Interpersonal Trust on Jihadi Internet Forums

Thomas Hegghammer*
Norwegian Defence Research Establishment (FFI)
hegghammer[at]gmail.com

19 February 2014

Draft chapter to be included in Diego Gambetta (ed.),
Fight, Flight, Mimic: Identity Signalling in Armed Conflicts, forthcoming.

Abstract: This chapter explores the effects of the trust problem on jihadi internet discussion forums. The scarcity of non-verbal cues in digital communication facilitates deceptive mimicry, which undermines the interpersonal trust required for sensitive transactions. Open-source data from Arabic-language jihadi forums between 2006 and 2011 indicate that distrust there was high and direct recruitment rare. General trust also declined over time as policing of the forums increased. As of 2014, forums are still in use, but primarily for low-stake activities such as propaganda-sharing and ideological debate, not recruiting or operational coordination. Confidence in the authenticity of propaganda remained relatively high, due to vetting institutions and hard-to-fake video formats. A modicum of interpersonal trust also remained, thanks to reputation systems and a few relatively reliable signs of trustworthiness involving time expenditure. The trust problem is an Achilles heel for high-risk activists online, including pro-democracy activists in authoritarian settings.

*Special thanks to Diego Gambetta for detailed comments on an early draft of the manuscript. Dorothy Denning, Lynn Eden, James Fearon, Tim Junio, Christopher Sullivan, and Aaron Weisburd also contributed constructive remarks. I thank all who participated in the seminars discussing the paper at the Stiftung Wissenschaft und Politik in Berlin, Stanford University, the Naval Postgraduate School, UC Berkeley, Lawrence Livermore National Laboratories, and Yale University.

Ask yourself, why does this person trust you? In a world where literally anyone can be a spy, why does this person trust you? Why are they claiming to be a Mujahid, and telling this to a person who they met over a computer or at the masjid? Why are they telling you they want to conduct Jihadist operations or make hijrah? You cannot know if anyone is sincere, and this is the sad reality. Think about why they would trust you of all people, and not someone else. The answer is because they are seeking to arrest you.

From "10 Methods To Detect And Foil The Plots Of Spies",
Ansar al-Mujahideen Forum, 19 December 2010

1 Introduction

The Internet is often believed to empower international terrorists by allowing them to communicate, recruit, and fundraise rapidly across long distances. This chapter argues that the Internet's usefulness for high-risk activists is limited, to at least some extent, by the trust problem. The scarcity of non-verbal cues in digital communication facilitates deceptive mimicry, which undermines the trust required for sensitive transactions such as recruiting. Below I present open-source evidence from jihadi discussion forums showing that distrust there is rampant and direct recruitment rare.¹ Users try to mitigate the problem with vetting agencies, reputation systems, complex document formats and sorting knowledge, but trust remains fragile. These insights have direct implications for counterterrorism policy and indirect relevance for online pro-democracy activism in authoritarian states.

The chapter speaks to a long-running scholarly debate over the Internet's usefulness for political activists. Technological optimists emphasise the Web's advantages, arguing that it empowers non-state actors and facilitates transnational activism (Arquilla and Ronfeldt 2001; Castells 2004; Tarrow 2006). A substantial literature expounds on the Internet's many presumed benefits for international terrorists in particular (Weimann 2006; Nacos 2002; Seib and Janbek 2011). Technological pessimists, by contrast, highlight the risks and problems terrorists face online (Amble 2012; Conway 2006b; Diani 2000; Kenney 2010; Torres-Soriano 2012; Zanini and Edwards 2001). This study sides with the pessimists by highlighting one of the most fundamental of these challenges, namely, the trust problem. Interpersonal

¹"Jihadi" is an adjective derived from "jihadism", which I equate with "violent Sunni Islamism". I define Islamism as "activism justified with primary reference to Islam".

trust, or "the willingness to accept vulnerability or risk based on expectations regarding another person's behavior" (Borum 2010), is a vital prerequisite for human cooperation (Misztal 1996). In cyberspace trust is fragile because the absence of non-verbal cues makes it is easy to lie. Hunted activists must be especially cautious, lest they fall victim to deceptive mimicry from a government *agent provocateur* or other types of "faux activists" (Marx 1974; 2012). The threat of digital surveillance adds to their woes.

The chapter is an empirical probe into the effects of the trust problem on the social interactions between militant Islamists online. I examine pro-al-Qaida discussion forums, asking three main questions: How much trust is there between users? What types of signs instil trust and distrust respectively? Which strategies do users follow to guard against deception? I also hope to shed light, in the process, on broader questions in trust research, including: can trust arise at all among high-risk activists in virtual settings? What happens to the semiotics of signs (Bacharach and Gambetta 2001) when all signs are virtual? What makes a costly sign in cyberspace? We lack answers to these questions because, with the exception of a few works on cybercrime (Lusthaus 2012), the online trust literature has been mostly concerned with low-risk activism.

I study jihadi forums because they are frequented by hunted men and their government foes; it is an arena where the trust problem should be particularly acute and its effects therefore more easily observable. Jihadi forums are also worth studying because they have been central to the al-Qaida movement in the post-9/11 era. In the words of a leading observer, this is where the global jihad is headquartered online (Zelin 2013: 6). I use open-source messaging data which I process qualitatively with content analysis.² The data have many limitations, but they allow at least for some tentative insights into the internal communications of an otherwise highly clandestine community.

The chapter has six parts. First I describe what a forum is; then I review the literature on online trust, before presenting and discussing my data. In the fourth part I document the various forms of deceptive mimicry taking place on the forums. The fifth part assesses the overall level of trust through indicators such as sensitive information exchanges and expressions of distrust. In the final part I examine the way in which users assess signs and the strategies they have developed to mitigate the trust problem.

² All the data used and primary sources cited will be made available on my personal webpage (www.hegghammer.com) in the Resources section.

2 Jihadi discussion forums

Radical Islamists established a presence on the Internet in the mid-1990s, and since the early 2000s they have been at the forefront of rebel Internet use, exploiting it more extensively than most other types of militants (Lappin 2011; Bunt 2003; Bunt 2009; Ranstorp 2004, 2007; Hoffman 2006; Drennan and Black 2007; Seib and Janbek 2011; Conway 2006a; Rogan 2006, 2007; Brachman 2006; Thomas 2003; Awan et al. 2011; Seib 2008). Today they are all over the World Wide Web, from static websites via blogs and forums to social media (Zelin 2013). In addition, they communicate by email, IP telephony (such as Skype), voice chat (such as Paltalk), text chat (such as MSN Messenger), and much more. The world of "online jihadism" is complex and in constant flux; websites come and go, new technologies replace old ones, and the actor landscape changes (Weisburd 2007; Lia 2005; Kimmage 2008).

Discussion forums were adopted as a communication platform by jihadists around 2000 and remained their most important online meeting place from the early 2000s to the early 2010s. Today forums remain important, but they seem to have been overtaken in 2013 by Facebook and Twitter as the preferred platform for internal multi-user communication. The jihadi migration to Facebook and Twitter has yet to be properly explained, but the breakdown in trust on the forums may have been a contributing factor. However, even if forums were to become obsolete in the coming years, they are worth studying for the light they may shed on general aspects of high-risk activism online.

A discussion forum is basically a digital notice board where users can post anything from one-word messages to elaborate propaganda products (Musawi 2010; ICT 2012). Access is generally open: all forums allow users to register with a username and password. Most forums are also accessible to non-registered visitors, but some forums require users to log on in order to access parts (and occasionally all) of the forum. This barrier is sometimes described by observers as password-protection, which is partly misleading because anyone can register and choose their own password.³

Forums are made up of individual messages or "posts". Users can add follow-up posts to existing posts, thereby creating "threads" (or "conversations"). Threads have headlines and are listed chronologically, the most recent on top, in a "section". A jihadi forum typically has 5-10 different

³ There have been instances of forums ceasing to accept new registrations, in which case access was limited to existing account-holders. However, existing account holders still numbered in the thousands and were not screened.

sections on different topics such as "news", "statements", "Sharia matters", "tactical matters", and the like. A section page (see Figure 1) is typically divided into three areas: the top part is filled with graphic banners advertising films and statements by major groups. The second part lists "sticky threads", i.e., the 10-20 threads deemed by forum administrators to merit extra attention. (They "stick" to the upper part of the page instead of being pushed down by new messages). The third part of the page lists the regular threads.

Since the early 2000s, there have been between 5 and 15 jihadi forums in operation at any one time, although traffic has tended to cluster in one or two "market leaders".⁴ The forum ecosystem is constantly changing; aside from URLs changing frequently (up to several times a year), a forum rarely exists for more than a few years (sometimes only months) before it disappears without explanation.⁵ We lack reliable traffic data, but messaging activity suggests that the top forums are frequented by at least several hundred individuals every day. Activity appears to have increased markedly in the second half of the 2000s: the aggregate annual number of threads on the al-Falluja forum, the market leader for most of this period, increased from 3,000 in 2006, via 18,000 in 2007 and 19,000 in 2008, to 56,000 in 2009.⁶ Subsequent activity appears to have stagnated at the 2009 level. In the spring of 2012, Zelin (2013) observed around 150 threads per day (corresponding to around 55,000 per year) on the al-Shumukh forum (the new market leader). According to Zelins count, al-Shumukh saw between 1500 and 2000 posts per day in early 2012, while the number two forum (al-Fida) had between 700 and 900 posts per day.

We cannot know exactly who the users are, but at least four ideal type categories appear to be represented. First and most numerous are the "consumers", the young unaffiliated Islamists who access forums primarily to read, exchange, and comment on news and propaganda products. Second most numerous are the "propagandists", whose main preoccupation is the

⁴ For names and URLs of jihadi forums from 2009 onward, see the article series titled "Top Ten Jihadi Forums" on Aaron Weisburds *Internet Haganah* website; for example at <http://internet-haganah.com/harchives/007253.html> (accessed 16 February 2013)

⁵ When the URL of a forum "breaks", users wait until the new address is announced on other forums or websites. The reemergence can take hours, days or even weeks, and meanwhile, users cannot know whether the forum is simply moving or gone for good. The cause of a forum's disappearance is almost never publicly known, but candidate explanations include hacking by governments and private actors, arrest of the site administrators, and eviction by the Internet service provider.

⁶ These are rounded numbers, obtained from the Dark Web Forum Portal at the University of Arizona (<http://ai.arizona.edu/research/terror/>).

distribution of ideological documents. Third and fewer in numbers are the "operatives", i.e., the members of active groups who seek to obtain operationally useful information and conceivably to recruit. Fourth is a small number of "impostors", consisting of the intelligence operatives, journalists and academics who listen in on the above while staying silent or mimicking jihadists. Virtually all impostors participate under false names, with the exception of a few government actors (notably the US State Department) who make a point out of being visible. Each of these actor categories has a different motivation for frequenting the forums. Important for our purposes is the fact that only a small subset of visitors — the operatives and some of the consumers — have an interest in engaging in a recruitment exchange.

3 The trust problem

There are good reasons to expect distrust among users on jihadi forums. Online trust research showed early that computer-mediated communication (CMC) is fraught with problems (Parks and Floyd 1996) and that interpersonal trust is notoriously difficult to establish in electronic contexts (Rocco 1998). The obstacles to online trust are many (Nissenbaum 2001), the most important being the absence of non-verbal cues, which gives CMC a "narrower bandwidth" than face-to-face (FtF) communication. Experimental studies suggest a correlation between the width of a given medium's range of cue types on the one hand and interpersonal trust on the other (Bos et al. 2002). Hancock (2007) also found that highly motivated liars get away with more in CMC than in FtF. Surveys also document a lower general trust in Internet-based acquaintances and transactions than in offline ones (Naquin and Paulson 2003). Studies of romantic online relationships show that involvement tends to be lower and misrepresentation (e.g. of age and appearance) tends to be higher in cyberspace than in offline relationships (Cornwell and Lundgren 2001). On this note, see Figure 2 for a classical illustration of the bandwidth problem.

In low-risk exchanges, such as casual chatting, low bandwidth is not necessarily a problem. On the contrary, early users of chat services argued that the Internet was powerfully inductive to intimacy and that people open up sooner to anonymous online friends than they would in real life (Van Gelder 1985). In a study of online communication, Parks and Floyd (1996) noted that "personal relationships were found far more often and at a far higher level [...] than can be accounted for by the reduced-cues perspective."

However, when stakes of an interaction increase to involve, say, the love,

Figure 2: Cartoon illustrating the "bandwidth problem" in computer-mediated-communication.

money, or especially the personal safety of the truster, then it becomes a different ballgame. The dangers of deceptive mimicry have been known since the early days of the Internet (Myers 1987; Van Gelder 1985; Lea and Spears 1995; Donath 1998; Hancock 2007). There was the famous case in the early 1980s of a male New York psychiatrist who passed himself off as a disabled woman named Joan on CompuServe networks in an odd search for female emotional intimacy (Van Gelder 1985). Pecuniary fraud has long marred e-commerce. Around 2000, three per cent of all American consumers had experienced credit card fraud while ten per cent had paid for items online that were never delivered (Williams 2001; Fox 2000). More recently, the Robin Sage Experiment (Ryan 2010), in which a security consultant used a fake Facebook profile to gather sensitive information about members of the US intelligence community and major corporations, illustrated that digital mimicry can be a national security issue.⁷

Unfortunately we know little about the sources of trust (i.e., the salient variables affecting trusting decisions) between people online. The online trust literature has paid far more attention to trust in commercial websites than to trust in individuals (Corritore et al. 2003). There is a large body

⁷ I thank Mark Stout for drawing the Robin Sage story to my attention.

of research aimed at finding ways to improve consumer trust in websites (Frankel 2001; Wang and Emurian 2005; Koehn 2003; Grazioli and Jarvenpaa 2000; Anderson 2006; Friedman and Kahn Jr. 2000). The sources of online interpersonal trust, on the other hand, are less well understood (Green 2007; Donath 2007; Feng et al. 2004; Kling 1996). There has been some work on avatars (Bailenson and Beall 2006; Galanxhi and Nah 2007), but avatar use appears to have only minor effects on perceived trustworthiness, even in low-risk interactions.

The general literature on trust has much to say about the sources of trust in offline contexts (see Borum 2010 for a review). A much-cited contribution is that of Sztopka (1999), who argues that people determine the trustworthiness of others based on three main variables: reputation (record of past deeds), performance (present conduct), and appearance. It is not immediately obvious, however, how these variables are assessed in cyberspace, where information about things like appearance and performance is both limited and unreliable. Moreover, reputation may not be relevant at all when a person's very identity is in question. In fact, very often, the main problem for high-risk activists online is not that interlocutors are less reliable than they say they are, but that they simply are not who they say they are.

Such "deceptive mimicry" has been analysed by Gambetta (2005), who argues that trusters vet trustees by looking for "costly signs". He proposes an analytical framework that builds on signalling theory and the idea of differential signal costs. He adds two important components, namely, a classification of signs and a taxonomy of mimicry systems. The former distinguishes between cues (congenital features), marks (lifestyle by-products) and symbolic signs (conventional gestures, dress or statements), with cues and marks being costlier to mimic than symbolic signs. The notion of mimicry system refers to the constellation between dupe, mimic and model in a given mimicry episode. As the other articles in this book demonstrate, Gambetta's framework has proved analytically useful in studies of many types of real-life mimicry, including terrorist recruitment (Hegghammer 2013). Transposed to an online setting, however, the framework is not immediately applicable, because the signs available online are different from those in the physical world. It is notably very difficult for the truster to assess the cost of a computer-mediated sign, since in principle, all digital messages can be manipulated. Gambetta himself (2005: 225) expects mimicry to be easier in low-bandwidth media (in the dark or over the telephone), but does not predict the precise effect of the low bandwidth on what he calls the "semiotic structure of signs".

In this chapter, I apply analytical concepts from the trust literature with minor modifications. I distinguish trust (the willingness to accept vulnerability) from trustworthiness (the individual property that inspires trust). I also reserve the term trust for human interaction; things or technologies are objects of confidence. In this context, confidence in communications technology is synonymous with low fear of surveillance. However, a website or a document can represent people and thus be an object of trust ("I trust this forum because I consider its administrators to be trustworthy"). Although the main focus is on interpersonal trust, the chapter also considers confidence in technology, since both affect users willingness to share sensitive information.

I focus on deceptive identity mimicry, but recognize that the threat of it is but one of several sources of interpersonal distrust. One need not be considered a potential spy to be untrustworthy; lack of commitment or sloppiness can also instil distrust. Jihadi forums contain several mimicry systems, of which I consider only one, namely, what Gambetta would call the "mimic versus dupe-model." Here, spies (mimics) pass themselves off as genuine activists (models) in order to obtain sensitive information from, or confuse, the real activists (dupes).⁸ In this system model and dupe are the same category of people.

4 Sources and methods

I use open-source data with several problems and limitations. The first is an epistemological one, namely, that trust is difficult to observe in forum posts, because users rarely make the outcome of their trusting decisions explicit. Positive trust may be expressed in many different ways depending on the purpose of the conversation, and distrust may produce either suspicious remarks or nothing at all. In fact, when someone decides not to trust, nothing special happens, and we will not even know that a trust exchange occurred in

⁸ Another system not examined here is mimic versus dupe via the model, which comes in two varieties: a) senior activists from group X produce propaganda in the name of a fake group Y in order to mislead spies, and b) unaffiliated junior activists try to pass themselves off as members of a known group to get attention from other activists or to mislead spies. One might expect to see a third variant of this system in the form of activists posing as informants in order to get sensitive information from spies, but I have not observed this, at least not on the Internet. However, it happens in real life, as illustrated by the case of the Jordanian double agent who killed six CIA operatives in Afghanistan in late 2009 after posing as an informant (Warrick 2009). One might also add the phenomenon of negative mimicry or camouflage, in which activists (mimics) mislead spies (dupes) by trying to appear less radical than they really are.

the first place. The second problem regards validity: it is difficult to extract a representative sample of messages because the universe of jihadi forums is diverse and shifting. Different forums may have slightly different user populations, constraints, and cultures, which presumably makes for variation in trust dynamics. Third, the reliability of the data is vulnerable to the same external manipulation that undermines online trust among jihadis. Some expressions of distrust, for example, may be forgeries produced precisely to undermine trust.

I pursued a four-pronged data collection strategy. First, I gathered a body of secondary literature on online jihadism by searching academic databases (EBSCO, WorldCat, Google Scholar) and media databases (Lexis-Nexus, Google News) for relevant terms such as "Internet / online / web / cyberspace / forums AND terrorism / terrorist / jihad / jihadism / Qaida / Qaeda." I then reviewed this literature, doing my best to identify references to 1) evidence of surveillance and infiltration on forums, 2) cases of successful direct recruitment or fundraising through forums, and 3) forum posts expressing distrust, such as spy accusations levelled at others, general warnings against surveillance, advice on how to spot an impostor, and the like. I would then dig deeper into each case by conducting additional searches and examining the available primary sources.

Second, I conducted a systematic search for select spying-related terms in the archive of the forum Falluja, available in a database called the Dark Web Forum Portal (DWFP) established by the University of Arizona.⁹ The archive covers the years 2006 through 2009 and includes content from all forum subsections, 96,000 threads in total. From these I collected all threads containing the Arabic words *tajassus* (spying), *jawasis* (spies), and *ikhтираq* (infiltration). This yielded a sample of 314 threads. I coded posts by topic to generate some descriptive statistics, and I used content analysis to identify the posts with the most detailed description of sign assessment.

Third, I browsed a small sample of forum threads from the "Umma affairs" section of the Arabic-language Ansar al-Mujahidin forum from the second half of 2011.¹⁰ I examined the posts, looking for: 1) examples of

⁹ See <http://ai.arizona.edu/research/terror/>.

¹⁰ <http://as-ansar.com/vb/forumdisplay.php?f=3> (accessed 16 February 2013). The "Umma Affairs" section is a regular feature on jihadi forums and constitutes its "center of gravity"; this is the most active (measured in threads per day) of all the forum sections, and it is where the latest news or the hottest topics are discussed. It arguably reflects the general atmosphere on the forum better than any of the other sections, which are devoted to more specialized topics such as legal matters, literature, statements etc. I deliberately did not sample the section on "technical security", because it is devoted to countersurveillance issues and would lead to overreporting of infiltration concerns.

users divulging autobiographical information, and 2) expressions of distrust of the same type as described above. My sample consisted of all threads that were last dated on the 9th and 23rd of each month from July to November 2011, 232 in all.¹¹ These threads contain between 1 and 202 individual posts, although most contain less than 10 posts. In this period, Ansar al-Mujahidin was the second most frequented Arabic-language jihadi forum.

Fourth, I examined the architecture and formal features of five different forums (Falluja, Shumukh, Ansar al-Mujahidin, Fida, Jihad) at different points in time between 2009 and 2013, looking for design features (such as reputation systems) that appeared to reflect trust concerns or have a trust-building purpose.

I then subjected these data to a three-step qualitative analysis. I started by reviewing open-source evidence of infiltration of jihadi forums to establish that the threat of deception is real and consequential. I then assessed the level of general trust on the forums through two indicators: 1) evidence that jihadis engage in sensitive transactions (such as recruitment) with people they first encounter on the forums, and 2) the number and content of messages expressing distrust. In the third step I sought to understand how users assessed signs in interlocutors and which strategies they use to avoid deception.

5 Assessing the repression level

Radical Islamists have good reason to be cautious online. Both governments and private actors take a range of hostile measures against jihadi websites (Weimann 2006; Shahar 2007). Much of this activity shrouded in secrecy, but we can get a whiff of what is going on from secondary sources.

Although some governments appear to have the technical capability to at least temporarily close down jihadi websites and occasionally do so (Mantel 2009:132-135; ICT 2012:35-39), most governments pursue a strategy of surveillance and subversion rather than direct attack. Closing websites permanently is legally complicated, users can always migrate to new websites, and there are intelligence benefits to leaving forums intact.

Jihadis thus face two main types of dangers online: surveillance and deceptive mimicry. Each involves a different set of dilemmas for its targets.

¹¹ The "last dated" criterion was primarily chosen for convenience since threads are listed that way on the forums but it also has the advantage of adding more randomness to the sample, since there is presumably no systematic relationship between a thread's initiation date and its "last modification" date. A thread last dated on, say, 23 July, could conceivably have been started on any day earlier that month, or even earlier.

Surveillance undermines confidence in the communication technology itself, while mimicry affects trust in ones interlocutors. Surveillance can be met with technological solutions (such as encryption), while deception requires vetting procedures.

5.1 Surveillance

Jihadi forums appear to be under close surveillance. Since at least the early 2000s, agencies such as the US National Security Agency (NSA) and the UK Government Communication Headquarters have had automated systems that capture, sift and store both content and user data on a range of digital communication channels, including forums (Talbot 2005). Documents leaked in 2013 by former NSA contractor Edward Snowden suggest that the surveillance and tracking capabilities of the NSA and GCHQ had reached a formidable level by the early 2010s. In addition, both intelligence services and private groups such as SITE and MEMRI manually monitor messaging content on jihadi forums. While formidable, the surveillance is clearly not comprehensive, otherwise all convictable online militants would presumably be captured. One challenge for authorities is stealth technology, such as web proxies, encryption software, and the like. Another is the sheer volume of traffic, which means that a particular message may be overlooked by analysts even if it is intercepted by their computers. Still, the tracking capability of governments is such that most high-profile online activists get caught eventually, even if they are very computer-savvy. For example, when the prominent forum figure Irhabi 007 (aka Younis Tsouli) was arrested in London in October 2005, it was considered remarkable that he had been able to taunt his online pursuers for two whole years before being caught.

5.2 Deceptive mimicry

Jihadis face three main types of deceptive mimicry on the forums: fake websites, false statements, and impersonations. The most famous case of website mimicry is that of the al-Hisba forum, which reportedly was operated by the CIA and Saudi intelligence as a "honey pot" from around 2006 to 2008 (Nakashima 2010).¹² Officials said the operation had been "a boon to Saudi intelligence operatives, who were able to round up some extremists before they could strike" (Nakashima 2010). A similar operation may have

¹² The forum was eventually dismantled in 2008 by the US military, reportedly against the wishes of the CIA. The former saw the forum as helping insurgents in Iraq, while latter saw it as a useful intelligence source (Nakashima 2010).

been attempted in 2009, when the al-Ekhlaas forum mysteriously resurfaced after a years absence, at the same time as the al-Fajr media distribution network was reportedly hacked and used to encourage forum members to sign up for al-Ekhlaas (Rawnsley 2011). Dutch intelligence (AIVD) is also reported to have carried out a honeypot operation, the details of which are not publicly known (Torres-Soriano 2012).

There is also some evidence that intelligence agencies manipulate statements in the name of jihadi organizations, though this is less well documented. Schmitt and Shanker (2011) quote a US intelligence official as saying that the ability of the intelligence community to persuasively imitate Al Qaeda web postings "does give an opportunity for confusion [...] if we can post an almost-authentic message. We have learned to mimic their 'watermarks.'" The official did not indicate which particular type of statements they had imitated.

Another type of document manipulation occurs when authorities capture unpublished propaganda during police raids and then post the material strategically on jihadi forums to see who accesses it. Saudi intelligence appears to have conducted such a mini-honeypot operation against al-Qaida on the Arabian Peninsula in early 2006 (Ulph 2006a).

Yet another variant of forgery is when governments distribute obviously false documents to send a blunt message that they are watching. In 2004, for example, online jihadists were confused by the appearance of two different versions of issue 14 of *Sawt al-Jihad* magazine, one of which appears to have been a government forgery (Torres-Soriano 2012). More entertaining was the co-called "Operation Cupcake" in 2010, in which British intelligence substituted bomb-making instructions in the magazine *Inspire* with a cupcake recipe (Gardham 2011). The purpose was primarily to make the bomb recipe unavailable, but perhaps also to poke fun at the real authors. Having said all this, it is implausible that governments manipulate more than a small proportion of all statements on the forums, because the overall quantity of propaganda is extremely large, and credible forgeries require highly skilled labour.

The third and for our purposes most important type of mimicry involves agents posing as real jihadis. According to Schmitt and Shanker (2011), the US military has "Digital Engagement Teams" consisting of fluent speakers of Arabic and other languages who infiltrate the forums under fake identities and "over time build up credibility and sow confusion." There are also unconfirmed but highly plausible claims that intelligence services from Arab countries, notably Jordan and Saudi Arabia, do the same (Ulph 2006b).

Detailed accounts of deceptive mimicry episodes are rare, presumably

because victims are imprisoned and governments are protective of their methods. It could also be that successful cases of deception are relatively infrequent due to the precautions taken by activists; we simply do not know. However, they do happen, and a good account is found in the testimony of Shannen Rossmiller, a municipal court judge in Montana who infiltrated forums as a self-appointed cyber-vigilante in the early 2000s (Rossmiller 2007). This is her account of the interaction with Ryan Anderson, a US soldier and convert to Islam:

In October [2003], while monitoring Arabic Islamist websites [...], I saw a message posted in English by a man calling himself Amir Abdul Rashid. He said he was a Muslim convert who was in a position to take things to the next level in the fight against our enemy (the U.S. government). He further requested that someone from the mujahideen contact him for details. I was suspicious because Rashid posted his message in English on an Arabic website and was openly seeking contact from the mujahideen. I traced his IP address back to an area outside of Seattle, Washington. Over time, it also became apparent to me that he was a member of the U.S. military. I posed as an Algerian with ties to that countrys Armed Islamic Group [...], and sent Rashid an e-mail in English with the subject line 'A Call to Jihad.' Rashid responded by asking if it was possible that a brother fighting on the wrong side could sign up or defect, so to speak. Over a period of four months, Rashid and I exchanged a series of thirty e-mails in English. I learned he was a member of the Army National Guard from Washington State, whose tank battalion unit was scheduled to be deployed to Iraq in February 2004. Through the course of our e-mail exchanges, Rashid provided me with information and materials on the weaknesses and vulnerabilities of the M1-AI and M1-A2 Abrams tanks as well as U.S. troop locations in Iraq. At all times during our communications, Rashid perceived me to be a mid-level Al-Qaeda operative. After our fifth e-mail exchange, I contacted the Department of Homeland Security, which put me in contact with my local FBI office.

Anderson's email exchange with Rossmiller earned him life in prison, which shows that bad trusting decisions on jihadi forums can carry very high costs. There are numerous other examples of people having been imprisoned as a result of their online activities (Mantel 2009). In addition to hurting

the individual, deception can damage networks and organizations. Schmitt and Shanker (2011) report one confirmed case in which a jihadist web site was hacked by American cyberwarriors to lure a high-value Al Qaeda leader to a surreptitious meeting with extremist counterparts only to find a U.S. military team in waiting.

The policing of jihadi forums appears to have become more systematic and aggressive over time. In 2001, the US Patriot Act made it illegal to advise or assist terrorists, including via the Internet, while the UK Terrorism Act of 2006 criminalised the encouragement or glorification of terrorism, including through Internet messaging. The mid-2000s saw a marked growth in forum monitoring and analysis by private actors, academics and other observers.¹³ Interviews with US officials suggest that a similar, if not larger, monitoring effort was exerted in the intelligence community.¹⁴

6 Gauging trust levels

Given what we know about the fragility of online trust and the dangers lurking on jihadi forums, we can make two testable predictions. First, we should expect users to be reluctant to engage in sensitive transactions that require divulging real-life contact details, because this makes them vulnerable to apprehension. Second, we should expect users to verbally express concerns about surveillance and deceptive mimicry.

6.1 Sensitive transactions

The available data suggest that sensitive transactions, which I assume to be indicators of positive trust, are very rare on the forums. Such transactions probably do happen occasionally, but if they were very widespread we would see more traces of them in the sources.

In fact, in the messaging data collected for this chapter, I observed no cases of direct recruitment, fundraising, or operational coordination mediated through the forums. There were no examples of two users exchanging contact details that would have allowed them to meet in real life. Nor were there cases of people exchanging account details that would have allowed for

¹³ Witness the increase in the output of monitoring services (e.g. SITE, MEMRI, BBC Monitoring and World News Connection), journals (e.g. Jamestown Terrorism Focus), and blogs (e.g. Internet Haganah) devoted to online jihadism during the late 2000s.

¹⁴ Author's interviews with US officials and former consultants to the US government, 2009-2011.

money transfers. Of course, I only reviewed a small sample of messages, so this is not sufficient evidence to conclude.¹⁵

However, other studies also report low levels of recruitment (Rogan 2006; Weimann 2007; Sageman 2004), operational coordination (Bergin et al. 2009; Tønnessen 2011), and financial transactions (Policy Planners' Network 2011; Tønnessen 2011) mediated directly through the forums. Moreover, one of the few available in-depth case studies of the recruitment tactics of a jihadi organization found that al-Qaida in Saudi-Arabia did not recruit directly online (Hegghammer 2013).

Some studies do argue that jihadis recruit, plot, and fundraise extensively online (Weimann 2007; Theohary and Rollins 2011; Denning 2009). They point to the fact that forums contain recruitment and fundraising calls, as well as travel advice for jihad fronts such as Iraq and Afghanistan (Kohlmann 2008). They also point to the several cases of people who say they joined a jihadi group after reading propaganda on jihadi forums.

However, these studies tend to speak of recruitment or fundraising in a broad sense, conflating radicalization processes inspired by online propaganda and recruitment transactions executed in cyberspace. On closer inspection, most of the available evidence of online recruitment are cases of forum-*inspired*, not forum-mediated recruitment. In most examples of "online recruitment" — see ICT (2012) for a good overview — we only hear about the recruiting organization reaching out (the demand side) or about the recruit responding to a general call (the supply side). None of the examples are cases of recruiters and recruits meeting online and exchanging contact details that enabled them to meet in real life. Forums probably do affect recruits wish to be recruited or funders wish to donate money, but they appear not to mediate sensitive transactions between people who only know each other online, at least not on a large scale.

A sceptic might ask why we should expect jihadists to exchange contact details on a forum in the first place, and whether the absence of such transactions tells us anything about trust. To this I would respond that al-Qaida and its affiliates are under-resourced and that forums have the potential to provide access to a much larger pool of recruits and funders than they would

¹⁵ It is possible that, by sampling only the Umma affairs section of the Ansar al-Mujahidin forum, I overlooked sensitive transactions on other sections of the forum. It is conceivable that recruiters, after identifying promising recruits in the Umma affairs section, diverted their targets to other parts of the forum for more sensitive exchanges. However, if this was a frequent occurrence, we should see examples of one user telling another to meet in another section, which we do not. The forum contains no sections labeled "recruitment", "for new members", "joining", or anything along those lines.

otherwise reach. For a labour market as small as this, where willing recruits are thinly spread out across the globe, the Internet could prove a highly effective mechanism connecting supply and demand. In an imaginary world where jihadis could operate freely, forums could serve as the LinkedIn or Craigslist for terrorist labour. For a more pertinent baseline comparison we may look to less contentious transnational activists such as WTO and G8 summit protesters, who have been able to use social media for recruitment and operational coordination (Van Laer and Van Aelst:236ff).

6.2 Expressions of distrust

In the absence of other indicators of positive trust, we may look to expressions of distrust as an negative indicator of trust levels. Presumably, the higher the frequency and intensity of the expressions of distrust, the lower the level of general trust in a community.

As one might expect, jihadi forums contain many warnings against spies, rumours of infiltration, advice on stealth tactics, and the like. To be sure, expressions of distrust represent only a small proportion of all forum posts. According to my Falluja message count, only some 0.3 percent of all threads contained the words spying, spies, or infiltration. Considering that this is only a subset of all possible word of distrust, my figure is reasonably consistent with the finding of another, unpublished study by Aaron Weisburd, which found some 1.5 percent of threads to be devoted to countersurveillance.¹⁶ This may not seem like much, but it is sufficient for the issue to come to readers' attention on a regular basis. Moreover, such messages may attract disproportionate attention; for example, on the Ummah News section on Ansar al-Mujahideen English forum in November 2011, three out of nine sticky posts were about how to avoid surveillance and spies on the forums.¹⁷

Another metric worth mentioning is the extent to which activists use web proxies, which hide IP addresses, or https URLs, which protect against data interception. According to Aaron Weisburd of Internet-Haganah.com, around 10-12 percent of jihadi forum users in 2010 employed proxies while even fewer used https URLs.¹⁸ These relatively low rates may be partly explained by the fact that most visitors only access forums to consume

¹⁶ Author's email correspondence with Aaron Weisburd, 23 February 2011.

¹⁷ See <http://www.ansar1.info/showthread.php?t=31326>; <http://www.ansar1.info/showthread.php?t=33459>; and <http://www.ansar1.info/showthread.php?t=29715> (accessed 21 November 2011).

¹⁸ Author's email correspondence with Aaron Weisburd, 23 February 2011.

propaganda, a relatively risk-free activity.

The concerns expressed in forum messages address a range of issues (for an extensive list of examples, see ICT 2012). Broadly speaking, they seem to cluster around the four dangers mentioned above, namely 1) surveillance, 2) website hijacking, 3) propaganda forgery, and 4) fake identities. In the following I present examples of such expressions.

First are surveillance fears, which make up the bulk of distrust messaging on the forums. Recurrent topics include:

- general warnings about surveillance¹⁹
- warnings about surveillance on other forums and communication channels (Biyokulule 2009)
- warnings against the use of internet cafes (Ulph 2006c)
- warnings against viruses and spyware (Rawnsley 2011)
- advice on using TOR and other advanced proxies²⁰
- advice on encryption software (Vijayan 2008)
- warnings about fake encryption software (Rawnsley 2011)

While most concerns appear in the form of separate threads or documents, they are also expressed during online conversations or in private messages. For example, in 2003 an user nicknamed "Aqil al-Masri" actively sought travel advice for Iraq on jihadi forums, after which he was contacted by another forum user who warned him against posting so much personal information online.²¹ Another academic forum observer, Torres-Soriano (2012), has noted jihadi "mistrust of anything originating in cyberspace: antivirus software, navigation tools, commercial e-mail accounts, and so on. Absolutely everything is suspected of concealing a trap. For example, a Jihadist site warned its followers 'to be careful with Google.'"

Second, forum users periodically flag their suspicion that specific forums and websites are operated or infiltrated by intelligence agents. Some examples:

¹⁹ See, e.g., "Essential advice and guidance to users of jihadi forums" <http://www.as-ansar.com/vb/showthread.php?t=31308>, dated 1 December 2010 [accessed 21 November 2011].

²⁰ "Explanation of how to use TOR, and how security and intelligence agencies can catch you like a fish," <http://202.71.102.68/alfalof/vb/showthread.php?t=46046> (accessed 9 August 2009).

²¹ <http://www.al-ekhlaas.net/forum/showthread.php?t=50742> (accessed 12 November 2007). I thank Truls Tønnessen for sharing this document.

- In 2004, the jihadist forum Al-Ma'sada warned about a possible CIA-sponsored forum called Batal (Ulph 2004).
- In early 2006, the Hisba forum was widely accused of being a "den of spies" by users on other forums, notably Tajdeed (Weisburd 2006b; Ulph 2006c).
- In November 2009, a Shumukh forum user issued a "Warning to followers and pioneers of jihadi forums about the Electronic Mujahidin Network."²²
- In 2010, an alleged Taliban spokesman warned on Falluja that "the [Taliban] main site and the site of its online journal al-Sumud, have been the subject of an 'infiltration operation.'" It warned others to not enter any of the links that concern these websites, and not even to surf [the content] until you receive the confirmed news by your brothers (Rawnsley 2010).
- In mid-2010, following a temporary, near-simultaneous shutdown of several jihadi forums, sites began blaming one another for the forums' collapse, with accusations about collaborating with the enemy against rival sites, or of having been infiltrated by enemy agents. Forum participants wondered which sites could be trusted and which were recognized by Al-Fajr, the prestigious jihadi media company organization that distributes videos and communiques from Al-Qaeda and its franchises. (MEMRI 2010).

Torres-Soriano (2012) argues that the forum users fear of infiltration has reached the stage of paranoia and notes that due to the fear of alleged infiltration, apparently innocuous events take on conspiratorial tones.

A third issue of concern is the authenticity of specific statements and videos. However, this suspicion is expressed much less frequently than surveillance or infiltration fears. One such message was entitled "A warning for those who post unconfirmed and false news about Jihad and Mujahideen."²³

Fourth and finally, numerous forum activists worry about *agents provocateurs*. Some posts advise general precaution, such as: "do not use the

²² <http://www.shamikh1.info/vb/showthread.php?t=52283> (accessed 21 November 2011).

²³ <http://www.ansar1.info/showthread.php?t=33459> (accessed 21 November 2011).

Internet for recruitment of new members under any circumstances.”²⁴ Others seek to intimidate potential spies, as did a ”Letter to the Treacherous Forum Spies” in 2011.²⁵ At other times, accusations target specific users. For example, in January 2004, the famous activist named ”Irhabi007” wrote, ”My brothers, I am convinced that there is a person spying on the forum, but fortunately I have figured out his IP, which is 62.233.243.116. The IP is registered in Poland” (Weisburd 2004). In some rare instances, victims of hacking warned about fake messages being sent from their own account; for example, in August 2011 a Shumukh user wrote: ”it seems that someone is using my account and is somehow sending messages with my name to the members” (Rawnsley 2011).

Forums also carry accusations against offline spies. In 2006, for example, there was much stir on the forums about a certain Abu al-Qaqa, an alleged Syrian agent supposedly involved in the capture of several volunteer fighters on the way to Iraq (Moubayed 2006). In August 2009 the name, picture, phone number and other details of an alleged Jordanian agent were posted on the Shumukh forum.²⁶ Forums have also been used to spread ideological treatises on spying in general and how to punish it. At least three such works have been widely publicized on the forums in recent years, namely Abu Yahya al-Libis (2009) ”Guidance on the Ruling on the Muslim Spy”, Abu al-Nur al-Maqdisi (2009) ”Ruling on the Spy in Islam”, and a more practical text entitled ”Dealing with Spies” by a certain Sayf al-Jihad (2010). Although these warnings and treatises are not expressions of *online* distrust, they are suggestive of a general fear of infiltration.

It is not surprising, then, that a substantial number of posts conclude that forums should not, under any circumstances, be used to exchange sensitive information. For example, one message on the Faluja forum in 2008 cautioned (ICT 2012):

Jihadist Web forums are not the appropriate place to plan or coordinate action in the field — that is, to plan an attack, to recruit participants in an attack, or to discuss implementing an attack, whether in a surfers home country or abroad. The forums are not sufficiently secure for this purpose: as noted, intelligence

²⁴ 911 Ghayr Muttasal, ”*al-amal al-jihadi al-sirri: istratijiyyat* (Strategies of secret jihadi operations)”, Muntadayat al-Masada al-Jihadiya, 18 March 2005 (accessed 13 May 2005).

²⁵ <http://sfir-arabicsource.blogspot.com/2008/06/rant-against-spies-in-forums.html> (accessed 21 November 2011).

²⁶ <http://www.shamikh1.info/vb/showthread.php?p=252283> (accessed 21 November 2011).

services can hack into them and their databases. Jihadist Web forums are not the place to make contact with other surfers or to divulge personal details — even if the other surfer asking for them has previously instructed you in the ways of jihad.

It should be noted that some qualified observers have assessed forum trust levels differently. A study by Dutch intelligence (AIVD 2012) argued that "there is great mutual trust on core forums [...] The virtual trust among members of such networks can be so unconditional that they may decide to meet offline and discover each others true identity." The study offered no examples of such meetings or estimates of their frequency. It is difficult to reconcile their assessment with mine. Perhaps classified sources show a different picture than open ones; perhaps they sampled a forum where trust levels happen to be higher, or perhaps they measured trust with a different method.

Interestingly, my data indicate that the level of distrust on the forums appears to have increased over time, especially in the second half of the 2000s. This author recalls seeing many cases in the early 2000s of forum users volunteering sensitive information such as their geographical location or even family connections.²⁷ For example, Saudi forum members would often post the telephone numbers to the homes of fellow Saudis killed in Iraq, indicating that they knew these families personally (Kohlmann 2008). Several long-time academic forum watchers have reported the same impression. Labi (2006) noted:

In the early days, before the Iraq War, the online global jihad amounted to a collection of chat rooms where angry members could let off steam and experiment with threatening graphics. The sites welcomed visitors, offering a painless process of registration; today they present tougher barriers to entry and place a greater emphasis on remaining anonymous and secure.

Similarly, Ulph wrote in 2006:

the number of postings on the Internet on the subject of infiltration has lately increased. Each jihadi forum site already includes a section on the use of proxies, giving detailed instructions on how to disguise the identity of reader and contributor and practical security precautions to take to ensure identity security.

²⁷ Unfortunately I did not think of storing the data at the time, so I cannot document these cases.

Likewise, Shahar (2007) observed:

jihadists confidence in their ability to dodge state control via the use of Internet forums has dropped significantly in the past couple of years. Despite the jihadist forum administrators best efforts to use proxies and to conceal participants identities, this kind of confidence may not be all that easily recovered.

By 2011, the forum users had become so jittery, according to one observer, that they "panic on hair trigger alert, at times blowing cyber incidents out of proportion" (Rawnsley 2011).

My count of spy-related threads on Falluja between 2006 and 2010 partly corroborates this anecdotal evidence. The data suggest that interest in spying as a general topic (i.e. offline as well as online) was stable in the late 2000s. However, the proportion of spy threads pertaining to online matters increased steadily, from 11 percent in 2006 to 22 percent in 2009. (The volume of messaging increased significantly in the same period.)

It is reasonable to assume that the increased interest in electronic spying is at least partly a response to the increase in government surveillance and subversion of jihadi forums from the mid-2000s onward. Increased repression, in other words, seems to have exacerbated the trust problem.

7 Exploring sign knowledge and mitigation strategies

7.1 Signs that instil and break trust

Knowing how jihadi forum users assess the trustworthiness of individual interlocutors is very difficult, since we have no detailed first-person accounts of trust exchanges. What we do have, however, is a number of texts offering general advice on "how to spot a spy", a genre that developed, perhaps not coincidentally, in the late 2000s. In principle, if we know what users consider red flags, we might be able to infer what they consider signs of trustworthiness. In the following, I examine two such texts.

The first example is a short forum post from 2009 entitled "Fake Profiles on Jihadi Forums" (Abu Jarir 2009) which lists six suspicious behaviours:

- "Working to sow discord among the mujahidin and their supporters"
- "Casting doubt on the overall method of the mujahidin, their leaders and clerics by highlighting their errors and disputes"

- "Working to hold Muslims back from jihad and supporting the mujahidin"
- "Asking about things regarding the mujahidin on the battlefronts, to obtain information enabling strikes at them" [...] "for example, one of them wrote asking about the number of groups fighting in Iraq, and are they mostly Sunni or Shiite? In which areas are they based? What are their names?"
- "Indirectly tarnishing the image of the mujahidin by mentioning some of their criminal acts such as killing ordinary Muslims and blowing up cars in markets, etc."
- "Working to spread defeatism and despair among members and visitors by exaggerating the capabilities of the enemy"

This unsophisticated text focuses exclusively on the political content of the mimic's verbal statements. By the logic of this analysis, anyone who asks detailed or critical questions is a potential spy.

More interesting is the document that surfaced in late 2010 under the title "10 Methods to Detect and Foil the Plots of Spies" (Anonymous 2010). In the introduction, the author makes explicit reference to a case in the US state of Oregon a few months earlier, in which a young Somali-American was arrested after being drawn into a fictitious terrorist plot staged by a FBI *agent provocateur* on a jihadi forum. The text was widely circulated and remained a sticky post on Ansar al-Mujahideen English forum over a year after its publication, which is much longer than usual. The text mentions the following red flags:

- Small talk ("Once they make contact, the dialogue is typically small. Such topics as translations, finding nasheeds, looking for a husband/wife, or best places for halal food are discussed, simply because they are low key.")
- Bluntness ("talking about Jihad from day one raises red flags")
- Inconsistencies and changes of stories ("Watch for small things which may seem insignificant, such as the mentions of family members, a job, or knowledge of a particular topic")
- Status claims ("These typically include claims to be a member of a [jihadi] organization, or to be in contact with Mujahidin [...] Anyone who makes these claims is either a liar, or [...] extremely [ignorant] when it comes to security").

- Absences ("A spy will typically claim to be busy, most likely with school [...] However, if one really seeks Jihad, and in particular [martyrdom], it is unlikely their primary focus is schooling.")
- Requests for clarification ("For example, if you say you say you are interested in Jihad, they will ask if you mean physical Jihad [...] because if and when you are arrested, they want to make sure a jury will understand what you meant and thus convict you.")
- Tolerance ("Typical behaviours such as smoking, listening to music, or hanging photos are never condemned [...] Spies never appear to get mad at or disagree with their targets")
- Excessive talk and training ("Most operations [...] does not need months upon months of training, but spies will make it appear as though it does [...] there will be numerous dry runs or explosive demonstration.")
- Requests for incriminating favours ("Ask yourself why do they want you to plant the bomb? [...] spies will more than likely ask to train on your property and to use your firearms if you have any.")

Note that all except one of these indicators are verbal cues; the exception being absences. This suggests that extensive online presence (i.e., high time expenditure), is one of the few non-verbal signs available to online trusters.

7.2 Strategies for building trust

Given that jihadi forums have existed for a while, it is fair to assume that activists have sought to mitigate the trust problem in some way. Since we have no primary sources detailing conscious such efforts, I return now briefly to the online trust literature for ideas on what we might expect activists to do, before comparing these expectations with what I observe. This deductive approach will not uncover the full range of strategies used, but it will allow us to confirm whether or not a limited number of expected behaviours occur. Note also that in this section, the distinction between trust in people and confidence in things becomes somewhat blurred, because strategies used to assess the true identity of people overlap with strategies to assess the authenticity of documents.

As noted earlier, Sztompka (1999) suggests that reputation, performance, and appearance are key variables affecting trusting decisions. We should

thus expect activists to do things that convey more and better information about each of these three variables in a given user or group.

At the macro level, we might expect collective measures in the form of technical or organizational systems that facilitate particular information displays. From the literature on trust in commercial exchanges we know of two systemic measures have proved particularly effective in reducing trust problems, namely, "reputation systems" and "vetting agencies". A reputation system preserves and conveys information about the past online behaviour of a given user account (Corritore et al. 2003). Online second-hand trading sites such as Ebay and Amazon use reputation systems with success. A vetting agency is an independent institution that approves products or services on a range of different websites. In regular online commerce, intermediaries such as Visa or Paypal can be effective mechanisms that reduce the costs and risks of personal trusting (Frankel 2009). One could imagine similar systems in the online jihadi world.

At the micro level, we should expect individual trustees to show a preference for displaying particular types of information. From Gambetta (2005) we learned that trusters vet interlocutors by looking for costly signs. While there are fewer sign types in cyberspace that reliably convey that a cost has been incurred, there are at least three types of signs that allows for some cost discrimination. One is time expenditure; spending large amounts of time on a forum is costlier than dropping by every now and then. Another is complex format use; it requires more effort to forge or manipulate a video than a written statement. A third is complex knowledge displays; certain types of insider knowledge are hard to acquire without engaging in activity that is costly in itself.

Based on these reflections, I expect to see at least four strategies: 1) the use of reputation systems, 2) the use of vetting agencies, 3) a preference for complex media formats, and 4) displays of complex knowledge. (The hypothetical emphasis on time expenditure would be confirmed by the existence of reputation systems and is thus not treated separately).

7.2.1 Reputation systems

All the five forums whose design features I examined (Falluja, Shumukh, Ansar al-Mujahidin, Fida, Jihad) had reputation systems integrated into the website architecture. Any message on these forums would be accompanied by a small display of key information about the author's history on the forum. The display typically showed: 1) the number of messages posted by the user, 2) the date of joining, and 3) one or more status titles determined

by some combination of the quantity and quality of the users past messaging. The status title tended to be displayed just below the profile name and be printed in colour (see Figure 3). For example, the 2012 market leader, Shumukh, had an elaborate title system, with one set of titles reflecting the quantity of messages (much like frequent flyer statuses in the airline industry), and other sets reflecting other contributions. Thus a given user would typically carry one of the six following titles:²⁸

- "Limitless member" (*shamikh bila hudud*), reserved for users who have contributed over 6000 messages
- "Gold member" (*shamikh dhahabi*), reserved for users who have contributed 3000-6000 messages
- "Exclusive member" (*shamikh mumayyiz*), reserved for users who have contributed 1000-3000 messages
- "Active member" (*shamikh nashit*), reserved for users who have contributed 500-1000 messages
- "Enthusiastic member" (*shamikh muharriidh*), reserved for users who have contributed 50-500 messages
- "New member" (*shamikh jadid*), reserved for users who have contributed less than 50 messages.

In addition, some users would also carry titles that presumably required attribution by some authority, such as:

- "Administrator" (*idari shabakat shumukh al-islam*, in bright red), presumably reserved for a small number of user with forum administrator rights.
- "Discussion Supervisor" (*majhud mumayyiz fi mutabaat mawadi al-shabaka*, in bold dark red), presumably a type of junior forum administrator.

Moreover, some had titles that may have been self-attributed, such as:

- "Student in the Shumukh Media College" (*talib fi kulliyat shumukh al-islam lil-Ilam*), a more frequent title than that of discussion supervisor; perhaps reserved for aspiring administrators.

²⁸ I reconstructed the message number thresholds by compiling some 100 user profiles and examining the message numbers associated with each status level.

Figure 3: Screenshot of message from user nicknamed "al-jundi al-majhul" (The Unknown Soldier) on the Shumukh forum, 5 February 2012. The signature is on the top right and the past message count (724) on the top left. The signature includes the titles "Active member" and "Student in the Shumukh Media College".

- "Your Sister in God" (*ukhtkum fillah*), title accompanying most users with female names.

7.2.2 Vetting agencies

An interesting feature of the online jihadi propaganda system is the existence of entities referred to in the literature as "distribution companies" (Kimmage 2008; Lia 2005). These entities are effectively vetting agencies that serve as intermediaries between groups in the field and the online forums. They receive original productions from established militant groups or ideologues, verify the documents before distributing them in the forums branded by their own logos (see Figure 4; see also Figure 1, upper right hand side). Much like record companies, each distribution company appears to maintain a portfolio of groups to whose publications it has exclusive rights. Distribution companies may occasionally distribute amateur productions by unknown "artists". In 2012 the most prominent distribution companies were al-Fajr Media and the Global Islamic Media Front, but there were several others.

Distribution companies are one of two key components the propaganda distribution chain, the other being the production companies, which are responsible for the propaganda production of individual groups. Together these make up the category Daniel Kimmage calls "MPDEs" — Media pro-

Figure 4: Sample logos of jihadi distribution and production companies, February 2012

duction and distribution entities — which, he argues, systematically brand jihadi media. A US intelligence official told Schmitt and Shanker (2011) that “all Al Qaeda products appear to go through a chain of preparation and approval. [...] its a complex system of validation. This makes messages posted on these sites official.” Kimmage also suggests that the current distribution system was inspired by a jihadi policy paper written in 2006 by an anonymous strategist who recommended branding as a solution to the problem of information saturation (or media exuberance) on the forums (Kimmage 2008). The policy paper does not explicitly mention trust concerns as a motivation, but the system likely increases confidence in those propaganda products that have been branded or vetted by the right agencies. It is not clear what effect, if any, these vetting agencies have on interpersonal trust on the forums, other than lending credibility to the individuals working directly for the agencies. It is worth noting that due diligence agencies specializing in the vetting of new collaborators, common in the business world, have yet to emerge on the forums.

7.2.3 Using hard-to-fake formats

While all digital messages can be manipulated, it is somewhat harder to forge documents in “higher-bandwidth” formats such as audio or video than it is to forge a typed text. For example, in the early 2000s, when people wondered whether Usama Bin Ladin was alive, the appearance of a video statement featuring the al-Qaida leader was considered more reliable evidence than a written statement signed in his name.

Over the past ten years, there has been a dramatic increase in the quantity and sophistication of audiovisual propaganda circulating on the forums. Although hard to measure, the proportion of audiovisual documents relative to the overall propaganda production also seems to have increased. The

growth in video production seems at least partly driven by trust concerns. To be sure, some of the increase observed in recent years may be caused by other factors, such as the expectation that visual messaging has a higher emotional impact on prospective recruits. However, large-n studies of jihadi video content indicate that most jihadi videos are not recruitment films, but short clips documenting individual attacks (Finsnes 2010). The purpose of these clips appears to be to attract funding from sympathizers abroad by demonstrating effectiveness. In this genre, credibility is presumably a more important attribute than emotional impact.

Anecdotal evidence also suggests that activists prefer complex formats when they make particularly risky trusting decisions or when they need to persuade highly sceptical interlocutors. For example, in the few known cases where representatives of militant groups have met "live" (i.e., in real time) with anonymous recruits online, the meetings took place on the audio chat program Paltalk and not on the forums. Similarly, when the Yemeni-American jihadist ideologue Anwar al-Awlaki needed to convince his followers in late 2009 that he had survived a widely publicized US drone attack in Yemen, he chose to record an audio message and send it by attachment to supporters with whom he had until then communicated primarily by encrypted email (Swann 2011).

7.2.4 Displaying hard-to-earn knowledge

The forums are replete with displays of hard-to-acquire knowledge, most of which is either technical or cultural. It is not surprising, of course, that jihadi forums contain manuals on explosives production, advice on countersurveillance, and the like. Many forums have devoted special sections to these types of topics. Users who combine displays of high technical expertise with lengthy online presence appear to gain in status and perceived trustworthiness. Irhabi007, for example, became so respected as a tech whiz in the online community that real-life operatives such as Mirsad Bektasevic (head of a terror cell arrested in Bosnia in 2006) and Abu Maysara al-Iraqi (a senior media official of al-Qaida in Iraq) trusted him enough to engage in bilateral email correspondence.

More unexpected is the extent to which forum participants seem to care about poetry, religious hymns (anashid) and other elements of what we may call "jihad culture" (Hegghammer 2013). Several forums have special sections devoted to such products, which is surprising given their limited military utility. There may be several reasons for this phenomenon, one of which is that cultural knowledge is considered a proxy for time spent in the

underground. It is worth noting that several of the most senior figures in the Shumukh reputation hierarchy, such as the forum administrator Abu Dharr al-Makki, include poetry in their signatures.²⁹

Displays of hard-to-earn knowledge seem to be valued more than simple declarations of extreme intent. Just as the author of 10 Methods dismissed bluntness as a red flag, many forum users seem unimpressed by radical talk, presumably because it is cheap. Of course, what counts as sorting knowledge probably changes over time as frequent exposure turns rare knowledge into common knowledge. A written poem, for example, can easily be copied and pasted, so the recital of an old classic will likely not instil trust.

8 Conclusion

This chapter probed the effects of the trust problem on radical Islamist discussion forums, a supposed recruiting ground for al-Qaida and related groups. I presented tentative data indicating that forums rarely mediate sensitive transactions such as direct recruitment because of the trust deficit. The social atmosphere on jihadi forums is characterised by distrust and paranoia: users withhold personal information, warn against intelligence agents, accuse each other of spying, and share advice on how to spot impostors. Moreover, interpersonal trust seems to have declined over time, from low levels in the mid-2000s to very low levels in the early 2010s, most likely as a result of increased government infiltration.

Interestingly, however, jihadi forums continue to attract thousands of users. One reason for their survival is probably that propaganda consumption and the expression of radical views are generally not criminalized and therefore constitute relatively low-risk activities. Another reason is that user confidence in the authenticity of propaganda products remains high, due in part to the emergence of jihadi vetting institutions and the growing availability of hard-to-fake video formats. A modicum of interpersonal trust also remains on the forums, thanks to reputation systems and the existence of a few relatively reliable signs such as spending much time online and displaying complex knowledge.

The chapter contributes to the literatures on terrorism, civil war, and social movements by highlighting an important limit to the Internet's usefulness for high-risk activists. Although the inquiry was narrow in its empirical scope, it identified a problem that likely plagues all contentious activists

²⁹ <http://www.shamikh1.info/vb/showthread.php?t=137267> (accessed 25 November 2011).

online to a greater or lesser extent. This idea is not new — Diani (2000) suggested early that ”engaging in high-risk activities requires a level of trust [...] which is unlikely to develop if not supported by face-to-face interaction” — but we now have empirics to support Diani’s prediction.

The study also contributes to the trust and signalling literature by offering a partial answer to the question of what constitutes a costly sign in cyberspace. *Time* is one currency in which digital signal cost can be differentiated. Time translates into signs in at least three different ways: aggregation (total time spent in activism), relative expenditure (time spent on the forums as a proportion of time available in a given period) and skill acquisition (time spent learning). From this I propose a tentative taxonomy of time-related virtual signs, consisting of historical signs, presence signs, and knowledge signs. Historical signs are things that show a person has been in the game for a long time. Presence signs show that a person is able to maintain a continuous or at least frequent presence on the forums over a certain period. Knowledge signs are displays of hard-to-earn knowledge. Future research may help evaluate this hypothetical categorization.

To be sure, this study has only scratched the surface of the topic of trust among high-risk activists online. More research is needed, especially on trust on other digital platforms and among other types of political activists online. It would be interesting to see, for example, whether low-bandwidth media such as Twitter see less interpersonal trust between jihadis than higher-bandwidth media such as Paltalk. Another question is whether platforms with different interface constraints (such as the ability, on Facebook, to see other users’ ”friends”) produce different trust dynamics or distrust mitigation strategies. Similarly, by studying forums for other types of militants, we might be able to observe how trust dynamics play out under different levels of repression, or to what extent ideological-cultural specificities affect signalling knowledge. So far, existing studies on non-jihadi forums such as the far-right *Stormfront* (Bowman-Grieve 2012) and dissident Irish republican websites (Bowman-Grieve and Conway 2012) do report symptoms of trust problems, but not on the scale documented in this chapter.

My findings have at least two policy implications. Most important is that undermining trust through deceptive mimicry may be one of the most efficient repressive strategies against terrorists online. Closing down websites is complicated, and monitoring all communications is resource-intensive, but distrust can be sown with relatively simple means. Small events — such as a well-publicised agent provocateur operation — can have a large impact on trust, because activists, like everyone else, are prone to the availability error, whereby a danger seems larger if it recently materialized near you.

Moreover, it takes much longer to build trust than to break it. Indeed, governments appear to have largely succeeded in causing a breakdown of interpersonal trust on jihadi discussion forums. Given the recent expansion of jihadi activity on Facebook and Twitter, governments should consider pursuing a more aggressive infiltration strategy against these platforms in order to prevent interpersonal trust levels from rising to levels where they allow recruitment and operational coordination.

A second, less intuitive implication is that Western counterterrorism specialists and experts of so-called liberation technologies have things to learn from one another, because the tactics that we use against al-Qaida online can also be used by dictators against pro-democracy activists. If Western counterterrorism and liberation technology communities share their latest insights on trust dynamics, both may enjoy at least a temporary advantage against their respective opponents.

Finally, a caveat: these findings should not be taken to mean that the Internet is inherently useless for terrorist recruitment, fundraising or operational coordination. The paranoia we now see on jihadi forums is most likely a fragile equilibrium, one that is sensitive to changes in repression levels and developments in stealth technology. If jihadi websites are left alone, or if activists discover a powerful new encryption tool, militants will be quick to exploit the Web for what it is worth.

9 References

- Abu Jarir. 2009. "al-mu'arrifat al-mashbuha fi'l-muntadayat wa'l-shabakat al-jihadiyya." Ansar al-Mujahidin (<http://www.as-ansar.com/vb/showthread.php?p=22750#post22750>) [Accessed 21 November 2011], 11 August.
- AIVD. 2012. "Jihadism on the web: A breeding ground for jihad in the modern age." The Hague: General Intelligence and Security Service.
- al-Jihad, Sayf. 2010. "al-ta'amul ma' al-jawasis [Dealing with Spies]." al-Falluja (<http://202.71.102.68/alfalof/vb/showthread.php?t=100961>) [accessed 2 February 2010], 26 January.
- al-Maqdisi, Abu al-Nur. 2009. "hukm al-jasus fil-islam [Ruling on the Spy in Islam]."
- Amble, John Curtis. 2012. "Combating Terrorism in the New Media Environment." *Studies in Conflict and Terrorism* 35 (5):339-353.
- Anderson, D. Scott. 2006. "What Trust Is in these Times? Examining the Foundations of Online Trust." *Emory Law Review* 54:1441-74.
- Anonymous. 2010. "10 Methods To Detect And Foil The Plots Of Spies." Ansar al-Mujaheen (<http://ansar1.info/showthread.php?t=29715>) [accessed 21 November 2011].
- Arquilla, John, and David Ronfeldt, eds. 2001. *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica, CA: RAND.
- Awan, Akil N., Andrew Hoskins, and Ben O'Loughlin. 2011. *Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology*. London: Routledge.
- Bacharach, Michael, and Diego Gambetta. 2001. "Trust in Signs." In *Trust and Society*, ed. K. S. Cook. New York: Russell Sage Foundation.
- Bailenson, Jeremy N., and Andrew Beall. 2006. "Transformed Social Interaction: Exploring the Digital Plasticity of Avatars." In *Avatars at Work and Play: Collaboration and Interaction in Shared Virtual Environments*, ed. R. Schroeder and A.-S. Axelsson: Springer.

Bergin, Anthony, Sulastri Bte Osman, Carl Ungerer, and Nur Azlin Muhammed Yasin. 2009. "Countering Internet Radicalisation in Southeast Asia." In ASPI Special Report no. 22. Canberra: Australian Strategic Policy Institute.

Biyokulule. 2009. "Forum Member Warns Pal Talk Program is 'Spying' Tool Against Mujahidin." Biyokulule.com [http://www.biyokulule.com/view_content.php?articleid=2521], 3 April.

Borum, Randy. 2010. *The Science of Interpersonal Trust*. McLean, VA: Mitre Corporation.

Bos, Nathan, Judy Olson, Darren Gergle, Gary Olson, and Zach Wright. 2002. "Effects of Four Computer-Mediated Communications Channels on Trust Development." In *Proceedings of Conference on Human Factors in Computer Systems (CHI)*, ed. CHI. Minneapolis, MN: ACM Press.

Bowman-Grieve, Lorraine. 2012. "Exploring Stormfront: A Virtual Community of the Radical Right." *Studies in Conflict and Terrorism* 32 (11):989-1007.

Bowman-Grieve, Lorraine, and Maura Conway. 2012. "Exploring the form and function of dissident Irish Republican online discourses." *Media, War, and Conflict* 5 (1):71-85.

Brachman, Jarret. 2006. "High-Tech Terror: Al-Qaedas Use of New Technology." *Fletcher Forum of World Affairs* 30 (2):149-64.

Bunt, Gary. 2009. *iMuslims: Rewiring the House of Islam*. London: Hurst & Co.

Bunt, Gary R. 2003. *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments*. London: Pluto Press.

Castells, Manuel. 2004. *The Power of Identity*. second ed. Vol. 2. Oxford: Blackwell.

Conway, Maura. 2006a. "Terrorism and the Internet: New MediaNew Threat?" *Parliamentary Affairs* 59 (2):283-98.

—. 2006b. "Terrorist 'use' of the Internet and fighting back." *Information and Security* 19:9-30.

—. 2007. "Terrorism and Internet governance: core issues." *Disarmament Forum* (3):23-33.

Cornwell, B., and D.C. Lundgren. 2001. "Love on the Internet: involvement and misrepresentation in romantic relationships in cyberspace vs. realspace." *Computers in Human Behavior* 17:197-211.

Corritore, Cynthia L., Beverly Kracher, and Susan Wiedenbeck. 2003. "Online trust: concepts, evolving themes, a model." *International Journal of Human-Computer Studies* 58:737-58.

Denning, Dorothy. 2009. "Terror's Web: How the Internet Is Transforming Terrorism." In *Handbook on Internet Crime*, ed. Y. Jewkes and M. Yar. London: Willan.

Diani, Mario. 2000. "Social Movement Networks Virtual and Real." *Information, Communication and Society* 3 (3):386-401.

Donath, Judith. 1998. "Identity and deception in the virtual community." In *Communities in Cyberspace*, ed. P. Kollock and M. Smith. London: Routledge.

—. 2007. "Signals in social supernets." *Journal of Computer-Mediated Communication* 13 (1):article 12.

Drennan, Shane, and Andrew Black. 2007. "Jihad Online: The Changing Role of the Internet." *Jane's Intelligence Review* 18 (8):16-20.

Feng, Jinjuan, Jonathan Lazar, and Jenny Preece. 2004. "Empathy and online interpersonal trust: A fragile relationship." *Behaviour and Information Technology* 23 (2):97-106.

Finsnes, C. 2010. "What is audio-visual jihadi propaganda? An overview of the content of FFI's jihadi video database." Kjeller: FFI.

Fox, S. 2000. "Trust and Privacy Online: Why Americans Want to Rewrite the Rules." In *The Pew Internet & American Life Project*. Washington,

DC: Pew.

Frankel, Tamar. 2001. "Trusting and non-trusting on the Internet." *Boston University Law Review* 457.

—. 2009. "Trust and the Internet." In *Aba Guide to International Business Negotiations*, ed. J. R. Silkenat, J. M. Aresty and J. Klosek.

Friedman, Batya, and Peter H. Kahn Jr. 2000. "Trust Online." *Communications of the ACM* 43 (12):34-40.

Galanxhi, Holtjona, and Fiona Fui-Hoon Nah. 2007. "Deception in cyberspace: A comparison of text-only vs. avatar-supported medium." *International Journal of Human-Computer Studies* 65:770-83.

Gambetta, Diego. 2005. "Deceptive mimicry in humans." In *Perspectives on Imitation: From Neuroscience to Social Science*, ed. S. Hurley and N. Chater. Cambridge, MA: MIT Press.

Gardham, Duncan. 2011. "MI6 attacks al-Qaeda in 'Operation Cupcake'." *Daily Telegraph* (online), 2 June.

Grazioli, Stefano, and Sirkka L. Jarvenpaa. 2000. "Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers." *IEEE Transactions On Systems, Man, And Cybernetics* 30 (4):395-410.

Green, Melanie C. 2007. "Trust and social interaction on the Internet." In *The Oxford handbook of Internet psychology*, ed. A. Joinson, K. McKenna, T. Postmes and U.-D. Reips. Oxford: Oxford University Press.

Hancock, Jeffrey T. 2007. "Digital deception: why, when and how people lie online." In *The Oxford handbook of Internet psychology*, ed. A. Joinson, K.

McKenna, T. Postmes and U.-D. Reips. Oxford: Oxford University Press.

Hegghammer, Thomas. 2013. "The recruiter's dilemma: Signalling and rebel recruitment tactics." *Journal of Peace Research* 50 (1):3-16.

Hoffman, Bruce. 2006. "The Use of the Internet By Islamic Extremists." In *Testimony presented to the House Permanent Select Committee on Intelli-*

gence. Washington, DC: RAND.

Human Rights Watch. 2005. "Black Hole: The Fate of Islamists Rendered to Egypt."

ICT. 2012. "In the Depths of Jihadist Web Forums: Understanding a Key Component of the Propaganda of Jihad." In *Insights*. Herzlia: ICT Jihadi Websites Monitoring Group.

Kenney, Michael. 2010. "Beyond the Internet: Metis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists." *Terrorism and Political Violence* 22 (2):177-97.

Kimmage, Daniel. 2008. "The al-Qaeda Media Nexus: The Virtual Network behind the Global Message." In *RFE/RL Special Report*. Washington, DC: Radio Free Europe/Radio Liberty.

Kling, Rob. 1996. "Social Relationships in Electronic Forums: Hangouts, Salons, Workplaces, and communities." In *Computerization and Controversy: Value Conflicts and Social Choices*, ed. R. Kling. San Diego, CA: Academic Press.

Koehn, Daryl. 2003. "The Nature and Conditions for Online Trust." *Journal of Business Ethics* 43 (1-2):3-19.

Kohlmann, Evan. 2008. "Al-Qaida's Myspace: Terrorist Recruitment on the Internet." *CTC Sentinel* 1 (2):8-9.

Labi, Nadya. 2006. "Jihad 2.0." *The Atlantic* (online).

Lappin, Yaakov. 2011. *Virtual Caliphate: Exposing the Islamist State on the Internet*. Dulles, VA: Potomac.

Lea, M., and R. Spears. 1995. "Love at first byte? Building personal relationships over computer networks." In *Understudied relationships: Off the beaten track*, ed. J. T. Wood and S. Dick. Newbury Park, CA: Sage.

Lia, Brynjar. 2005. "Al-Qaeda Online: Understanding Jihadist Internet Infrastructure." *Jane's Intelligence Review* 17 (12).

Lusthaus, Jonathan. 2012. "Trust in the world of cybercrime." *Global Crime* 13 (2):71-94.

Mantel, Barbara. 2009. "Terrorism and the Internet: should Web sites that promote terrorism be shut down?" *CQ Global Researcher* 3 (11):129-53.

Marx, Gary. 1974. "Thoughts on a Neglected Category of Social Movement Participant: The Agent Provocateur and the Informant." *American Journal of Sociology* 80 (2):402-42

Marx, Gary. 2012. "Agents Provocateurs as a Type of Faux Activist." In *Encyclopedia of Social and Political Movements*, eds. D. Snow, D. Della Porta, B. Klandermans, and D. McAdam. Hoboken, NJ: Blackwell.

MEMRI. 2010. "Tension, Suspicion Among Jihadi Websites Following Infiltration, Collapse of Several Sites." *Memri Inquiry and Analysis* (625).

Misztal, Barbara. 1996. *Trust in Modern Societies: The Search for the Bases of Social Order*. New York: Polity.

Moubayed, Sami. 2006. "Syria's Abu al-Qaqa: Authentic Jihadist or Imposter?" *Jamestown Terrorism Focus* 3 (25).

Musawi, Mohammed Ali. 2010. "Cheering for Osama: How Jihadists use Internet Discussion Forums." London: Quilliam Foundation.

Myers, D. 1987. "'Anonymity is part of the magic': Individual manipulation of computer-mediated communication contexts." *Qualitative Sociology* 10:251-66.

Nacos, Brigitte L. 2002. *Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Counter-Terrorism*. Maryland: Rowman & Littlefield.

Nakashima, Ellen. 2010. "Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies." *Washington Post*, 19 March.

Nakashima, Ellen, and Joby Warrick. 2012. "Al-Qaedas online forums go dark for extended period." *Washington Post*, 2 April.

- Naquin, Charles E., and Gaylen D. Paulson. 2003. "Online bargaining and interpersonal trust." *Journal of Applied Psychology* 88:113-20.
- Newsweek. 2000. "Tracking Bin Ladens E-mail." *Newsweek*, 21 August.
- Nissenbaum, Helen. 2001. "Securing Trust Online: Wisdom or Oxymoron." *Boston University Law Review* 81 (3):635-64.
- Parks, Malcolm R., and Kory Floyd. 1996. "Making friends in cyberspace." *Journal of Computer-Mediated Communication* 1 (4):80-97.
- Policy Planners' Network. 2011. "Radicalisation: The Role of the Internet." London: Institute for Strategic Dialogue
- Ranstorp, Magnus. 2004. "Al-Qaida in Cyberspace: Future Challenges of Terrorism in the Information Age." In *Terrorism in the Information Age - New Frontiers*, ed. L. Nicander and M. Ranstorp. Stockholm: Swedish National Defence College.
- . 2007. "The virtual sanctuary of al-Qaida and terrorism in an age of globalization." In *International Relations and Security in the Digital Age*, ed. J. Eriksson and G. Giacomello. London: Routledge.
- Rawnsley, Adam. 2010. "Taliban Webmaster: Weve Been Hacked!" *Wired.com*, 10 June.
- . 2011. "'Spyware' incident spooks jihadi forums." *Wired.com*, 1 September.
- Renieris, Elizabeth. 2009. "Combating Incitement to Terrorism on the Internet: Comparative Approaches in the United States and United Kingdom and the Need for an International Solution." *Vanderbilt Journal of Entertainment and Technology Law* 11 (3):673-709.
- Rocco, Elena. 1998. "Trust Breaks Down in Electronic Contexts but Can Be Repaired by Some Initial Face-to-Face Contact " In *CHI 98: Proceedings of the SIGCHI conference on Human factors in computing systems*. Los Angeles, CA: ACM Press.

Rogan, Hanna. 2006. "Jihadism Online - A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes." Kjeller: FFI.

—. 2007. "Al-Qaeda's online media strategies: From Abu Reuter to Irhabi 007." Kjeller: FFI.

Rossmiller, Shannen. 2007. "My Cyber Counter-Jihad." *Middle East Quarterly* 14 (3):43-8.

Ryan, Thomas. 2010. "Getting in Bed with Robin Sage." *Black Hat Briefings and Training* (<http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf>).

Sageman, Marc. 2004. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

Schmitt, Eric, and Thom Shanker. 2011. *Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda*. New York: Times Books.

Seib, Philip. 2008. "The Al-Qaeda Media Machine." *Military Review* 88 (3):74-80.

Seib, Philip, and Dana M. Janbek. 2011. *Global terrorism and new media: the post-Al Qaeda generation*. London: Routledge.

Shahar, Yael. 2007. "The Internet as a Tool for Intelligence and Counter-Terrorism." In *Hypermedia Seduction for Terrorist Recruiting*, ed. B. Ganor, K. Von Knop and C. A. M. Duarte. Amsterdam: IOS Press.

Torres-Soriano, Manuel R. 2012. "The Vulnerabilities of Online Terrorism." *Studies in Conflict and Terrorism* 35 (4):263-77.

Swann, Steve. 2011. "Rajib Karim: The terrorist inside British Airways." *BBC News Online*, 28 February.

Sztompka, Piotr. 1999. *Trust: A Sociological Theory*. Cambridge: Cambridge University Press.

Talbot, David. 2005. "Terror's Server: How radical Islamists use internet fraud to finance terrorism and exploit the internet for Jihad propaganda and

recruitment." *TechnologyReview.com*, 27 January.

Tarrow, Sidney. 2006. *The New Transnational Activism*. Cambridge: Cambridge University Press.

Theohary, Catherine A., and John Rollins. 2011. "Terrorist Use of the Internet: Information Operations in Cyberspace." In CRS Report for Congress. Washington DC: Congressional Research Service.

Thomas, Timothy L. 2003. "Al Qaeda and the Internet: The Danger of Cyberplanning." *Parameters* 33 (1):112-23.

Tønnessen, Truls H. 2011. Paper presented at the FFI seminar on "Terrorist uses of the Internet", Oslo, 29 November.

Ulph, Stephen. 2004. "Forum Warnings of a Spy Website." *Jamestown Terrorism Focus* 1 (9).

—. 2006a. "Fears of Intelligence Penetration of the GIMF." *Jamestown Terrorism Focus* 3 (16).

—. 2006b. "Intelligence War Breaks out on the Jihadi Forums." *Jamestown Terrorism Focus* 3 (14).

—. 2006c. "Mujahideen Explain Away Failures of the Abqaiq Attack." *Jamestown Terrorism Focus* 3 (9).

Van Gelder, Lindsay. 1985. "The strange case of the electronic lover." *Ms* 14 (4):94-124.

Van Laer, Jeroen, and Peter Van Aelst. 2013. "Cyber-protest and civil society: The Internet and action repertoires in social movements." In *Handbook of Internet Crime*, ed. Y. Jewkes and M. Yar. London: Routledge.

Vijayan, Jaikumar. 2008. "Updated encryption tool for al-Qaeda backers improves on first version, researcher says." *www.computerworld.com*, 4 February.

Wang, Ye D., and Henry H. Emurian. 2005. "An overview of online trust: Concepts, elements, and implications." *Computers in Human Be-*

havior 21:105-25.

Warrick, JOby. 2011. *The Triple Agent: The al-Qaeda Mole who Infiltrated the CIA*. New York: Doubleday.

Weimann, Gabriel. 2006. *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: United States Institute of Peace.

—. 2007. "Using the Internet for Terrorist Recruitment and Mobilization." In *Hypermedia Seduction for Terrorist Recruiting*, ed. B. Ganor, K. Von Knop and C. A. M. Duarte. Amsterdam: IOS.

Weisburd, Aaron. 2004. "Poor 007." *Internet-Haganah.com*, 28 January.

—. 2006a. "al-Hesbah posts fake 'suspended site' message." *Internet-Haganah.com*, 18 March.

—. 2006b. "Irhabi007 as a case-study in jihadi counter-intelligence efforts." *Internet-Haganah.com*, 11 March.

—. 2007. "The shifting sands of the global jihad online." In *Hypermedia seduction for terrorist recruiting*, ed. B. Ganor, K. Von Knop and C. A. M. Duarte. Amsterdam: IOS Press.

Williams, M. 2001. "A Living Dream." *Wall Street Journal*, 24 September.

Zanini, Michelle, and Sean J. A. Edwards. 2001. "The Networking of Terrorism in the Information Age." In *Networks and Netwars: The Future of Terror, Crime and Militancy*, ed. J. Arquilla and D. Ronfeld. Santa Monica, CA: RAND.

Zelin, Aaron Y. 2013. "The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis." Washington, D.C.: New America Foundation.