lower levels of organisational hierarchy, where network structure with exponential distribution of the number of links among network nodes is clearly visible. Such networks tend to grow organically, are very efficient in information diffusion, and are robust regarding stochastic failures and targeted attacks. These network features are illustrated by recent example based on network data about September 11, 2001 attacks on New York and Washington.

KEY WORDS

complex networks, network structure, network properties

CLASSIFICATION

APA: 3020, 2910

PACS: 89.75.Hc

*Corresponding author, η: drazen.penzar@soko.hr; +385 1 4855 422;
Soko Z. I., Hebrangova 33, HR – 10000 Zagreb, Croatia

INTRODUCTION

After catastrophic terrorist attacks by kidnapped airlines on New York and Washington in September 2001 the interest for al-Qaeda terrorist organisation in public and media rose immediately. Experts and analysts all over the world started to offer various explanations of al-Qaeda's origins, membership recruitment, modes of operation, as well as of possible ways of its disruption. Journalists in search of hot topics took over and publicized most of the publicly available materials, often revising them further and making them even more intriguing and attractive for wide audiences.

One could thus read or hear that al-Qaeda is "a net that contains independent intelligence", that it "functions as a swarm", that it "gathers from nowhere and disappears after action", that it is "an *ad hoc* network", "an atypical organisation", extremely hard to destroy, especially by traditional anti-terrorist methods. In a similar tone, the day after July 7, 2005 simultaneous explosions in London subway British Home Secretary referred to the attack as coming "out of the blue in a way that there was no knowledge of beforehand in any respect whatsoever" [1]. This statement is all the more surprising when we know that many state intelligence and security services have been exerting serious efforts for more than four years in attempting to disrupt al-Qaeda network. Descriptions like the ones above sound extraordinary, sometimes almost fantastic, and provoke questions such as which master mind, if any, created such powerful organisation and what efforts are needed to put it into operation. Fortunately, the amount of concrete data and facts on al-Qaeda and similar organisations is constantly growing and our understanding of their ways of functioning is improving.

The main purpose of this article is to shed some light on the structure of contemporary, relatively decentralised terrorist organisations of which al-Qaeda is a primary example. The intent is also to show how and why these networked organisations possess particular properties. As we shall see, many of these regularities are common for a whole spectrum of organisational forms, of which terrorist organisations are only a small part.

HIERARCHICAL ELEMENTS OF ORGANISATIONAL STRUCTURE

Military, paramilitary and other similar organisations have usually been associated with hierarchical structure. Execution of orders without complaints, minimal deviation from plans, close coordination resulting from strict division of labour, and precise common guidelines are all deemed necessary for the efficiency and control of such organisations.

Numerous terrorist organisations, especially those preoccupied with ideological or nationalist goals, are structured according to similar principles. Although this may sound paradoxical, these organisations attempt to strictly control the amount of violence. Violence is usually subordinate to the achievement of other, often political, goals such as acquiring sympathies in public, attracting attention, exerting pressure needed for political negotiations, exhausting the opposing side, and lowering its morale. For example, it is probably more than a pure coincidence that the IRA refrained from using violence some ten days after the London subway attacks [2]. The desire to distinguish itself from perpetrators of massive, non-discriminating violent acts was likely one of the factors influencing IRA's decision. To control the amount of violence it is necessary that organisation's "political arms" control terrorist activities. Lower-ranking members need to be under strict control of higher headquarters in order to prevent undesirable individual transgressions. This is why the organisations like the Red Brigades, ETA, or IRA are strictly hierarchically structured [3] (see Fig. 1 also).

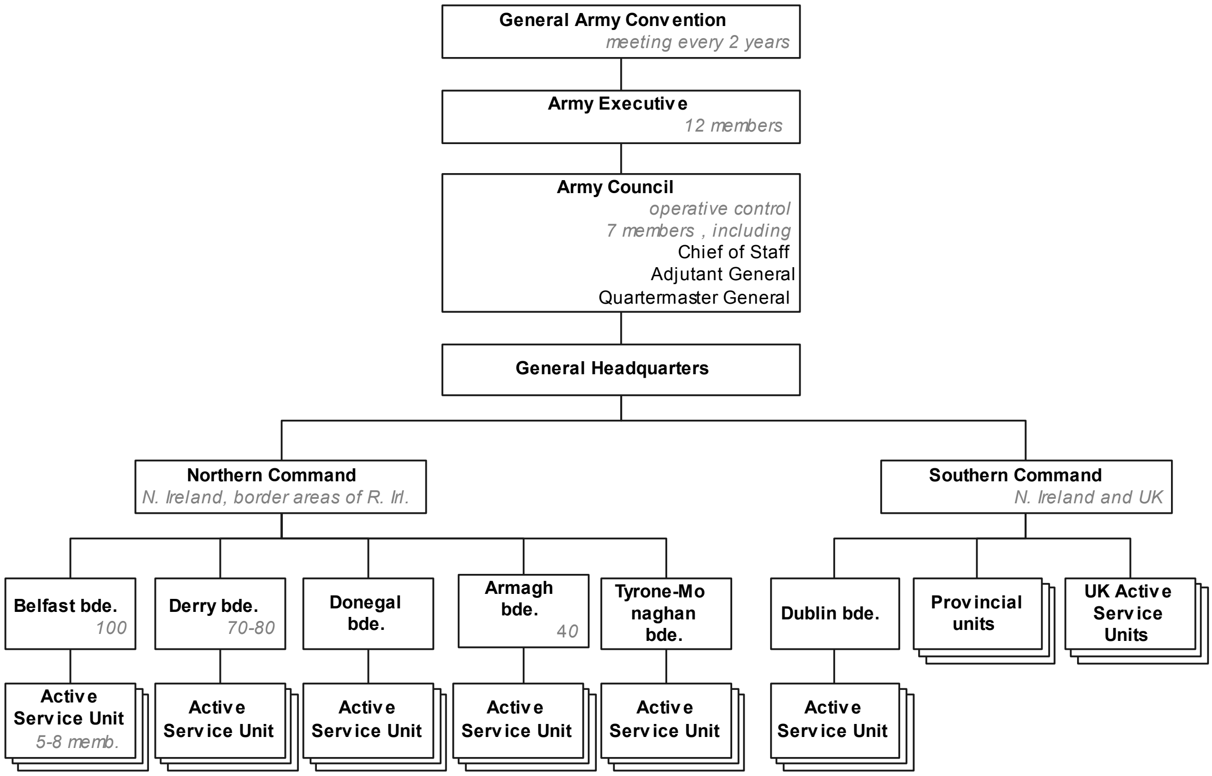

Figure 1. Organisational structure of the IRA in the second half of the nineties: hierarchical organisation with territorially organised divisions (based on [4]).

relatively recently are oriented towards maximisation of casualties and terror. For them, terror is more the aim in itself, than it is the means of political fight. Such groups have much less interest in maintaining strict hierarchical structure, which would ensure operative control over terrorist activities. One of such groups is al-Qaeda, especially when viewed as a wider structure encompassing various groups and individuals inspired by the spiritual leadership of Osama bin Laden.

Al-Qaeda in a narrower sense, as an organisation formed and led by bin Laden, also possesses hierarchical structure [5 – 7], but hierarchy is only one form of its complex structuring. Figure 2 presents the top of al-Qaeda organisation in the way the organisation of corporations or public institutions is usually depicted. The organisation is headed by Emir – the leader, which is the indisputable position of Osama bin Laden. The Emir is supported by Shura or the High Council, the activities of which are not much known of. In 2001 Shura supposedly had twenty to thirty members, many of which were not living in Afghanistan. Members of Shura have high authority and high degree of freedom, but are at the same time absolutely loyal to bin Laden and the organisation. The frequency of their meetings, their ways of communication, and the content of Shura's decisions are not publicly known.

In 2001 al-Qaeda had four organisational units, called committees, responsible for political and religious, financial, military, including terrorist, activities, and for propaganda and relations with media (Fig. 2). Military committee consisted of three departments. One of them was responsible for external military activities conducted during nineties in Chechnya, Bosnia, Kashmir, and perhaps some other countries affected by wars. Another department supervised terrorist operations all over the world. The third one was responsible for internal operations in Afghanistan, where al-Qaeda had entire military units. Special training camps were managed by this department and used for recruitment and training of new members from all over the world.

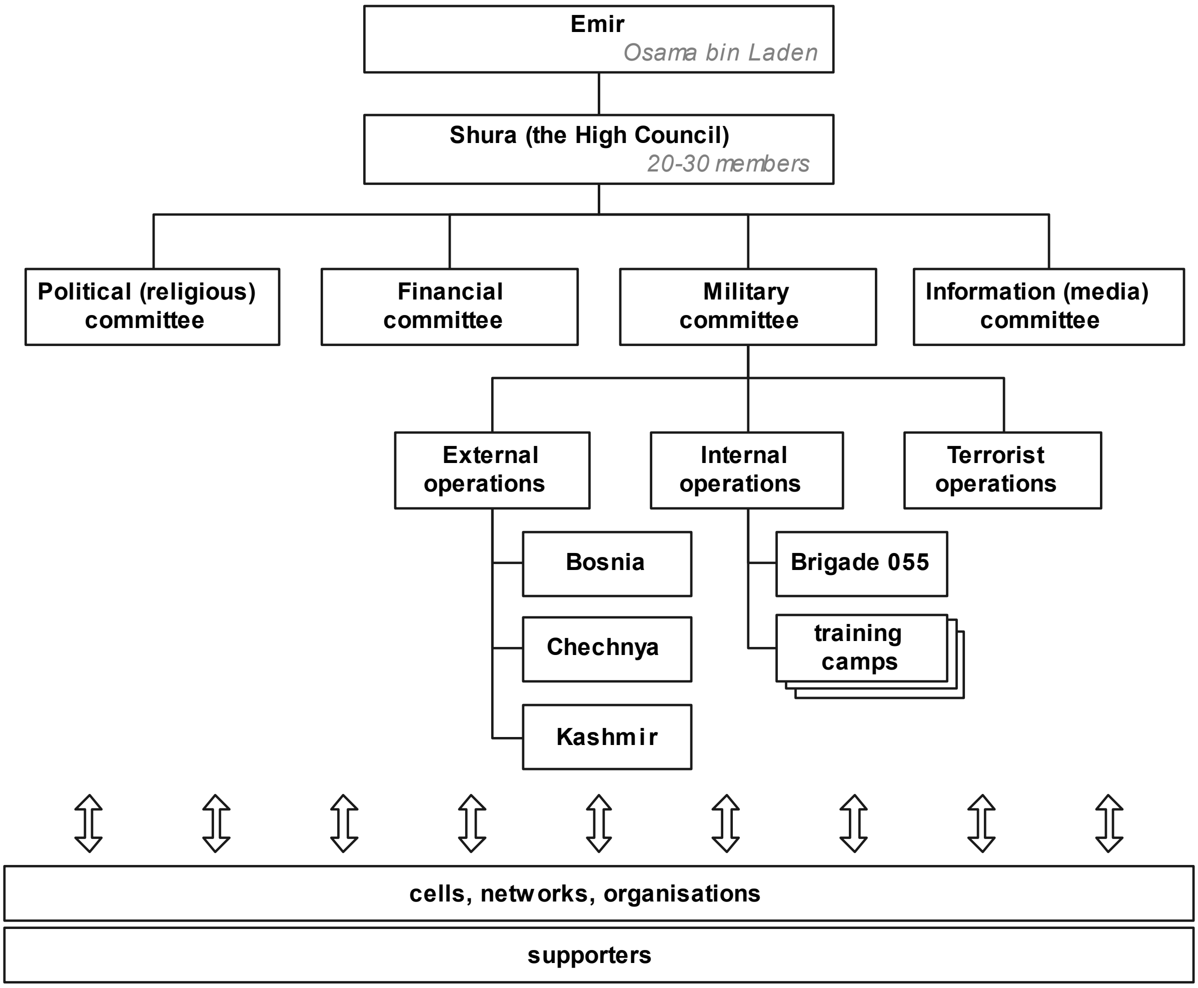

Figure 2. Hierarchical structure of al-Qaeda's core in 2001.

However, presented structural analysis, describing al-Qaeda as a hybrid organisation with its highest levels structured primarily according to functional principles, and with divisional structure at the lower levels, does not contain all the elements needed for understanding its functioning.

First, it must be noted that the formal structure of Figure 2 does not perfectly match all the relations and connections existing within the organisation, which are in reality much more complex. Additional relations including personal ties and multiple roles, which certain individuals attain, often exist aside from the specified lines of control. All of them constitute a network organisation, the lower hierarchical levels of which will be examined more closely in the forthcoming chapters. Moreover, connections between individuals and organisational units are often multiple, so that in reality multiple networks and hierarchies often exist. Thus we may speak about a whole meta-network of networks consisting of the operative network, the financial network, the administrative network, the network of trust, the knowledge network, the information network, and so on. The same node[1] may have different roles in these different networks. The complexity of the meta-network makes the structure of a terrorist network organisation extremely difficult to uncover [8].

Second, it is questionable whether a fundamentalist terrorist organisation can be analysed in the same ways and with the same tools as those used in structural analysis of modern business corporations. Membership in al-Qaeda undoubtedly has important spiritual dimension, and the organisation is at least as similar to a secret religious society as it is to a modern corporation. This opens another view on the structure of the organisation as a series of layers [9], which are often depicted as concentric circles. Members of the organisation believe that each subsequently inner circle is situated closer to a comprehensive revelation of the absolute truth in the centre (Fig. 3). The inner circles draw their indisputable authority in operative and tactical decisions from the assumed divine superiority. Advancement in such organisation is not so much related to the merits or deeds of an individual, as to his or her inner transformation in accordance with the organisation's spiritual teachings. Initiation rituals at certain organisational levels symbolise this spiritual development. The increased willingness to act in accordance with the organisation's goals is an important consequence of the increasingly resolute religious conviction.

The al-Qaeda's leadership does not exercise direct control over all activities of the organisation, not even over most of the activities carried out in the name of the organisation. This is not only because there is no need to control the amount of violence for attaining political goals. Control of violence is also not possible for technical and organisational reasons. What is then the role of leadership in such an organisation?

The leadership provides motivation for actions of the followers – a kind of a common vision or a narrative. It also provides organisational structure, doctrine and methods of operation, and, particularly, the means of personally connecting members of the organisation and the means of communication between them [10; p.324]. Using military terminology, for a network to achieve "self-synchronisation of dispersed forces", needed for its functioning, the leadership must ensure the unity of effort, define commander's intent and determine the rules of engagement [11; p.7].

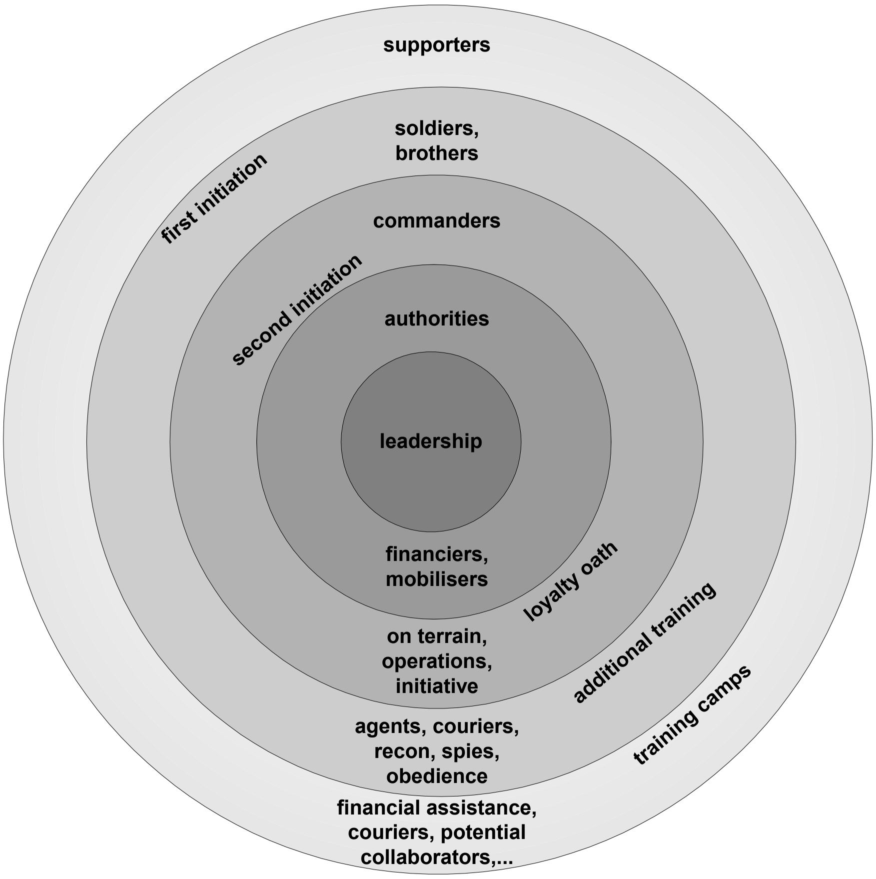

Figure 3. Concentric structure of al-Qaeda as a secret religious society.

It must be admitted that the al-Qaeda's leadership was exceptionally successful in fulfilling its duties. The commander's intent, i.e. the vision to fight for, was provided to membership through *fatwas* – religious decrees requesting death of Americans, their allies, and other infidels. The unity of effort was ensured through common fundamentalist Sunni religion, and reinforced by personal ties and mutual trust developed among the members in training camps in Afghanistan and in religious schools in Pakistan. The rules of engagement, including organisation, doctrine, techniques and methods of operation, were also developed through training, and they were even coded in a kind of training manual [12].

Once developed, "self-synchronised network of dispersed forces" may function without any direct interference or control of the leadership. The role of bin Laden, and probably of al-Zarqawi today in Iraq, becomes similar to the role of a manager of a business incubator [13]. While the manager provides entrepreneurs, or terrorists in this particular case, with start-up conditions, teaches them methods of operation, connects them with one another, monitors their more promising projects, and provides some inspiration and guidance, the initiatives and actions of newly-emerging leaders are autonomous in all other respects.

NETWORK ELEMENTS OF ORGANISATIONAL STRUCTURE

Most expert analyses and media reports on al-Qaeda's structure agree that all of al-Qaeda's organisational levels are structured according to hybrid network-hierarchical principles. Although complete data on the organisation are inaccessible, important studies of certain parts of al-Qaeda's network have been done. Valdis E. Krebs published one of particularly informative articles, reconstructing in considerable detail the portion of the network that prepared and executed September 11, 2001 attacks in the U.S. [14]. Much of the rest of our work is based on Krebs' findings.

Figure 4 depicts the network of airplane kidnappers – perpetrators of the attacks on New York and Washington. Four groups of kidnappers, each of which kidnapped one airplane, are marked with four different symbols for network nodes. Three groups consisted of five members, and one group of only four. One group did not complete its terrorist mission because passengers distracted terrorists enough to miss the planned target, but unfortunately not enough to escape crashing the plane. According to Christopher Allen's analysis [15], based on studying size of functional groups successfully collaborating over the Internet, successful small teams consist of 5-9 members, and the optimal size is 7-8. It is interesting to note that the only terrorist group that did not complete its mission had only four members, which is one below Allen's lower bound of five.

Let us now focus on the number of connections between team members and on the topology of the network. Bold lines in Figure 4 denote "old ties" between terrorists that had existed even before preparation of the attacks began. These ties of trust are typically formed through common schooling or common lodging. We can see that the kidnappers were only weakly connected, as each of them personally knew only three other network members on average. The average length of shortest path[2] between two nodes of the network is as high as 4,75, meaning that members were socially quite distant from one another. Low connectedness certainly favours secrecy, but it may impede network's operability.

During preparation of the attacks, kidnappers connected themselves more closely, increasing thus network's operability. These newly formed ties are denoted in Figure 4 with thin grey lines. It remains unclear, however, why had not all members of the same team known each other prior to boarding the planes. In teams marked with circles and pentagons, for example, each member knew maximally two other members of the same team.

Figure 5 depicts the network of airplane kidnappers, augmented with nodes representing their supporting assistants. According to Krebs' analysis, this wider network had 62 members in total, of which 19 were kidnappers, and 43 assistants: organisers, couriers, financiers, scouts, counterfeiters etc. Allen found that successfully functioning large networks typically comprise 25-80 members, with optimal size between 45 and 50. Again, a close match exists between the results of Allen's analysis of collaborating networked groups and this particular example of a terrorist group.

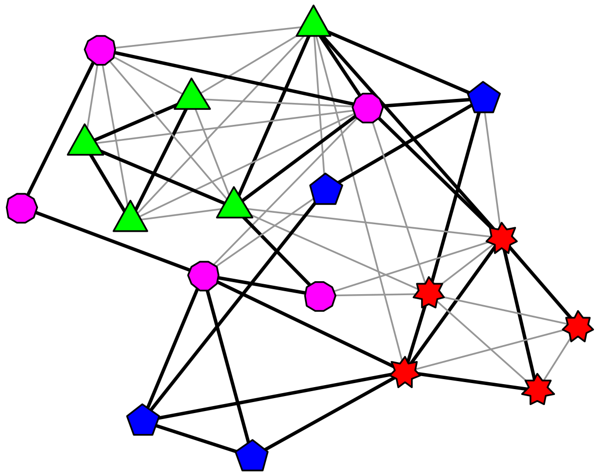

Figure 4. The network of airplane kidnappers participating in September 11, 2001 attacks in the U.S.

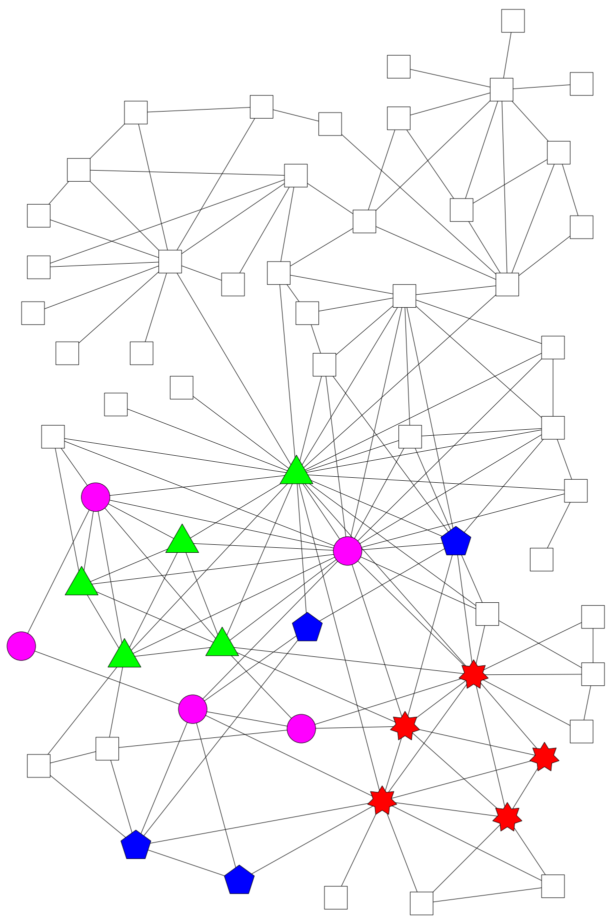

Figure 5. The network of airplane kidnappers and their supporters preparing September 11, 2001 attacks in the U.S.

Inspection of this network by standard measures of network structure [16 – 18] reveals firstly its low connectedness. A member of this network holds only 4,9 connections with other members on average[3], which means that average members are rather isolated from the rest of the network. (Try to imagine a group of 62 people of which you know only five – you would probably hardly feel a sense of belonging to such a group, or hardly expect any coordinated action of such a group.) Connectedness measure[4] of this network is only 0,08, meaning that only 8 % of all possible connections in the network really exist.

In spite of the low connectedness, however, nodes of this network are relatively close. The average length of shortest path between two nodes is 2,9, and the average closeness[5] of nodes is 0,35. Betweenness[6] is another important measure in social network analysis and it indicates a node's importance for communication among other nodes. The average betweenness of this network is 0,032, indicating relatively high average redundancy. However, betweenness of forty nodes is in fact less than 1 %, and only six nodes have betweenness higher than 10 %. These six nodes are obviously critical for information flow, especially the one with betweenness of almost 60 %, meaning that almost 60 % of communication paths among other nodes pass through this central node. This node represents Mohamed Atta, the leading organiser of the attack whose central position in the network is confirmed by other centrality indicators as well.

The values of centralisation measures[7] equal 23 % for degrees, 48 % for closeness, and even 56 % for betweenness of nodes. These results imply that links are relatively evenly distributed among nodes, but that some nodes' placements in network's topology are more significant than others'. Such nodes are in favourable positions regarding information diffusion and distribution of power, and are often referred to as central.

Distribution of degrees of nodes is particularly interesting. Degrees of nodes are exponentially distributed: the degree of most nodes is small, while only few nodes have high degree (Fig. 6). This property characterises the so-called scale-free networks [19, 20; pp.104-111][8], commonly found in diverse areas of science, technology, and society. The same property possess, for example, many traffic networks, networks of social contacts and social influence, networks of Internet servers, and many others, including also brain's neural network. Scale-free networks form spontaneously, without needing a particular plan or interventions of a central authority. Nodes that are members of the network for a longer time, that are better connected with other nodes, and that are more significant for network's functioning, are also more visible to new members, so that the new members spontaneously connect more readily to such nodes than to other, relatively marginal ones.

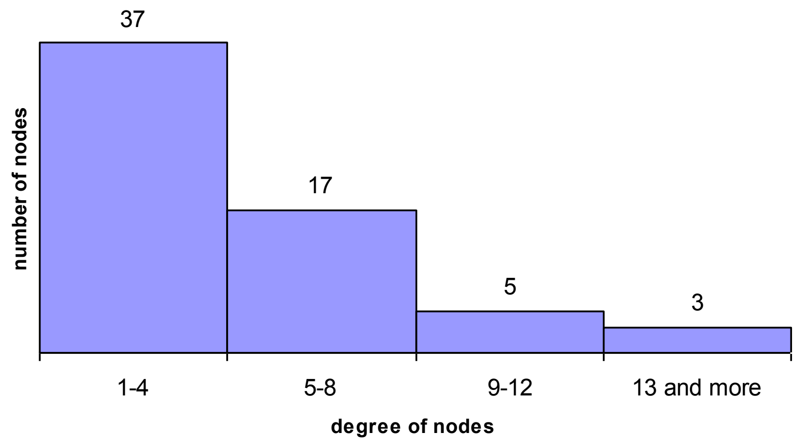

Figure 6. Distribution of degrees of nodes in the network of kidnappers and their supporters.

The al-Qaeda network was also organically formed, under influences of external conditions, operative needs and initiatives of group members. Most likely, the only important network's property resulting from intentional design is low connectedness, which is dictated by the need for secrecy and security of operation. Al-Qaeda's Training Manual states: "Cell or cluster methods should be adopted by the Organization. It should be composed of many cells whose members do not know one another, so that if a cell member is caught, the other cells would not be affected, and work would proceed normally." [12; Third Lesson].

Several other properties of scale-free networks have significant influence on network's functioning, so that the network may often appear as possessing almost supernatural properties. This may explain quotations describing al-Qaeda in the introductory chapter, whose authors were probably under impressions of a similar kind. The next two chapters will describe two of the potentially perplexing properties: speed of information diffusion through the network, and the network's resilience to loss of nodes.

INFORMATION DIFFUSION THROUGH THE NETWORK

When designing transport networks and telecommunication systems, including Internet networks, one of the most critical requirements is on the network's capacity of transferring certain amounts of commodities or information over certain distances in certain time. Methods of graph theory are often used for estimating network's capacity, including identification of directions, capacities, and perhaps transfer costs for each of the links.

Unfortunately, in the case of al-Qaeda network such methods are not particularly helpful because of their exceedingly demanding data requirements. Therefore we shall attempt to illustrate al-Qaeda network's information diffusion capabilities by means of an illustrative example. The example will use three networks of different structural types, but otherwise similar general properties. All three networks consist of 62 nodes. Attempts were also made at keeping the average degree of nodes close to 5 for all three networks. Schematic representations of the three networks are given in Figure 7.

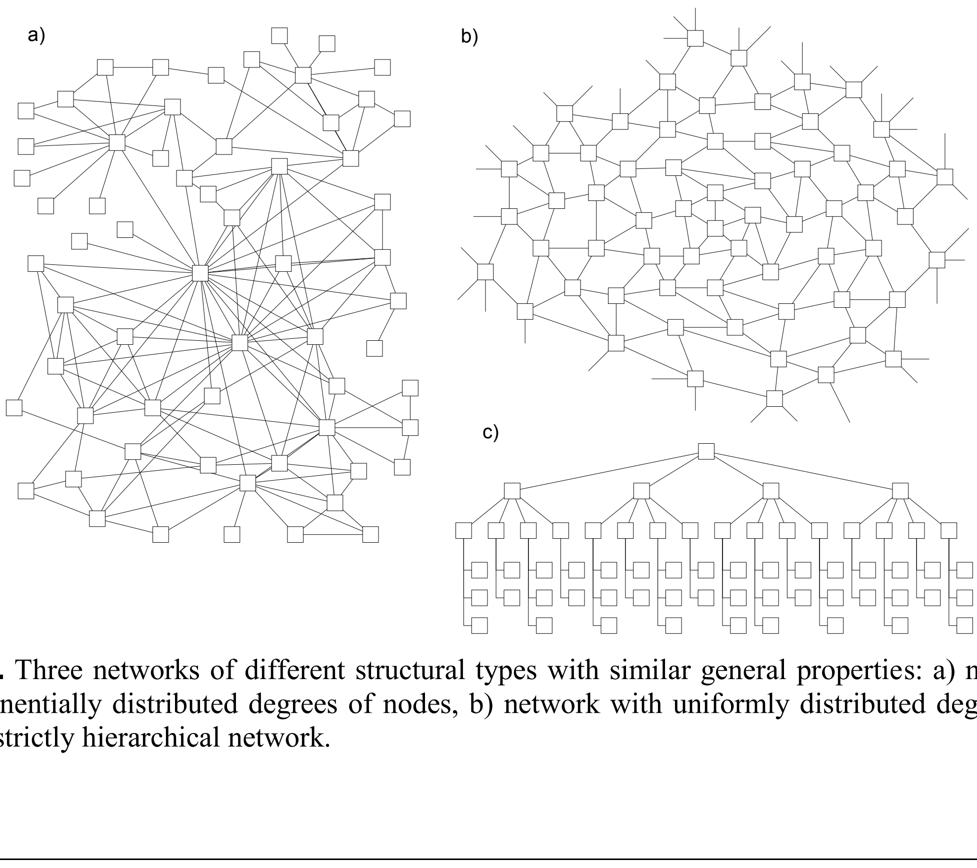

Figure 7. Three networks of different structural types with similar general properties: a) network with exponentially distributed degrees of nodes, b) network with uniformly distributed degrees of nodes, c) strictly hierarchical network.

First of the three networks (Fig. 7a) is Krebs' reconstruction of the network of airplane kidnappers and their supporters that we have already encountered in Figure 5. As we have also already noticed, this network's distribution of degrees of nodes is exponential. Degrees of nodes belonging to the second of the three networks (Fig. 7b) are uniformly distributed and each node is connected to exactly five other nodes. We can easily imagine this network as spreading over a sphere so that the outward-stretching links at borders of Figure 7b in fact connect nodes at the opposite borders. Such network does not possess any central or marginal nodes. As one can hardly find an example of organisation that would be structured in this way, this case is of primarily theoretical significance. Finally, the third network (Fig. 7c) represents standard hierarchical organisation with the structure of a tree. Note that the number of nodes in such network is always one more than the number of links, so that it is not possible to form the hierarchical network in which average degree of nodes would be five. As closest approximation we chose hierarchical tree consisting of 62 nodes, with degrees of all nodes at the second highest hierarchical level equalling five. This requirement automatically generates the rest of this network's structure.

In the first experiment, we were interested in speed at which information originating from the central node diffuses through the rest of each of the three networks. In the case of exponential network central node is located close to the middle of a graph. As we have already noted, this node possesses highest values of all three centrality indicators: degree, closeness, and betweenness. In the case of uniform network no node is distinguished by its centrality, so that the choice of the central information source is completely arbitrary. We have simply chosen the node in the middle of the graphical representation (Fig. 8b). Finally, in the case of hierarchical network central node is the one at the top of the hierarchy. It does not possess highest degree of all the nodes in the network, but is outstanding by its closeness and betweenness values.

We assume that, in each of the networks, information is released by the central node and that it diffuses through the rest of network in discrete steps. In the first step central node dispatches information to all of its neighbouring nodes, and in each next step each of the nodes that received information in the previous step dispatches it further to all of its neighbours. It is assumed that the time to traverse each of the links equals exactly one step, that there are no information losses, and that all links are of sufficient capacity to diffuse information further without any distortion. Time dynamics of information diffusion is schematically represented in Figure 8. Identically shaded areas comprise all the nodes that received information in the same time-step. Darker shading corresponds to areas that received information earlier. For each network, Table 1 contains percentages of nodes that received information in specified time-steps.

As can be seen in Figure 8 and Table 1, information diffusion from centre to periphery was slowest in the uniform network. The hierarchical and the exponential network both transferred information much faster, in only three time-steps. However, the transfer process was much more efficient in the exponential than in the hierarchical network. After only one step, information reached almost 40 % of nodes in the exponential, and only 8 % of nodes in the hierarchical network. After two steps, information reached over 90 % of nodes in the exponential network, and only about one third of the total number of nodes in the hierarchical network.

In the second experiment we investigated the speed of information diffusion in the opposite direction: from periphery to centre, i.e. the source of information is now a peripheral node. In the exponential network our choice for the starting peripheral node was one of the nodes located furthest from the central one, and with the value of betweenness equalling zero (Fig. 9a). In the uniform network the choice of both centre and periphery is completely arbitrary, so we simply repeated the same experiment as in the previous case. In the hierarchical network

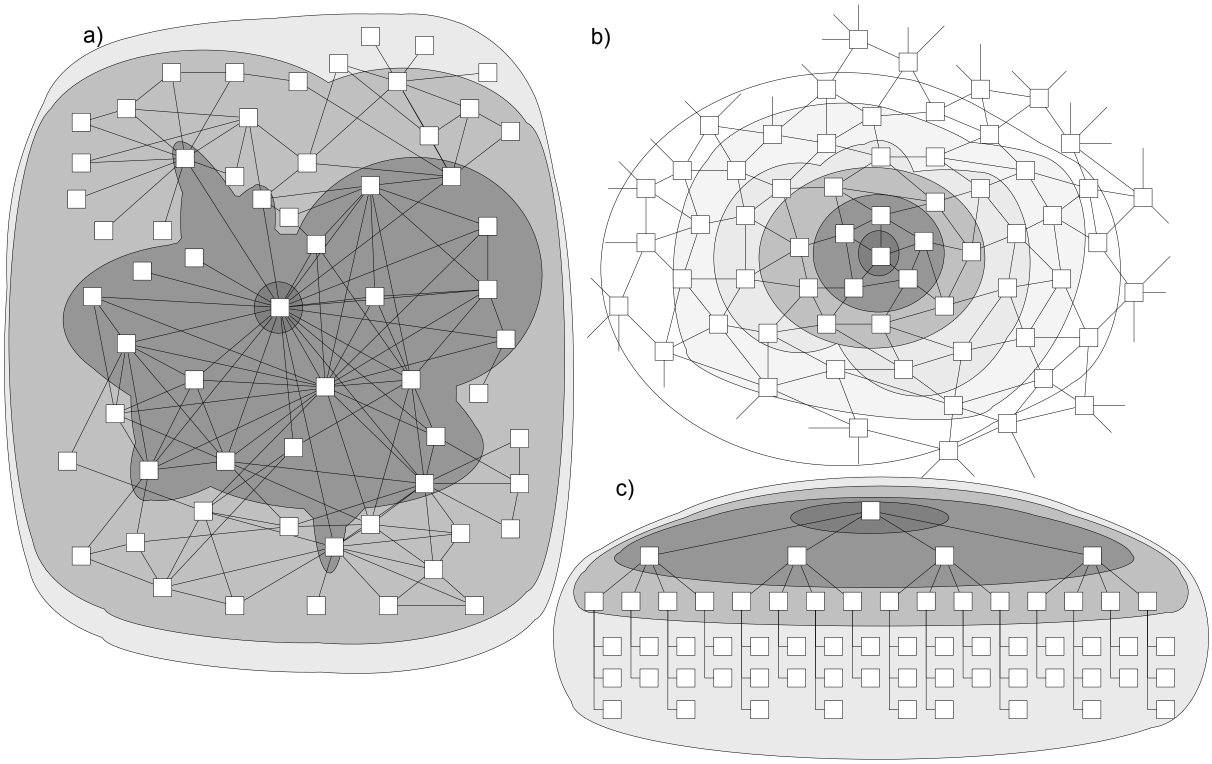

Figure 8. Information diffusion from centre to periphery: identically shaded areas comprise all the nodes receiving information in the same time-step.

Table 1. Percentage of nodes that received information for each time-step and each network – the case of information diffusion from centre to periphery.

Network	Step 0	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Exp.	2 %	39 %	94 %	100 %			
Unif.	2 %	10 %	23 %	39 %	61 %	86 %	100 %
Hier.	2 %	8 %	34 %	100 %			

one of the nodes from the bottom of hierarchy was chosen as the starting peripheral node. Time dynamics for the case of information diffusion from periphery to centre is schematically represented in Figure 9. Darker shading again corresponds to areas that received information earlier. Table 2 summarizes percentages of nodes that received information in each of the time-steps.

Information diffusion was in this case slower in both the exponential and the hierarchical network. Diffusion through the exponential network completed fastest. What may surprise us is that the uniform network was in this case more efficient than the hierarchical network: in each intermediary time-step larger percentage of nodes received information in the former than in the latter network. This finding is in accordance with numerous empirical observations of serious inefficiencies in processing data and initiatives issuing from bottoms of hierarchies towards their upper levels. Most importantly, this particular case of an alarm notice, coming from a peripheral node and disseminating towards upper hierarchical levels, is typical in data gathering for intelligence purposes. It is therefore not surprising that restructuring of the existing hierarchical organisational structures became one of hot topics in the U.S. intelligence community after September 11, 2001 attacks.

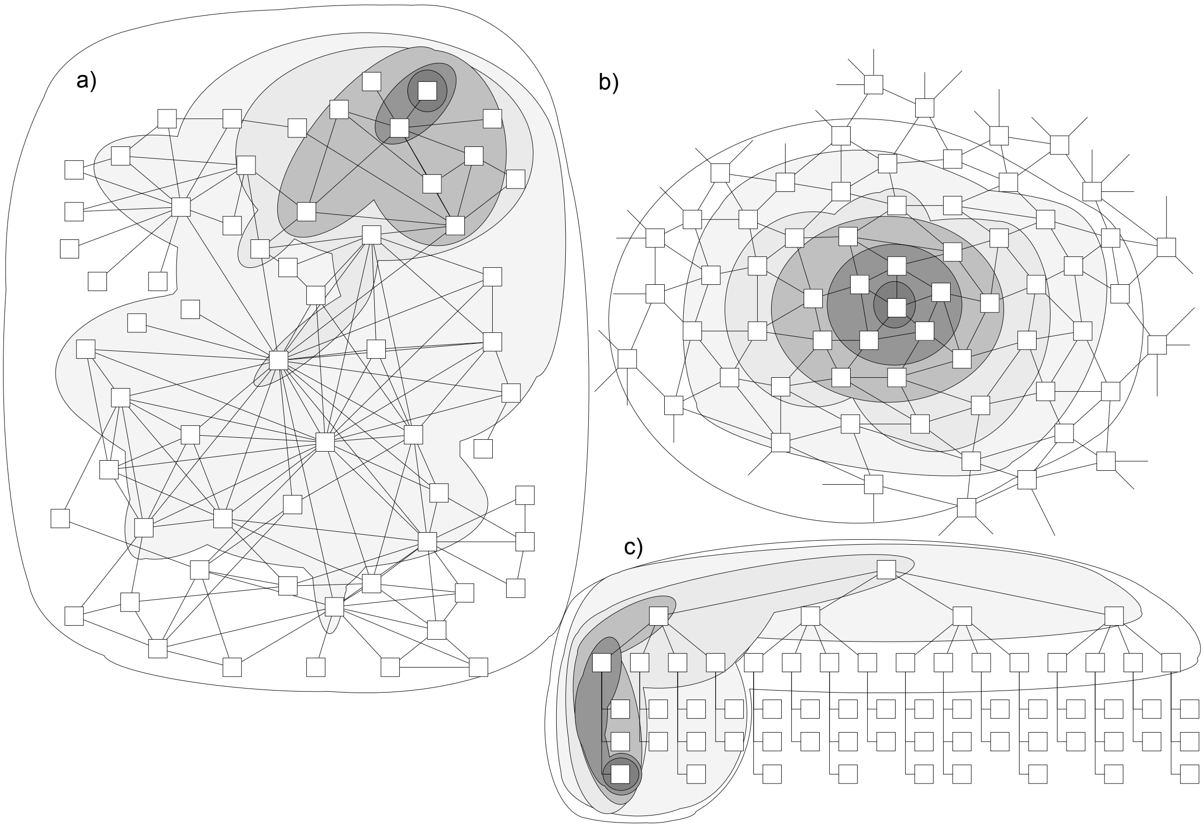

Figure 9. Information diffusion from periphery to centre: identically shaded areas comprise all the nodes receiving information in the same time-step.

Table 2. Percentage of nodes that received information for each time-step and each network – the case of information diffusion from periphery to centre.

Network	Step 0	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Exp.	2 %	3 %	13 %	21 %	56 %	100 %	
Unif.	2 %	10 %	23 %	39 %	61 %	86 %	100 %
Hier.	2 %	3 %	8 %	15 %	34 %	53 %	100 %

The ease of information diffusion through networks with exponentially distributed degrees of nodes is often referred to as a "small-world property" [20, Ch. 3], meaning that it does not take many steps to get from one node to another. Together with secrecy of operation, this property significantly improves operational tempo of terrorist network's activities. In other words, terrorist operations can today be quickly prepared with very moderate requirements for personnel and assets, and without giving many clues at what is going on to external observers. In the right moment network may activate instantly, so that an observer is really left with the impression of terrorists "gathering from nowhere and disappearing after action". The metaphor of terrorists gathering as a swarm, and then quickly dispersing after action is also in place [21]. Another intriguing and analytically useful image is that of a critical mass of passive supporters to terrorists all over the world, who can rapidly self-organise and, through the process of "filtering", enable execution of deadly terrorist attacks anywhere in the world [22].

NETWORK'S RESILIENCE TO ATTACKS AND LOSS OF NODES

Resilience of a terrorist network in cases of arrestment, death, or any other loss of their members is of utmost importance for the network's survival. Conversely, network's vulnerability in such cases is critically important for successfully destabilising the network. There are at least three indicators of network's destabilisation [23]: first, the information flow through the network is seriously reduced, possibly to zero; second, the network, as a decision body, can no longer reach consensus; and third, network, as an organisation, loses the ability to effectively perform its tasks.

Removal of a central node in a hierarchical network has drastic consequences for the information flow, decision making, and task execution. Therefore very detailed rules regulating inheritance of commanding duties exist in, e.g., military organisations for protection against the loss of a commander.

Investigations of networks with exponentially distributed degrees of nodes show, however, extraordinary resilience of such networks to loss of nodes. This is the consequence of their redundant design, which is particularly important, thoroughly investigated, and intentionally applied in traffic, telecommunication and other technical networks. Robustness of terrorist networks is further enhanced by their multi-layered structure. As we have already noted, multiple connections exist among the members so that the whole network may be viewed as one huge meta-network of various functional sub-networks. Obviously, removal of one node does not affect each of the sub-networks uniformly, so that many sub-networks will often not experience serious disturbances.

Finally, network's flexibility is an element contributing perhaps most to its robustness. As there are no strict hierarchical rules, individuals easily change their roles depending on external circumstances. Therefore, when a node is lost, surrounding nodes quickly establish new connections and share responsibilities of the lost member. The network changes its structure and adapts to new circumstances without prolonged loss of functionality. The process of recovery is completely different than in hierarchical organisations, where the organisational structure does not change when a node is lost, but another member occupies the empty position and takes over all the responsibilities of the predecessor.

Robustness analysis of scale-free networks was first motivated by safety requirements for technical networks, but its results are equally relevant for social networks of the same type [24]. These results show that scale-free networks are exceptionally resilient to the loss of a random node. This is not surprising if we remember that most of the nodes in a scale-free network possess only few connections. Loss of such nodes does obviously not have significant impact on network's functioning. More surprising, however, is the fact that scale-free networks may suffer, without being destroyed, random losses as serious as 80 % of their total number of nodes. Another surprising finding is that scale-free networks are often not destroyed even when their central node is removed. As already noted, redundancy and flexibility enable network's quick restructuring without losses of functionality. To destroy a scale-free network, one must simultaneously remove 5-15 % of its nodes, primarily those in central positions[9]. Only such simultaneous attack can destroy redundancies in network connections in the amount needed to prevent any possibility of network's recovery.

Let us check this last property for the network of airplane kidnappers and their supporters from Figure 5. Successive removal of central nodes from this network is schematically represented in Figure 10.

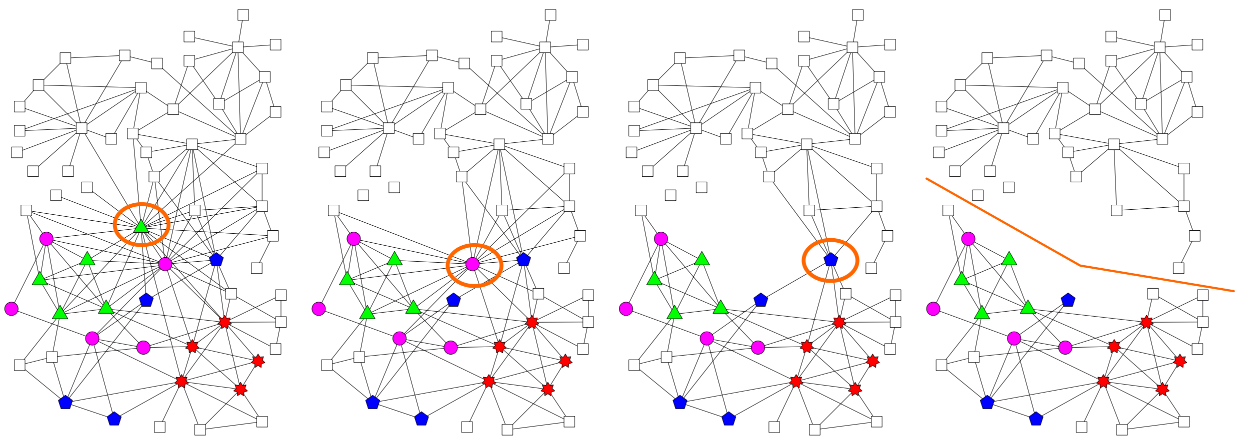

Figure 10. Network's destruction by successive removals of its central nodes: after three removals network disintegrates into two mutually disconnected parts.

As can be seen, three central nodes need to be removed in order to break up this network. This must be done almost simultaneously to prevent network's recovery. Three nodes make up 5 % of the total number of nodes in this network, which is in accordance with the theoretical results cited above. Taking into account that, for secrecy reasons, the number of connections in a terrorist network is kept near minimum, it is not surprising that this network is slightly more sensitive to removal of nodes than technical networks, i.e. that it already breaks down at the lower theoretical bound for percentage of nodes that need to be removed.

CONCLUSIONS

This article shows that terrorist organisations like al-Qaeda present no especially ingenious case of organisational design, but that there exist spontaneously emerging and nevertheless perfectly sensible regularities between the structure of such organisations and their manifest properties. We still need to learn how to detect these regularities and how to understand them better. These regularities are not typical of only terrorist organisations. Networked organisations are present in almost all areas of life and their influence on our social and economic life is important and probably still increasing. Sales networks, open source code community, anti-globalisation movement, and scientific research networks are only some of the examples that have recently attracted much attention in public and in scientific communities.

As we have argued here, in some circumstances these networked organisations have significant advantages over classical hierarchies. Understanding and knowledge gathered in studying network structures in one area can often be more or less directly applied to organising complex systems in some other area. For example, problems of organising a number of autonomous or semi-autonomous software agents to perform business transactions on Internet or some other computer network are in certain aspects similar to problems of organising networks such as al-Qaeda. As another example, in the "net-war" of the future, networked organisation would consist of platforms equipped with various sensors or arms, operating on a battlefield with considerable autonomy, and exchanging information with each other. The real strength of such systems would lay not so much in their number or firepower, as in flexibility and coordination emerging from their networked organisation.

Understandably, very often and especially in situations where strict control over all parts of organisation is necessary, where efficient use of resources is paramount, or where strict responsibility and traceability are critical, hierarchies will still find their application domain.

REMARKS

[1]Using the terminology of graph theory, which is fundamental for the network analysis, a network will be sometimes called a graph, members of the network will be referred to as nodes of the graph, while the connections between members will be referred to as links of the graph.

[2]A path is an alternating sequence of nodes and links, starting and ending with a node. The length of a path is defined as the number of links in it.

[3]This means that average degree of nodes is 4,9, where degree of a node represents the number of links coming out of the node.

[4]Connectedness of a given network is the ratio of actually existing number of links in this network and the maximal number of links that would be possible in a network with the same number of nodes, where each node would be linked to each other.

[5]Closeness of a node is an inverse of the average length of shortest paths from the given node to all other nodes of the network.

[6]Betweenness of a node is the number of shortest paths that go through that node, divided by the number of shortest paths in total.

[7]Degree, closeness, and betweenness of a node are varieties of centrality indicators. Each centrality indicator has its corresponding centralisation measure. The centralisation measure measures unevenness in distribution of centrality indicator's values over all network's nodes. Higher centralisation means higher unevenness.

[8]The term "scale-free network" originates from the fact that for such networks the ratio of number of nodes with degree k and the number of nodes with degree αk does not depend on the scaling factor k for any fixed $\alpha > 0$. This property is also related to the property of self-similarity, which indicates fractal structure of a network.

[9]The exact percentage is dependent on the amount of redundancy and, to some extent, on the choice of nodes to be removed.

REFERENCES

[1] *Transcript of Home Secretary Charles Clarke's Interview with Channel 4 News, July 8, 2005.* http://www.channel4.com/news/special-reports/special-reports-storypage.jsp?id=328,

[2] *July 16, 2005 IRA statement in full.* http://news.bbc.co.uk/1/hi/northern_ireland/2132113.stm,

[3] Bremer, P.L.: *New Terrorist Threats and How to Counter Them*. The Heritage Foundation, Washington DC, 2000, http://www.heritage.org/Research/HomelandDefense/hl678.cfm,

[4] Boyne, S.: *Uncovering the Irish Republican Army*. Jane's Intelligence Review, August 1, 1996, http://www.pbs.org/wgbh/pages/frontline/shows/ira/inside/org.html,

[5] Boettcher, M.: *Charting Al'Qaeda's Structure*. CNN video presentation, 2001, http://www.cnn.com/video/world/2001/09/21/mb.al.qaeda.org.cnn.med.html,

[6] Hoffman, B.: *Al'Qaeda's Organization*. Microsoft Encarta Online Encyclopedia, 2005, http://encarta.msn.com/text_701610346__3/Al-Qaeda.html,

[7] National Commission on Terrorist Attacks upon the United States: *Overview of the Enemy*. Staff Statement No. 15, June 16, 2004, http://www.globalsecurity.org/security/library/congress/9-11_commission/040616-staff_statement_15.pdf,

[8] Dombroski, M.J.; Carley, K.M.: *NETEST: Estimating a Terrorist Network's Structure*. CASOS 2002 Conference, June 21-23, 2002. Carnegie Mellon University, Pittsburgh, http://www.casos.cs.cmu.edu/events/conferences/student_papers/Dombroski.pdf,

[9] Robb, J.: *Al Qaeda's Structure*.
Post on the Global Guerrillas forum, posted on August 12, 2004,
http://globalguerrillas.typepad.com/globalguerrillas/2004/08/al_qaedas_struc.html,

[10] Arquilla, J.; Ronfeldt, D.: *Networks and Netwars: The Future of Terror, Crime and Militancy*.
RAND publication MR-1382-OSD, RAND, Santa Monica, 2001,
http://www.rand.org/publications/MR/MR1382/MR1382.ch10.pdf,

[11] Sanders, C.D.: *Al Qaeda: An Example of Network-Centric Operations*.
Naval War College, Newport, 2002,
http://handle.dtic.mil/100.2/ADA401158,

[12] *Al Qaeda Training Manual*.
US Department of Justice,
http://www.usdoj.gov/ag/trainingmanual.htm and
http://www.pbs.org/wgbh/pages/frontline/shows/network/alqaeda/manual.html,

[13] Robb, J.: *Mapping Terrorist Networks*.
Post on the Global Guerrillas forum, posted on April 23, 2004,
http://globalguerrillas.typepad.com/globalguerrillas/2004/04/mapping_terrori.html,

[14] Krebs, V.E.: *Uncloaking Terrorist Networks*.
First Monday – Peer Reviewed Journal on the Internet **7**(4), 2002,
http://www.firstmonday.org/issues/issue7_4/krebs/,

[15] Allen, C.: *The Dunbar Number as a Limit to Group Sizes*.
Post on the Life with Alacrity forum, posted on March 10, 2004,
http://www.lifewithalacrity.com/2004/03/the_dunbar_numb.html,

[16] Krebs, V.E.: *An Introduction to Social Network Analysis*.
2005, http://www.orgnet.com/sna.html,

[17] Wolfe, A.W.: *Applications of Network Models – Glossary to Accompany the Course and the Manuscript*.
2001, http://luna.cas.usf.edu/~wolfe/glossary.html,

[18] Borgatti, S.P.: *Intra-Organizational Networks*.
Handouts for the course Introduction to Organizational Behavior, 1996, revised 2002,
http://www.analytictech.com/mb021/intranet.htm,

[19] Li, L.; Anderson, D.; Tanaka R.; Doyle J.C.; Willinger, W.: *Towards a Theory of Scale-Free Graphs: Definition, Properties, and Implications*.
Technical Report CIT-CDS-04-006, Engineering and Applied Sciences Division, California Institute of Technology, Pasadena, 2004,
http://arxiv.org/PS_cache/cond-mat/pdf/0501/0501169.pdf,

[20] Watts, D.J.: *Six Degrees – The Science of a Connected Age*.
W. W. Norton & Company, New York, London, 2003,

[21] Kreisler, H.: *International Relations in the Information Age: Conversation with John Arquilla, Professor at the Naval Postgraduate School Monterey*.
Institute of International Studies, University of California, Berkeley, 2003,
http://globetrotter.berkeley.edu/people3/Arquilla/arquilla-con0.html,

[22] Galam, S.: *The September 11 Attack: A Percolation of Individual Passive Support*.
2002, http://xxx.lanl.gov/PS_cache/cond-mat/pdf/0204/0204052.pdf,

[23] Carley, K.M.; Lee, J.S.; Krackhardt, D.: *Destabilizing Networks*.
Connections **24**(3), 79-92, 2002,
http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Carley.pdf,

[24] Robb, J.: *Scale-Free Networks*.
Post on the Global Guerrillas forum, posted on May 7, 2004,
http://globalguerrillas.typepad.com/globalguerrillas/2004/05/scalefree_terro.html.

O MODELIRANJU KOMPLEKSNIH MREŽA S PRIMJENOM NA MODELIRANJE TERORISTIČKIH SKUPINA

D. Penzar[1], A. Srbljinović[2]

[1]Soko Z. I.
Zagreb, Hrvatska
[2]Institut za obrambene studije, istraživanja i razvoj Ministarstva obrane Republike Hrvatske
Zagreb, Hrvatska

SAŽETAK

Na temelju dostupnih podataka o različitim organizacijama i mrežama članak istražuje neka ključna svojstva strukture terorističkih organizacija. Težište analize je na nižim razinama organizacijske hijerarhije, gdje je jasno vidljiva mrežna struktura s eksponencijalnom distribucijom broja lukova između čvorova mreža. Takve mreže rastu organički, vrlo su učinkovite u širenju informacija te robusne s obzirom na slučajne gubitke čvorova i na ciljane napade. Navedene osobine mreža ilustrirane su na primjeru terorističke mreže koja je izvela napade na New York i Washington 11. rujna 2001.

KLJUČNE RIJEČI

kompleksne mreže, struktura mreže, svojstva mreže