Comparing terrorist and Internet networks

Fall 2010, markus.sabadello@gmail.com

The network, stronger than the node,
Can circumvent a failing part,
Security and control code
keep alive the network's heart.

But what if every spark goes dark,
abandons network, node and core,
what if they cease to light the night,
because the people send no more?

Contents

1. Introduction

The ubiquitous processes sparked by globalization have – besides having had many other impacts on societies, economies and politics[1] – also led to a new kind of global "superterrorism" that is transnational and often organized in a form that is best described as a "network", which poses new challenges for international relations and counter-terrorism efforts that are concerned with the security of societies worldwide. One example for this is modern Islamist terrorism, which is sometimes referred to as "Post-Al-Qaeda" or "Global Jihad", and classified as superterrorism for its global scope, transnational way of operation and unlimited goal of changing the world order toward the utopian vision of a global Islamic Caliphate, free from nation-states, governments and hierarchies in general. This constitutes a threat emerging from an enemy that is neither a state nor a formal organization, but rather a hard to understand social and/or organizational network.

At the same time, the Internet is the largest computer network ever created. On this network, a multitude of more or less complex applications are available to end users – from E-Mail to filesharing software such as BitTorrent, from the Google search engine to Facebook and Twitter. These applications make use of the basic technical, electronic infrastructure in various ways. They run on top of the relatively static hardware that makes up the Internet, and in doing so they create "logical" network structures which can take a wide variety of forms, from strictly hierarchical client/server architectures to distributed and highly dynamic peer-to-peer systems.

When it comes to analyzing the relation between the emergence of superterrorism such as the Post-Al-Qaeda movement, and the nature and evolution of Internet networks, several fields of study can be distinguished:

[1] Since at least (Castells, 2000), we have a good scientific understand for analyzing the influence of the Internet on social structures.

- Just like “regular” political and social movements such as the Serbian “Otpor!”[2] or the Mexican “Zapatista Army of National Liberation”[3] used the Internet for disseminating their political messages and for attracting new members to their cause, this is also the case with terrorist groups seeking to publish their messages to a wide audience.
- In most definitions, the spread of fear among a civilian population is a prerequisite for acts of violence to be labeled terrorism. Therefore, prior to the invention of technologies such as the telegraph and the radio, there was no terrorism, because there was no way to spread fear at large scale. The coverage and attention made possible by Internet applications toward terrorist attacks has therefore greatly enlarged their targeted audience.
- The use of the Internet as a tool to effectively run an organization is also an important factor. This can range from the dissemination of operational know-how such as bombmaking plans to the coordination of joint resources and activities[4].

Finally, the arrival of the Internet with its semi-anonymity, interactivity and ability to overcome large geographical distances at low costs and high speeds has also acted as a catalyst for transforming the very structures of terrorist movements themselves. According to (Sageman, 2008), until 2004 most of the networks of global Islamist terrorism were based on face-to-face interactions among friends, whereas later these network links were increasingly replaced by communication via Internet applications such as E-Mail and dedicated chat rooms and forums.

However, the main purpose of this paper is not to analyze in great detail how Internet applications are used by terrorist groups in any of the above ways, or how the

[2] Otpor! (“Resistance” in Serbian) was the nonviolent movement against the socialist regime of Slobodan Milošević. According to the movie “Bringing down a Dictator”, before this movement even had an office, they already had a website for spreading their political messages to the public.

[3] In (Castells, 1997), this movement – which had a comprehensive nonviolent communications strategy – was called the “first informational guerrilla movement”.

[4] This potential of the Internet is of course not just available to terrorist groups, but also to nonviolent social movements such as the 2008 Anti-FARC protesters that managed to organize a march of hundreds of thousands of people via the Facebook social networking platform.

globalization process and the Internet have influenced the transition from traditional hierarchical terrorism to transnational superterrorism[5].

Rather, the motivation for writing this paper is to look at the emerging network structures themselves, to argue that the forms of both terrorist networks such as in the case of Post-Al-Qaeda and modern Internet network structures are comparable in various ways, and to try understand their respective similarities and differences, in an attempt to anticipate potential future developments in either of them.

2. Networks

In the social sciences, networks and other structures can be analyzed both from a social perspective for explaining personal relations between individuals, and from an organizational perspective for looking at the logistical infrastructure that make up a more formal organization in the traditional sense. Prior to the relatively new idea of describing social/organizational structures as "networks", many other kinds of models have been developed that are still useful today. Such structures include hierarchies, associations, brotherhoods, markets, clans and many more[6]. Besides for the purpose of analyzing terrorist groups, the network concept has also been applied to other areas of social studies, such as the structures of corporations and international relations, however it must be pointed out that terrorist networks are in many aspects different from other social/organizational networks because of their secretive nature and unique aims.

Because of the broad application of the term, it is difficult to come up with a universal definition of networks that covers all their variations and all fields of study where the concept has been applied. The common elements of networks in both the social/organizational context of terrorist networks and in the Internet context are the concepts of nodes, links and messages. Nodes are participants of the network (e.g. individuals, computers, etc.), links are enduring connections or communications channels between nodes, and messages are pieces of information that are periodically

[5] These topics have been extensively covered by literature, e.g. see chapters 2 ("The Globalization of Jihadi Terror") and 6 ("Terrorism in the Age of the Internet") of (Sageman, 2008) for a good overview as well as for several examples of terrorist groups that have used the Internet for their purposes in various ways.

[6] See (Weber, 1947), (Powell, 1990) and (Tsoukas & Knudsen, 2005).

exchanged between nodes via links. Other important elements in the possible definitions of networks are theirdecentralized nature (i.e. the absence of any central authority for managing the structure), the existence of a common goal or purpose, and an ability for rapid addition or removal of nodes and links.

2.1. Graph Theory

In mathematics, the study of networks is the subject of an extensive academic field known as graph theory. In this field, networks are sometimes referred to as "graphs", nodes as "vertices", and links as "edges" that connect pairs of "vertices". This mathematical field has developed a multitude of terms and tools for describing and analyzing the various forms and properties of graphs. They may be directed, undirected, planar, complete, bipartite, sparse or dense. Special types of graphs and subsets of graphs are known, such as trees, cliques, knots and "Eulerian" or "Hamiltonian" paths or cycles. Formulae exist for describing various properties of graphs, nodes and edges, such as size, degree, density and variability. If the entire graph is known, these properties can be calculated exactly. If it is only partially known, sometimes properties can still be mathematically estimated.

Graph theory also offers algorithms for fulfilling various common tasks in network structures, such as enumerating all nodes, traversing a graph in the most efficient way, searching for nodes with given properties or restructuring networks in accordance with given specifications. In efforts to analyze and describe both social/organizational and Internet networks, the terms and tools of mathematical graph theory are a useful resource.

2.2. Forms and Properties of Networks

Networks do not always look the same. They can come in different forms, sometimes exhibiting more hierarchical, sometimes more distributed features. Using the terminology of graph theory, the three main overall topological properties are 1. a network's average node degree (i.e. the average amount of links from one node to other nodes), 2. the node degree variability (i.e. how much individual nodes can divert from the average node degree) and 3. the average route length (i.e. the amount of intermediary nodes a message must pass through between a sender and a receiver). A high node degree variability introduces some amount of centralization into the network, and nodes of high degree are then sometimes referred to as "hubs", "supernodes" or "ultrapeers". Nodes of low degree are sometimes called "leaves". Hubs do not necessarily have a higher authority or more control over other nodes, but they deserve special attention because of their increased topological importance and their resulting significance for the stability of a network. In a terrorist network, hub nodes may provide key logistical support that is important for many other nodes in the network. In the Internet world, one example of an application that makes use of supernodes is Skype[7]. Extreme, degenerate forms of networks are possible[8], e.g. an "all-channel" network, where every node has links to every other node[9], or a "hub-and-spoke" network, where every node has a link only to a single central node through which all message must pass[10]. Such special forms are often considered to not optimally exploit the potential advantages of networks. Instead, both social/organizational and Internet networks should generally seek to keep the node degree variability low, and to find balanced values for the average node degree and average route length, in order to maximize the strengths and minimize the weaknesses of such networks.

In many cases, a clear distinction between networks and other structures is difficult or even impossible. The combination of elements, strengths and weaknesses of multiple forms can lead to hybrid structures, or to new forms of organization altogether. It is interesting to note that in an attempt to explain the structures of both terrorist and Internet networks, different "layers" can be distinguished, each of which exhibits its own networking characteristics. In the terrorist context, those are the social layer and the organizational layer. In the Internet context, various "layers" also exist that build and rely on each other. On the lowest (hardware) layer, basic electronic exchange of information takes place. Higher layers are responsible for more advanced functionality such as routing and message integrity. The two best-known models for explaining

[7] See (Baset & Schulzrinne, 2006). In Skype, supernodes are chosen based on their technical capabilities, i.e. bandwidth, latency and reliability. Those supernodes take additional responsibility in maintaining the network's functionality, i.e. performing phone calls.

[8] See (Eilstrup-Sangiovanni & Jones, 2008) pp 12-13

[9] An "all-channel" network consisting of n nodes has an average node degree of (n-1), a low node degree variability, and an average route length of 1.

[10] A "hub-and-spoke" network consisting of n nodes has an average node degree of ≈2, a high node degree variability, and an average route length of ≈2.

network layers are the Open Systems Interconnection (OSI) model that distinguishes between seven different layers, and the TCP/IP model used by the Internet that is based on four layers. Just like in social/organizational networks, each layer in these electronic networking models also fulfill specific purposes.

2.3. Terrorist Networks

The Post-Al-Qaeda movement, which has emerged out of the classic, hierarchical Al-Qaeda organization that has committed several high-profile terrorist attacks, is one example for a hybrid structure, where a classic hierarchy can be observed at the top strategic and ideological leadership levels, while a decentralized network structure is used at the lower operational levels. As (Eilstrup-Sangiovanni & Jones, 2008) put it, today this movement operates less like a top-down structure and more like a loose umbrella group, offering inspiration and legitimacy to radical Islamists from varying backgrounds. It has therefore come to both enjoy the strengths and be vulnerable to the weaknesses of networks.

Other groups engaged in violent activities such as the IRA in Northern Ireland or Hamas and the Al-Aqsa Martyrs Brigades in the Palestinian territories are also known to have introduced network structures, especially at their lower, operational levels[11].

2.4. Internet Networks

On the Internet, the kinds of logical networks that build on the low-level electronic infrastructure are diverse. During the last few years, several trends could be observed. One general long-term trend in mainstream applications has been toward hierarchical paradigms, traditionally known as client/server architectures, or more recently described with marketing terms such as “software as a service”. Today, most applications used by the average Internet user are organized this way. Services such as Google Search, Gmail, Facebook and Twitter are all based on a strictly centralized hierarchy involving a powerful server structure at the top of the system and large numbers of clients on the bottom layer that both use services and receive commands from the servers. Such architectures are known for being efficient, reliable and secure as long as all key components of the hierarchy function correctly. Sometimes, while overall

[11] See chapters 4 and 5 of (Stepanova, 2008)

being organized in a hierarchical fashion, systems can be built with some amount of decentralization at the top, for example in the “cloud computing” paradigm that is based on the idea of distributing servers to different locations in a network.

While most mainstream Internet applications follow a hierarchical pattern, there have always been countertrends to move toward a more networked form of communication. Such forms are commonly referred to by the technical terms “decentralized”, “distributed” or “peer-to-peer”. Examples include file-sharing applications such as Napster[12] or BitTorrent[13], collaboration tools such as Google Wave, or – more recently – efforts to build a “Federated Social Web”[14], a “Facebook without a single Facebook”, or in other words, an online social networking system where multiple providers and users can interact with each other and fulfill their social communication needs, without being dependent on any single company or server system. Some of these applications still contain certain hierarchical elements and distinctions between clients and servers and should therefore be considered hybrid structure. Another interesting class of Internet applications that is based on a “pure” network structure and able to operate without any hierarchies is known as Distributed Hash Tables[15], which provide nodes with advanced communication and information storage services.

Attempts to build decentralized Internet applications have recently achieved a lot of attention and hype[16]. This attention can be explained by a mix of technical rationale and irrational allure that is often inherent to technological experimentation.

[12] Napster (http://www.napster.com) – today mostly remembered for having sparked massive illegal sharing and downloading of copyrighted music and other material – is generally considered the first mainstream application that effectively demonstrated the advantages of peer-to-peer network architectures over traditional hierarchical systems.

[13] BitTorrent (http://www.bittorrent.com) is today’s most used peer-to-peer file-sharing technology for transferring large amounts of data, e.g. movies or software packages.

[14] This effort was launched in July 2010. See http://federatedsocialweb.net, also see the following concrete implementations of this effort: http://status.net, http://cliqset.com, http://projectdanube.org.

[15] Example implementations include Chord (http://pdos.csail.mit.edu/chord) and FreePastry (http://www.freepastry.org).

[16] For example, the Diaspora project (http://joindiaspora.com) consisting of four young students has raised USD 200,000 via a “crowdfunding” platform, and has attracted significant media attention.

2.5. Node Identity

When looking at terrorist networks and Internet networks, perhaps one of the biggest differences lies in the way nodes are identified within a network. This is also the area where the two kinds of networks can potentially learn and benefit from each other the most. In technical terms, in order to form a network and establish links between nodes, at least a minimal concept of identity is required for the purpose of referring to nodes and for distinguishing one from another.

In Internet networks, a naming and addressing schema for the network's nodes is essential before any communication can take place. In "Zooko's Triangle"[17], Zooko Wilcox-O'Hearn describes three desirable properties of such a naming and addressing schema: *Decentralized* (i.e. the independence of the schema from a central authority), *Human-meaningful* (i.e. the memorability of a node's identity) and *Secure* (i.e. the guarantee that a node's identity is unique and cannot be claimed by another node). Wilcox-O'Hearn argues that any possible naming and addressing schema in a network can only ever fulfill two of these three properties. In social and organizational networks between human beings (including terrorist networks such as the Post-Al-Qaeda movement), the predominant schema of providing identity is the use of either real names or pseudonyms (noms de guerre). The identity of a node can also be as simple as a known face, or as complex as a full postal address. Most identity schemas used in social and organizational human networks fulfill the *Decentralized* and *Human-meaningful* properties of Zooko's Triangle, but not the *Secure* property. This last property *Secure* however is considered the most important one in Internet networks. Not only does it make sure that nodes cannot impersonate each other, it also (usually) makes it possible to look up and contact any node in the network from any other node, provided there is at least one existent path to the target node.

Internet network structures typically fulfill either the *Secure* and *Human-meaningful* properties (e.g. all DNS[18]-based applications such as the World Wide Web and the Internet's E-Mail system), or the *Secure* and *Decentralized* properties (e.g. applications

[17] Wilcox-O'Hearn, Zooko, Names: Decentralized, Secure, Human-Meaningful: Choose Two.

[18] The Internet's Domain Name System (DNS) provides a centralized naming system for nodes and resources on the Internet.

based on a Public Key Infrastructure and digital signatures, or highly distributed applications such as Distributed Hash Tables). Technologies that have been specifically designed to establish identity within networks include URIs[19], XRIs[20], UUIDs[21], public keys and others.

2.6. Node Membership

From a mathematical perspective, a node is usually defined to be a member of a network if it has at least one link to another node. Sometimes a node could also be a member without having any such link; In this case, its membership is defined either by the node's own mere existence, or by some property or function of the node.

In terrorist and other social/organizational networks, the process of being considered a member can come in many variations. In the original Al-Qaeda organization, it was common for new members to explicitly state their membership by swearing "bayah" – an individual oath of loyalty – to Osama bin Laden or one of his lieutenants[22], therefore being admitted to the organization and assuming a fixed position in its hierarchy. However, many individuals could also be considered part of the group by mere virtue of their ideology or operational function. In other words, formal initiation procedures can sometimes be identified to "mark" an individual as a member of a structure. In the more modern Post-Al-Qaeda social movement, membership is much more loosely

defined and can be as simple as subscribing oneself to a common ideology, or to start perform terrorist attacks consistent with the movement's goals. Often, approximation to a network starts on the social level, i.e. by developing strong interpersonal relationships, before also extending these links to the organizational level.

In the Internet context, membership in a network requires active cooperation with other nodes on the technical level. For any given node at any given time, membership in one or more networks is either existent or non-existent according to strict technical criteria – there is never a gray area. In order to participate, nodes must run specific software and have the ability to establish links (connections) with other nodes. Just like in the case of

[19] See (Berners-Lee, 1998)

[20] See (Reed & McAlpin, 2005)

[21] See (Leach, 2005)

[22] See p. 28 of (Sageman, 2008)

terrorist networks, the exact form of Internet networks and the messaging patterns can vary greatly. For example, in the global E-Mail system, anyone with suitable E-Mail software can participate. In this case, messages are sent only sporadically, i.e. when an E-Mail is actually being delivered. In the case of other applications such as Distributed Hash Tables, relatively permanent links between nodes can be observed, and messages are exchanged frequently.

In both terrorist and Internet networks, a distinction can be made between latent and manifest membership. The former refers to a state of general inactivity with no or only inactive links to a network, while the latter implies active participation with one or more established links to other nodes and with some amount of messages being sent and received over those links.

3. Network abilities

3.1. Communication

The ability to exchange messages is an essential feature of any network, whether social/organizational or electronic. This ability naturally depends directly on the notion of node identity (see 2.5) within the network. It is important to note that the more advanced the notion of identity is, the better communication patterns (routing) and other functionality can be provided by the network. Sometimes, highly specialized knowledge about specific, local network features can help to make communication more efficient[23].

Decentralized Internet applications such as Distributed Hash Tables offer several ways of communication inside a network:

- **Direct Neighbors:** In this case, a node simply sends a message to one or more of the nodes it has direct links to. This is the most trivial form of communication, because it does not require advanced knowledge of the network's topology or any notion of distributed node identity beyond what is needed to identify a

[23] In Internet networks, the approach of having locally specialized knowledge about a network's topology is sometimes known as "hints".

node’s own neighbors. This is the most common, and sometimes the only possible form of communication in social/organizational networks.

- **Unicast:** Messages can also be sent to a node at any arbitrary location within the network, provided that the node’s identity within the network is known. The routing process from the sender to the receiver works reliably over any number of intermediary nodes. Unicast is by far the most common form of communication in most Internet applications. Messages typically also include the sender’s identity in order to enable replies by the recipient.
- **Multicast:** This is a one-to-many method where messages can be delivered to multiple receiver nodes, potentially even without knowing their identities within the network. Just like in the case of Unicast, no assumption is being made about the topological proximity between the sender and the receiver(s). This method is often used in publish/subscribe scenarios, where one node (the publisher) frequently generates information that is of interest to multiple other nodes (the subscribers).
- **Random Unicast/Multicast:** These are small variations of the previous two cases, meaning that messages can also be sent to one or more random nodes within the network, without knowing their identities in advance. The practical usefulness of this case may seem limited at first, however, random communication patterns within networks have the advantage of being hard to trace by outside observers. Also, in a process known as load balancing (i.e. the equal distribution of tasks), random messaging patterns are an effective strategy.
- **Anycast:** In this case, a message is sent to one or more nodes fulfilling certain properties or being able to perform certain services. This can be used in situations when a sender has to deliver a message that only makes sense for certain receiver, whose identities need not necessarily be known to the sender. In such situations, Anycast algorithms will make sure that the message efficiently finds its way to a suitable receiver.
- **Broadcast:** Like Multicast, this is also a one-to-many method which however delivers messages to entire network. This can be used for announcement or coordination purposes. Using Broadcast algorithms, a message will efficiently find its way to all nodes in a network, without reaching any node more than once.

3.2. Distributed Storage

Some Internet networks such as Distributed Hash Tables not only allow various ways of communication between nodes, but also make it possible to store information within the network. In doing so, pieces of information cannot anymore be logically attributed to individual nodes. Information is replicated within the network, i.e. exists at several nodes at ones, and information may even dynamically be moved from one place to the other in the case of network restructuring. Despite this seemingly complex process of distributing storage in the network, the algorithms for storing and retrieving requireds piece of information are reliable and efficient.

3.3. Public Key Infrastructures

A Public Key Infrastructure (PKI) is another feature commonly observed in Internet networks. This is a cryptographic technology that associates a pair of digital keys with each node's identity in a network. One of the keys is private and only known to the node it belongs to, while the other key is public and can be looked up by any other node on the network. The two main abilities provided by this technology are authentication, i.e. a recipient of a message can reliably verify the sender's identity, and confidentiality, i.e. a message can be transmitted in an encrypted way without being exposed to intermediary nodes during the routing process.

3.4. Reputation Systems

Reputation systems within Internet networks are approaches where nodes observe and evaluate each other's trustworthiness by assigning numerical values (ratings) to various aspects of their behaviors[24]. In doing so, it becomes easier to identify malicious nodes and potentially exclude them from the network.

4. Network Strengths and Weaknesses

When it comes to analyzing the strengths and weaknesses of networked forms of organization, the obvious primary properties to consider are their decentralized nature

[24] One such standardized approach is the OASIS Open Reputation Management System (ORMS): http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=orms

and lack of central authority. Virtually all strengths and weaknesses can be directly derived from these properties[25].

4.1. *Strengths*

In both the terrorism and the Internet context, networked forms of organization offer advantages over hierarchical forms. As early as 1969, Carlos Marighella hinted at the strengths of networks by stating that an urban guerrilla group should seek to avoid centralization and to avoid looking like the enemy (i.e. the strictly hierarchical police)[26].

Perhaps the most important advantage of networks lies within their resilience against disruptions and attacks. Whereas hierarchical structures contain potentially weak points that offer attractive targets for attackers, networks are less likely to contain such weak spots. Even when attacks occur, networks are more effective in repairing topological damages due to their redundant and easily readjustable links. In the Internet context, although the popular idea that the Internet has been designed from the start by the U.S. military to maintain a stable communication system in the event of a large-scale nuclear attack is by large an urban legend, it is true that its low-level hardware infrastructure can theoretically withstand significant disruption and interference. The ability to easily add and remove new links also makes networks highly scalable, i.e. makes it possible to recruit and integrate new nodes into the network at any time, or even join separate networks together.

In networked structures, several types of problems can be distinguished, such as the failure of individual nodes and the failure of individual links. Such failures can have several effects on a network: The overall least harmful case is a fail-silent fault, i.e. a node or link becomes completely non-operational. On the other end of the spectrum, the most harmful case is a so-called Byzantine fault, which means that the affected node or link stay operational, but alter their behavior in a way that causes the largest possible adverse effect on the network, e.g. by transmitting illicit and confusing messages. Examples for fail-silent faults would be the hardware failure of an Internet server or connection, or the arrest of an individual member of a terrorist network. A typical example for a Byzantine fault is the infiltration of a network with a malicious node that

[25] For a great overview of network strengths and weaknesses, see (Eilstrup-Sangiovanni & Jones, 2008).

[26] See (Marighella, 1969)

consciously tries to damage it. In classic theory of distributed systems, it can be shown that in order to resist N fail-silent faults, a network has to consist of at least 2*N+1 nodes, and in order to resists N Byzantine faults, a network has to consist of at least 3*N+1 nodes, assuming that networks are well designed and equipped with algorithms to handle such fault situations.

Another well-documented strength of networks is their ability to transmit and process messages in a very efficient way, bypassing hierarchies that may cause obstruction and delays, and getting information directly to the node(s) that needs it. Links between nodes can dynamically be optimized, and communication channels that are found to be valuable can immediately be used again.

Yet another possible strength of networks is the concentration of all its resources toward a single goal (which however presumes the existence of a solution to coordination problems; see next section). This kind of activity is usually referred to as "swarming" and can be compared to bees attacking a superior foe: By itself, a bee sting is usually harmless, but when an entire swarm of bees attacks a single target at the same time, the effect is much greater. A similar kind of attack exists in the context of Internet networks and is well document. In a so-called denial-of-service attack, a single centralized server system is simultaneously flooded with requests by a large amount of client computers, rendering the target unable to response to legitimate requests.

4.2. Weaknesses

Although network structures offer several potential advantages, there are weaknesses as well. In fact, the two most often cited advantageous properties of networks – their decentralized nature and lack of central authority – can simultaneously also be seen as the source of weaknesses. Basically, the absence of a central structure can make it hard to make decisions, hard to resolve emerging conflicts within the network, hard to locate and contact nodes and resources within the network, hard to agree on joint initiatives and hard to control the implementation of such initiatives. Another disadvantage – especially of social/organizational networks, not so much of Internet networks – is that participation in is usually voluntary (see 2.6), and that there are no orders and no or hardly any notion of personal obligation and accountability. In some social/organizational networks, the individual nodes have no common ground except for a common purpose or ideology, which however may be too loosely defined to be useful for network coordination purposes.

Also, while a network is flexible in providing logistical resources to its nodes, it can be difficult or impossible to concentrate the resources of the entire network for a larger operation. As (Eilstrup-Sangiovanni & Jones, 2008) explain, the type of terrorist attack of 9/11 that was executed by the classic, hierarchical Al-Qaeda organization is unlikely to be executed again by the more decentralized Post-Al-Qaeda movement which today consists mostly of small cells, which – although dangerous – mostly lack the resources for large-scale operations.

Similar difficulties of coordination and joining of resources can be found in the context of Internet networks. In some cases, applications offering the same functionality have been built in both centralized and decentralized ways, with the former usually winning the race for reliability, performance and – most importantly – user acceptance. One example is the Joost[27] video distribution platform, which was initially developed as a peer-to-peer system where large amounts of video data were streamed[28] directly between end-user computers, with only some hierarchical elements incorporated into the structure. This approach however proved to create insurmountable challenges in terms of reliability and performance of the network, and the project leadership soon

decided to completely replace their decentralized architecture with a classic centralized approach. Another example is the popular micro-blogging service Twitter[29], whose technology does not actually offer much functionality to end-users beyond what has already existed before, but which proved to be immensely successful due to the simple user experience offered by its centralized architecture.

[27] http://www.joost.com, formerly known as "The Venice Project"

[28] "Streaming" is a delivery method for multimedia data that constantly sends pieces information just in time as they are needed. This method heavily relies on stable bandwidth and latency parameters which can be hard to achieve by end-user computers.

[29] http://www.twitter.com

5. Adoption of Internet Network Methods by Terrorist Networks

I have outlined various forms of social/organizational and Internet network structures as well as communication patterns, strengths and weaknesses of such structures. It can be argued that software architects and engineers have had much more resources at their disposal in designing and implementing robust Internet network structures than the actors of terrorist groups have had in the introduction of social/organizational networks e.g. in the Post-Al-Qaeda movement. Furthermore, while the former case is based on coordinated, well-planned efforts, the latter has evolved in a relatively spontaneous if not anarchic way. The conclusion from this realization is that despite the many similarities, Internet networks are likely better designed than terrorist networks.

In this section I will now describe potential ways in which terrorist networks could adopt well-known methods of Internet networks. This could potentially lead to more advanced communication and cooperation patterns that might result in more stable links, more reliable message transmission and networks that are harder to understand and disrupt. While considering this, it is important to keep in mind that from a security perspective, an Internet network developer would find himself in the opposite role of a counter-terrorism agent. While the former should be interested in making the Internet network secure, stable and hard to disrupt, the latter will try to attack the terrorist network's structure and disrupt its information flow.

The first step in such an evolutionary process to adopt Internet networking methods by terrorist groups would be the introduction of a robust concept of identity through the entire network that goes beyond Human-meaningful names (see 2.5). This naming system can then serve as a basis for establishing the network's links as well as for providing a set of new services.

The fact that a lack of central authority complicates coordination, decision making and controlling an implementation process can potentially be alleviated by the effective use of communication patterns such as Multicast, Anycast and Broadcast (see 3.1).

Lessons from Distributed Storage systems (see 3.2) could help terrorist networks to more efficiently learn and preserve information, even if major restructuring processes occur in the network.

The introduction of cryptographic paradigms such as a Public Key Infrastructure (see 3.3) can introduce reliable authentication and confidentiality to the messages that are being exchanged between nodes.

The absence of central oversight, orders and punishments can be compensated for by the augmentation of stabilizing factors such as social bonds, trust, reciprocity and common ideology with methods known from Reputation Systems (see 3.4), in order to make nodes more accountable for both immediate actions and long-term behavior, and more resistant against attacks from malicious actors.

6. Conclusion

I have given an overview of some basic properties of two kinds of networks – terrorist networks such as the kind that can be referred to as Post-Al-Qaeda, and various kinds of Internet structures, such as the Federated Social Web and Distributed Hash Tables.

I would like to reemphasize the observation that in recent years, both terrorist and Internet networks have seen shifts toward more decentralized and less hierarchical forms of organization. First, there is the transformation from the classic hierarchical organization called Al-Qaeda to the much more decentralized, networked social movement referred to as "Post-Al-Qaeda". Second, there is this movement's vision of replacing the current world order with a global Islamic Caliphate that is free of nation-states and enables men to stand directly before God. Third, in the Internet context, decentralized technologies such as the Federated Social Web and Distributed Hash Tables have recently attracted a lot of attention. These three observations are all strikingly similar insofar as they abolish – almost antagonize – hierarchies in favor of flat networks.

I have argued that from the host of experiences that software architects and engineers have gathered during the evolution of modern Internet networks structures, terrorist groups could potentially be able to augment their own networks to be more robust and efficient. Such networks would be able to withstand high restructuring and high degrees of infiltration, and they would expose new services to their individual nodes. In other words, detailed knowledge about the inner workings of certain Internet networks can provide added stability as well as new "functionality" such as unicast, multicast and broadcast sending of messages, storage of information in the network itself, cryptographic features and reputation system.

Given the probable fact that Post-Al-Qaeda's top strategic and ideological leadership today is comprised of young, educated people of the so-called "Internet generation", it may only be a matter of time until such learning takes place. At that point, one of the most promising approaches in counter-terrorism strategies of nation-states and international organizations could be to also learn lessons about the properties (especially the weaknesses) of well-known Internet networks.

7. Bibliography

Arquilla, J., & Ronfeldt, J. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militanc.* Santa Monica, CA: RAND.

Baset, S., & Schulzrinne, H. (2006). An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. *Proc. IEEE INFOCOM.*

Berners-Lee, T. (1998). *Uniform Resource Identifiers (URI): Generic Syntax.* Retrieved from http://www.ietf.org/rfc/rfc2396.txt

Castells, M. (1997). *The Information Age: Economy, Society and Culture: The Power of Identity* (Vol. 2). Oxford: Backwell.

Castells, M. (2000). *The Information Age: Economy, Society and Culture: The Rise of the Network Society* (2 ed., Vol. 1). Cambridge, MA.

Eilstrup-Sangiovanni, M., & Jones, C. (2008). Assessing the Dangers of Illicit Networks: Why al-Qaida May Be Less Dangerous Than Many Think. *International Security, 33*(2), 7-44.

Leach, P. (2005). *A Universally Unique IDentifier (UUID) URN Namespace.* Retrieved from http://www.ietf.org/rfc/rfc4122.txt

Marighella, C. (1969). *Minimanual of the Urban Guerrilla.* Retrieved from http://www.marxists.org/archive/marighella-carlos/1969/06/minimanual-urban-guerrilla/index.htm

Powell, W. (1990). Neither Market Nor Hierarchy: Network Forms of Organization. In *Research In Organizational Behavior* (Vol. 12, pp. 295-336).

Redwine, E., & Holliday, J. (2003). Reliability of Distributed Systems. In *Encyclopedia of Distributed Computing.* Kluwer Academic Publishers.

Reed, D., & McAlpin, D. (2005). *Extensible Resource Identifier (XRI) Syntax Version 2.0 - Committee Specification.* Retrieved from http://www.oasis-open.org/committees/download.php/15377

Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century.* University of Pennsylvania Press.

Stepanova, E. (2008). *Terrorism in Asymmetrical Conflict: Ideological and Structural Aspects.* Oxford: Oxford University Press.

Tsoukas, H., & Knudsen, C. (2005). *The Oxford Handbook of Organization Theory.* Oxford: Oxford University Press.

Weber, M. (1947). *The Theory of Social and Economic Organization.* (A. M. Henderson, & T. Parsons, Trans.) Glencoe, IL: Free Press.