Studies in Conflict & Terrorism
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uter20

Applying the Notion of Noise to Countering Online Terrorism

Gabriel Weimann [a] & Katharina Von Knop [b]
[a] University of Haifa, Haifa, Israel
[b] Bundeswehr University Munich, Neubiberg, Germany
Published online: 13 Oct 2008.

To cite this article: Gabriel Weimann & Katharina Von Knop (2008): Applying the Notion of Noise to Countering Online Terrorism, Studies in Conflict & Terrorism, 31:10, 883-902

To link to this article: http://dx.doi.org/10.1080/10576100802342601

Studies in Conflict & Terrorism, 31:883–902, 2008

ISSN: 1057-610X print / 1521-0731 online
DOI: 10.1080/10576100802342601

Routledge
Taylor & Francis Group

Applying the Notion of Noise to Countering Online Terrorism

GABRIEL WEIMANN
University of Haifa
Haifa, Israel

KATHARINA VON KNOP
Bundeswehr University Munich
Neubiberg, Germany

The growing presence of modern terrorism on the Internet is at the nexus of two key trends: the democratization of communications driven by user-generated content on the Internet; and the growing awareness of modern terrorists of the potential of the Internet for their purposes. How best can the terrorists' use and abuse of the Internet be countered? As this article argues, the answer to violent radicalization on the Internet lies not in censorship of the Internet, but in a more sophisticated and complicated strategy, relying on the theoretical notion of "noise" in communication process theory.

Terrorism as a Communication

During the recent decades the world has witnessed the emergence and proliferation of media-wise terrorism. Modern terrorists have become exposed to new opportunities for exerting mass psychological impacts as a result of technological advances in communications. The emergence of mass-mediated terrorism led several communication and terrorism scholars to re-conceptualize modern terrorism within the framework of symbolic communication theory. As Jenkins concluded in his analysis of international terrorism: "Terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press. Terrorism is aimed at the people watching, not at the actual victims. Terrorism is a theater."[1] Indeed, modern terrorism can be understood in terms of the production requirements of theatrical engagements.[2] Terrorists pay attention to script preparation, cast selection, sets, props, role playing, and minute-by-minute stage management. Just like compelling stage plays or ballet performances, the media orientation in terrorism requires full attention to detail in order to be effective. The growing importance attributed to publicity and mass media by terrorist organizations was revealed both in the diffusion of media-oriented terrorism as well as in the tactics of modern terrorists who have become more media-minded. Nacos noted that since the first World Trade Center bombing in 1993 and the Oklahoma City bombing in 1995, the world has entered into a

Received 20 October 2007; accepted 7 February 2008.

The authors are listed alaphabetically by first name; both authors contributed equally.

The authors thank Bruce Hoffman and Joshua Sinai for their helpful comments on earlier versions of this article.

Address correspondence to Gabriel Weimann, Department of Communication, University of Haifa, Haifa 31905, Israel. E-mail: weimann@soc.haifa.ac.il

new age of megaterrorism, and the new age of terrorism is a more powerfully media-oriented production than ever before.[3]

The most powerful and violent performance of the modern "Theater of Terror" was the 11 September 2001 (9/11) attack on American targets. In November 2001, shortly after the 9/11 attacks, Osama bin Laden discussed the twin attacks. Referring to the suicide terrorists whom he called "vanguards of Islam," bin Laden marveled, "Those young men said in deeds, in New York and Washington, speeches that overshadowed other speeches made everywhere else in the world. The speeches are understood by both Arabs and non-Arabs, even Chinese."[4] From the "Theater of Terror" perspective, the 11 September attack on America was a perfectly choreographed production aimed at American and international audiences. Although the theater metaphor remains instructive, it has given way to that of terrorism as a global television spectacular with "live" breaking news, watched by international audiences, and transcends by far the boundaries of theatrical events. In the past most, if not all, acts of terrorism resulted in a great deal of publicity in the form of news reporting, but the 11 September attack introduced a new level of mass-mediated terrorism because of the choices the planners made with respect to method, target, timing, and scope.

The growing use and manipulation of modern communications by terrorist organizations led governments and several media organizations to consider certain steps in response. These included limiting terrorists' access to the conventional mass media, reducing and censoring news coverage of terrorist acts and their perpetrators and minimizing the terrorists' capacity for manipulating the media. However, the new media technologies and especially computer-mediated communication and the Internet allow terrorist organizations to transmit messages more easily and freely than through other means of communication. Terrorist groups and organizations have identified the Internet has an important communication platform. This global and cheap communication tool allows them to enhance their communication strategy.

The Advantages of the Internet for Modern Terrorism

The network of computer-mediated communication (CMC) is ideal for terrorists-as-communicators: it is decentralized, it cannot be subjected to control or restriction, it is not censored, and it allows access to anyone who wants it. The loosely knit network of cells and divisions and subgroups, typical to modern terrorists all make the Internet an ideal and necessary tool for inter-group and intra-group networking. Al Qaeda, for example, has shown itself to be a remarkably nimble, flexible, and adaptive entity, mainly due to its decentralized structure.[5] The rise of networked terrorist groups is part of a broader shift to what Arquilla and Ronfeldt have called "netwar."[6] Netwar refers to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war in which the protagonists are likely to consist of small, dispersed groups who communicate, coordinate, and conduct their campaigns in an "internetted" manner and without a precise central command. Al Qaeda operatives now are urging their members to use caution on the Internet. Just before their first official website, alneda.com, was pulled off its server, it warned its members that the FBI, CIA, and Customs Service were probably monitoring the site. It promised to e-mail members the new address of the website once it was in operation. It also told them they could find the address in chat rooms on other terror sites, such as Hamas's qassam.net. "We strongly urge Muslim Internet professionals to spread and disseminate news and information about the jihad through e-mail lists, discussion groups and their own Web sites," says a statement on azzam.com. "The more Web sites, the better it is for us. We must make the Internet our tool."[7]

Websites are only one of the Internet's services used by modern terrorism; there are many other facilities in the Net—e-mail, chat rooms, e-groups, forums, virtual message boards, YouTube, Google Earth—that are used more and more by terrorists. Thus, for example, Yahoo! has become one of Al Qaeda's most significant ideological bases of operation. They utilize several facets of the Yahoo! service, including chat functions, e-mail, and, most importantly, Yahoo! Groups. Yahoo! Groups are electronic groups (e-groups) dedicated to a specific topic whereby members of the group can discuss the topic, post relevant articles and multimedia files, and share a meeting place for those with similar interests. Creating a Yahoo! Group is free, quick and extremely easy, and several terrorist groups have used Yahoo! Groups to communicate with their supporters, to post the latest links to other terrorist websites and to post communiqués to the public.[8]

The great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, fast flow of information, and so forth—have been converted into the advantage of groups committed to terrorizing societies to achieve their goals. The anonymity offered by the Internet is very attractive for modern terrorists.[9] Due to their extremist beliefs and values, terrorists require anonymity to exist and operate in social environments that may not agree with their particular ideology or activities. The Internet provides this anonymity as well as easy access from everywhere with the option to post messages, to e-mail, to upload or download information—and to disappear into the dark.

These advantages have not gone unnoticed by terrorist organizations, no matter what their political orientation. Islamists and Marxists, nationalists and separatists, fundamentalists and extremists, racists and anarchists: all find the Internet alluring. Today, all active terrorist organizations maintain websites, and many maintain more than one website and use several different languages. As the following illustrative list shows, these organizations and groups come from all corners of the globe:

- *From the Middle East,* Hamas (the Islamic Resistance Movement), the Lebanese Hezbollah (Party of God), the Al Aqsa Martyrs Brigades, Fatah Tanzim, the Popular Front for the Liberation of Palestine (PLFP), the Palestinian Islamic Jihad, the Kahane Lives movement, the People's Mujahedin of Iran (PMOI—Mujahedin-e Khalq), the Kurdish Workers' Party (PKK); the Turkish-based Popular Democratic Liberation Front Party (DHKP/C), and the Great East Islamic Raiders Front (IBDA-C), which is also based in Turkey.
- *From Europe*, the Basque ETA movement, Armata Corsa (the Corsican Army), and the Real Irish Republican Army (RIRA).
- *From Latin America,* Peru's Tupak-Amaru (MRTA) and Shining Path (Sendero Luminoso), the Colombian National Liberation Army (ELN-Colombia), and the Armed Revolutionary Forces of Colombia (FARC).
- *From Asia,* Al Qaeda, the Japanese Supreme Truth (Aum Shinrikyo), Ansar al Islam (Supporters of Islam) in Iraq, the Japanese Red Army (JRA), Hizb-ul Mujehideen in Kashmir, the Liberation Tigers of Tamil Eelam (LTTE), the Islamic Movement of Uzbekistan (IMU), Moro Islamic Liberation Front (MILF) in the Philippines, the Pakistan-based Lashkar-e-Taiba, and the rebel movement in Chechnya.

Terrorists' Uses of the Internet

Today, all terrorist organizations, large or small, have their own websites.[10] They use this medium to spread propaganda, raise funds and launder money, recruit and train members,

communicate and conspire, and launch attacks while governments are trying to counter and catch them using traditional means.[11]

Terrorism and the Internet are related in several ways. First, the Internet has become a forum for terrorist groups and individual terrorists both to spread their messages of hate and violence and to communicate with one another and with sympathizers. Secondly, individuals and groups may attack computer networks, including those on the Internet, what has become known as cyberterrorism or cyberwarfare. At this point, terrorists are using the Internet for propaganda and communication more than they are attacking it. Former FBI's Associate Director for Counterterrorism Buck Revell told *U.S. News and World Report* that "As long as they don't specifically engage in criminal acts, they can do anything they want to aid and abet their activities. This is a safe haven for them."[12]

The use of the Internet by modern terrorists is well-related to the conceptualization of terrorism as a psychological warfare. Cyber-fear, argues Thomas, is generated by the fact that what a computer attack *could* do (bring down airliners, ruin critical infrastructure, destroy the stock market, reveal State secrets, etc.) is too often associated with what *will* happen.[13] It is clear that the Internet empowers small groups and makes them appear much more capable than they might actually be, even turning bluster into a type of virtual fear. The Net allows terrorists to amplify the consequences of their activities with follow-on messages and threats directly to the population at large, even though the terrorist group may be totally impotent. In effect, the Internet allows a person or group to appear to be larger or more important or threatening than they really are. The Internet can be used to spread disinformation, frightening personal messages, or horrific images of recent activities (one is reminded of the use of the Net to replay the murder of the Jewish-American reporter Daniel Pearl by his Pakistani captors). There are numerous ways terrorists use the Net.[14] The most frequent are:

Psychological Warfare. The Internet is used to deliver threats and disseminate multimedia content designed to create fear and panic, as seen in Iraq. Nearly all insurgent groups in Iraq have media teams that post statements and create videos and Web broadcasts.

Online Indoctrination. The Internet became an instrument for radicalization and indoctrination by modern terrorists. Many of the recent terrorist attacks in Europe, North Africa, and the Middle East were executed by people indoctrinated on the Internet.

Recruitment and Mobilization. The Internet and advanced technology provide powerful tools for recruiting and mobilizing group members, through integrated communications.

Planning and Coordination. Terrorist groups take advantage of new technologies such as encryption, voice-over-IP, and secure messaging systems to improve the ease, speed, and cost of their communications. This enables the sharing of information such as training videos and manuals, enhancing their planning efforts, and agility in an ever-changing environment.

Fund-Raising. Terrorist groups leverage Internet user demographics and online front groups to execute aggressive funding drives, collecting vast amounts of money through online payment systems that are difficult to track.

Data Mining. Gathering information to facilitate terrorists' strategic knowledge of an opponent and to facilitate terrorist attacks. A sophisticated array of open-source

technologies is used, including search engines and website analytics, to collect intelligence on enemies and potential recruitment and funding targets.

Disinformation. A deliberate propagation of conspiracy theories that undermine public confidence and trust both in government and more traditional media.

The Challenge: Online Counterterrorism

Counterterrorism on the Net is certainly lingering behind the terrorists' manipulative use of this medium. Given the growth of Internet research in recent years, it is rather surprising that research of online countermeasures has been overlooked, or at least, not provided efficient strategy and fruitful devices or tactics. According the Westby, several factors combine to explain this gap: (a) difficulties in tracking and tracing cyber communications, (b) the lack of globally accepted processes and procedures for the investigation of cybercrimes and cyberterrorism, and (c) inadequate or ineffective information sharing systems between the public and private sectors, between governments and between counterterrorism agencies.[15] To these factors one should add the problems of "who is in charge" within governments to direct, much less coordinate, the response.

The technological difficulties associated with tracking and tracing terrorist communications online are particularly related to the use the Internet Protocol (IP) version 4 (IPv4). This packet is not large enough to hold authenticated tracking and audit information for the entire path of the packet. These inadequacies with IPv4 significantly hamper tracking and tracing of cyber-communications and the investigation of cybercrimes. But the technological reasons are marginal when compared with the legal problems. Responding to terrorist websites is an extremely sensitive and delicate issue because most of the rhetoric disseminated on the Internet is considered protected speech under the First Amendment. The case of Carnivore may illustrate the problematic state of online counter measures. In February 1998, Attorney General Janet Reno unveiled plans to establish a new FBI command center to fight "cyber attacks" against the nation's critical computer networks. In October 2001 U.S. House of Representatives approved an antiterrorism bill that gave law enforcement officials expanded surveillance powers to monitor Internet behavior and e-mail. After the 9/11 attacks FBI agents were already visiting the offices of Internet service providers (ISPs), network providers, and e-mail vendors around the country in search of those who perpetrated the attacks. The tool they used to conduct that investigation was the controversial e-mail surveillance system, Carnivore. The system forces Internet service providers to attach a black box to their networks—essentially a powerful computer running specialized software—through which all of their subscribers' communications flow. In traditional wiretaps, the government is required to minimize its interception of non-incriminating—or innocent—communications. But Carnivore does just the opposite by scanning through tens of millions of e-mails and other communications from innocent Internet users as well as the targeted suspect. To use an analogy, Carnivore is like the telephone company being forced to give the FBI access to all the calls on its network when it only has permission to seek the calls for one subscriber. Carnivore can be configured to do one of several things: it can record all of the e-mail messages sent to and from a specific e-mail account. It can record all of the network traffic to and from a specific IP address. It can record all of the e-mail headers (i.e., TO and FROM addresses) sent to and from a specific e-mail account. It can record all of the servers, web-pages, or FTP files visited by a particular IP address. And it can track everyone who accesses a particular web-page or FTP file. When the FBI's use of Carnivore was revealed in July 2000, there was a great

deal of concern expressed by members of Congress, who stated their intent to examine the issues and draft appropriate legislation. Because Carnivore provides the FBI with access to the communications of all subscribers of a monitored Internet Service Provider (and not just those of the court-designated target), it raises substantial privacy issues for millions of Internet users.

Another interesting challenge is the Tor-System. Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. Tor protects the user by bouncing his or her communications around a distributed network of relays run by volunteers all around the world. The system claims that it prevents somebody watching the users of certain Internet connection from learning what sites the users visit and it prevents the sites the users visit from learning the users' location.[16] Following the announcements on the Tor Website it might be nearly impossible for governmental institution to trap somebody in the cyberspace when the user uses this system. Various people with no criminal intention use the Tor to protect their privacy and on the other hand like all dual-use ware it might be a useful tool for terrorists and their supporters.

The virtual war between terrorists and counterterrorism forces and agencies is certainly a vital, dynamic, and ferocious one. The National Security Agency, the CIA, the FBI, the Defense Intelligence Agency, other U.S. and foreign intelligence agencies, and some private contractors are fighting back, cracking terrorist passwords, monitoring suspicious websites, cyberattacking others, and planting bogus information. However, as some argue, there could be better ways to counter the threat: "The government efforts are inadequate. The private sector is doing a better job than the government. Our enemies have embraced the Internet. We have to ask how closely the government is monitoring it."[17]

Beside the legal and practical issues, counterterrorism on the Net suffers from the lack of strategic thinking. Various measures have been suggested, applied, replaced, changed, and debated. Yet, there was never an attempt to propose a general model of online counterterror strategy. Countering terrorist use of the Internet to further ideological agendas will require a strategic, government-wide (interagency) approach to designing and implementing policies to win the war of ideas. The article now suggests the theoretical notion of "noise" in communication theory as a basic theoretical framework to conceptualize various measures and their applicability.

Noise in Communication Processes

In communication theory, noise is that which distorts the signal on its way from transmitter to recipient. Noise interferes with the communication process as it keeps the message from being understood and achieving its desired effect. It is inevitable that noise distorts the message being sent by getting in the way. The concept of noise was introduced as a concept in communication theory by Shannon and Weaver in the 1940s.[18] They were mostly concerned with mechanical noise, such as the distortion of a voice on the telephone or interference with a television signal producing "snow" on the TV screen. In the succeeding decades, other kinds of noise have been recognized as potentially important problems for communication:

- Semantic noise occurs because of the ambiguities inherent in all languages and other sign systems
- Psychological noise occurs when the psychological state of the receiver(s) is such as to produce an unpredictable distraction from receiving intended message

- Cultural noise occurs when the culture or subculture of the audience is so different from that of the sender that the message is understood in a way the sender might not have anticipated

Thus, while the concept of noise was first perceived as relevant only to interference with the transmission of a message, it became recognized later as a crucial element in the communication process, potentially affecting each stage of the process. Shannon and Weaver created a linear model that proposed all communication must include six elements: (1) source, (2) encoder, (3) message, (4) channel, (5) decoder, and (6) receiver. However, the noise factor in the Shannon–Weaver model was applied only to the "message" element in the process. Since then, however, noise has come to represent much more than that. The extraneous variable of noise can become a great barrier to the communication process. Noise can represent physical noise (e.g., loud music, screaming reporters) as well as mental noise such as stress, anxiety, or time constraints that distracts one's thoughts. Today noise is used more as a metaphor for all the problems associated with effective communication, interfering with every stage of the process (including encoding, decoding, transmission, and interpretation).

The concept of noise in communication theory and research has been often treated as a negative element, damaging the communication process. In fact, most empirical uses of the concept were directed at reducing or minimizing noises to improve the flow of communication. However, today, noise is breaking away from the status of undesirable phenomenon bestowed on it by traditional communications theory. No longer merely an undesirable element to be eradicated so as to retain the purity of the original signal, noise can be regarded as a more complex and even desired element. When it comes to the terrorist (or any other illegal, harming, and dangerous) communication, one may question the instrumentality of creating noise that may reduce the communicator's efficiency and success. As demonstrated by the following sections, one can use noises to harm the flow, the decoding, the communicator's credibility and reputation, the signal's clarity, the channel's reach, the receivers' trust, and so on. Creating and using semantic, psychological, cultural, and physical noises may describe a rich variety of countermeasures and organize them in a strategic framework. Thus, noise could become a key conceptual and theoretical foundation in the strategy of countering terrorism online.

Vulnerabilities of Terrorist Online Activity

To identify the vulnerabilities of online terrorism it is essential to understand why their messages are so seductive to certain target audiences.[19] First, the anonymity of the Web allows the users to search the Net, to obtain and become a part of the terrorist narratives without being exposed or identified. Second, many terrorist websites reach out to alienated, frustrated minorities, offering them the sense of social identity and social bonding. Muslim communities in Europe and North America are considered as "Diaspora Communities" by many *jihadist* groups who try to channel these often understandable feelings of social alienation, discrimination, and hopelessness to the ideological, religious, and mostly social bonding. To be seduced by terrorist messages and narratives, the user must be in a condition of emotional need. To be persuasive, the narratives have to suggest goal fulfillment, namely the achievement of a sense of identity. To provide that identity, personal motivation must become influenced by a higher motivation, which in turn determines the goal formation. Users may quickly develop the illusion that the many share the same beliefs. Once inside this online community, users gain acceptance, attention, and approval. Additionally, the real

world community, namely the users' friends, provide feedback loops. This confirmation from the real world is important to create a more stable sense of identity, which in turn ensures that the users themselves are transformed into a human guidance system that is programmed for a one-way trip.

The radicalization process involves several stages, with each open to counter campaigns, thus knowing these stages is vital to recognizing the vulnerabilities of the process.[20] First, the users have to inhibit an individual interest or motivation that leads them to search for radical websites. This phase is called "Searching Phase" because the users look for specific answers that may provide full or partial fulfillment of their needs. In the second phase, the "Seduction Phase" the users start to visit specific websites and are thus being introduced to the radical ideology. The third step, the "Captivation Phase" is being considered as the most important one because in this phase the users start to visit blogs, forums, and chat rooms and become attracted by their seductive messages. The forth phase is the "Persuasion Phase" when the users make the decision to become active in the online exchange and are integrated into the online community. For many, the road ends here but few will be selected to move on, to the final step, the "Operative Phase." In this phase the user is introduced to various operative activities of the online community and/or of a specific terrorist organization. It should be noted that throughout the stages of the online radicalization process the user is also interacting with the real world environment (including, most often, family members, friends, and the mass media). The process may require weeks, months, or years but it is always a gradual, multi-stage process. An understanding of this process is essential to identify the stages where a user is still open for alternatives ideas and messages or how to interfere with the process with specific "noises." Thus, for example, it will be assumed that as long as the individual is not totally indoctrinated he or she is still open for alternative worldviews.

Another important factor is the organization's structure. The vulnerability of the terrorist online activity relates also to the group's "structuredness": the more hierarchical the structure is, the more effective will be the "silencing," neutralization or discreditation of leaders and centrally positioned operators. When a terrorist organization has more the form of loosely knit network with several hubs, the targets for counterattack are numerous and harming only one or some may be futile.

Finally, the terrorist online activity is mostly "visible," open to all. Especially when it comes to propaganda, psychological warfare, publicity and early stages of the radicalization process—terrorists are seeking exposure and try to reach vast audiences. Their online activity is open to all: the way they invade the Internet and abuse its liberal spirit and unregulated nature—their own activity is open to such intrusions.

Conceptualizing the Notion of Noise into a Strategy

Strategic communication planning is one of the most neglected areas of counterterrorism, especially when it comes to the disruption of terrorist communication.[21] Strategic communication requires a sophisticated method that maps perceptions and influences networks, identifies policy priorities, formulates objectives, focuses on "doable tasks," develops themes and messages, employs relevant channels, leverages new strategic and tactical dynamics, and monitors success. This approach has to build on in-depth knowledge of radical thinking, radicalization processes, and factors that motivate radical or terrorist behavior. To make such an approach successful one has to learn how to combine hard and soft power in terms of strategic communication.[22] Joseph S. Nye, *Power in the Global Information Age, from Realism to Globalization* (London: Routledge, 2004). The principal

understanding of power, to make the others to do what you want or to produce the outcomes you want has not changed. Whereas hard power means the ability to order others to do what you want, "Soft power is the ability to get what you want through attraction rather than coercion or payments. When you can get others to want what you want, you do not have to spend as much on sticks and carrots to move them in your direction. Hard power, the ability to coerce, grows out of a country's military and economic might. Soft power arises from the attractiveness of a country's culture, political ideals, and policies."[23]

An effective communication strategy to counter terrorist online activities has to combine both hard power elements (such as hacking) and soft power elements (such as psychological warfare) because "soft power and hard power can reinforce each other; one is not contrary to each other."[24] Finally, Nye assumes that soft power does not increase relative power on the hard side, but it does make hard power more acceptable, lowering the costs of exercising such power. Returning to the notion of noise, mechanical noise includes the elements of "hard power" and the term "soft power" enfolds the characteristics of social and psychological noise. There are certain key elements in the application of "noise" as a counter strategy against terrorists' appeal on the Net. These elements include:

Credibility. As in other communication processes, a key factor in determining the persuasiveness of terrorist messages is the credibility of the source. Thus, a counter strategy may involve a systematic damaging of the terrorist authority, a partial or full destruction of its credibility while an alternative authoritative or credible source may be introduced. Weimann's studies of the inner debates and disputes among terrorists online may expose those cleavages and splits that can be used to attack the credibility of terrorist online authorities.[25]

Terminology. Terminology plays a significant role in the process. For example, one needs to understand better the nuances of Islam in contrast to extreme Islamic preaching, the nuances of *jihad*, *salafist* terminology, and the subtexts of their communication. An effective application of "noise" may rely on the use of key terms, exposing their manipulative uses, relating new meaning to them or weakening of their conventional use. For instance, should the terms *jihad* and *jihadist* be replaced with their nonviolent interpretations by leading Muslim figures? The term Islamism may be replaced with the term anti-Islam suggesting that it is far from being in line with the pure and original values of Islam.

Traditions. The rhetoric of online preaching and radicalization relies on traditions. Thus, one should look for solutions from within Muslim traditions, because solutions derived from Western traditions will by definition be rejected as illegitimate. This requires a deep understanding of the traditional thinking, values, and symbols of the community targeted.

Partners. In order to be truly effective in de-legitimizing radical appeals and attraction the counter campaign may involve the activation of "partners" who come from within the targeted community. Thus, the alternative voices, suggesting alternative narrative and discourse—should come from within Muslim religious leadership, not from the West.

Act local, think global. A long-term perspective starts with the search for additional "agents" of change, for supporting actors and institutions. Such actors may include state institutions that provide education, medical treatment, and social warfare. Furthermore, universities in the Arab world as well as schools and nongovernmental organizations (NGOs), could provide useful venues in which to open up the "modernization" debate.

The same debate can be continued via Islamic education in public schools throughout Europe, articles in journals, and the efforts of individual intellectuals. Such debate would allow all parties to hear different views and engage in a discussion that can truly educate, without appearing from the start to be a narrowly construed instrumental propaganda effort. Again, these educational reforms need to come from within the Muslim world, although the West can support it with its resources.

An effective strategy must be multifaceted, addressing all these aspects. This is a long-term undertaking that needs to be based on familiarity with the targets' background, mentality, values, beliefs, history, frustrations, and hopes. Moreover, before a communication strategy could be developed it is essential to define the strategic goals, to identify potential partners and to characterize the target audiences. As one U.S. counterterrorism official argued, the problem is "that we focus on the terrorists and very little on how they are created. If you looked at all the resources of the US government, we spent 85, 90 percent on current terrorists, not on how people are radicalized."[26]

The first step involves the identification of terrorist websites and the study of their contents to determine the necessity of applying various disruptive tactics. This monitoring can be done by human analysts and coders (i.e., the manual approach) or by automatic Web crawlers. The manual approach is often used when the relevance and quality of information from websites is of the utmost importance. However, this approach is labor-intensive and time-consuming, and often leads to inconclusive results. The automatic Web crawling technique is an efficient way to collect large amounts of web-pages. This can be done using retrieval systems such as Convera RetrievalWare. Cross-lingual information retrieval (CLIR) can help break language barriers by allowing users to retrieve documents in foreign languages, via queries in their native languages.

The monitoring covers not only websites but also forums and chat rooms: Observation is essential to learn about the target groups, the participants, the key players, the appeals and rhetorical motives, the ideas and rewards promised. The information gathered at this stage may indicate what measures are required if at all and the urgency to apply noise tactics. The article now turns to illustrative examples of actual "noise," distinguishing between mechanical/technological noises and psychological/social noises (See Figure 1).

Mechanical/Technological Noises

This type of noise refers to technological disruption of the flow of communication. The mechanical/technological tactics include a rich variety of interferences, from damaging websites, defacement, and redirection of users to spreading viruses and worms, blocking access, hacking, and total destruction. If mechanical/technological tactics are to be used the arsenal include a rich variety of actions learned from cyberattacks, cybercrime, cyberactivism, and hacking. These deviant measures can be adopted and used against online terror and to minimize their reach and impact. In the most severe cases, hacking the websites may be the most extreme measure although not always the most efficient one in the long run.

Needham and Lampson describe an impressive arsenal of common hacking techniques, available also for counterterrorism.[27] Many actual attacks, they argue, involve combinations of vulnerabilities. Examples of vulnerabilities include stack overflow attacks, used by Internet worms. A common strategy is to get an account on any machine on a target network, then install a password sniffer to get an account on the target machine, then use a stack overflow to upgrade to a root account. Needham and Lampson provide a list of "the

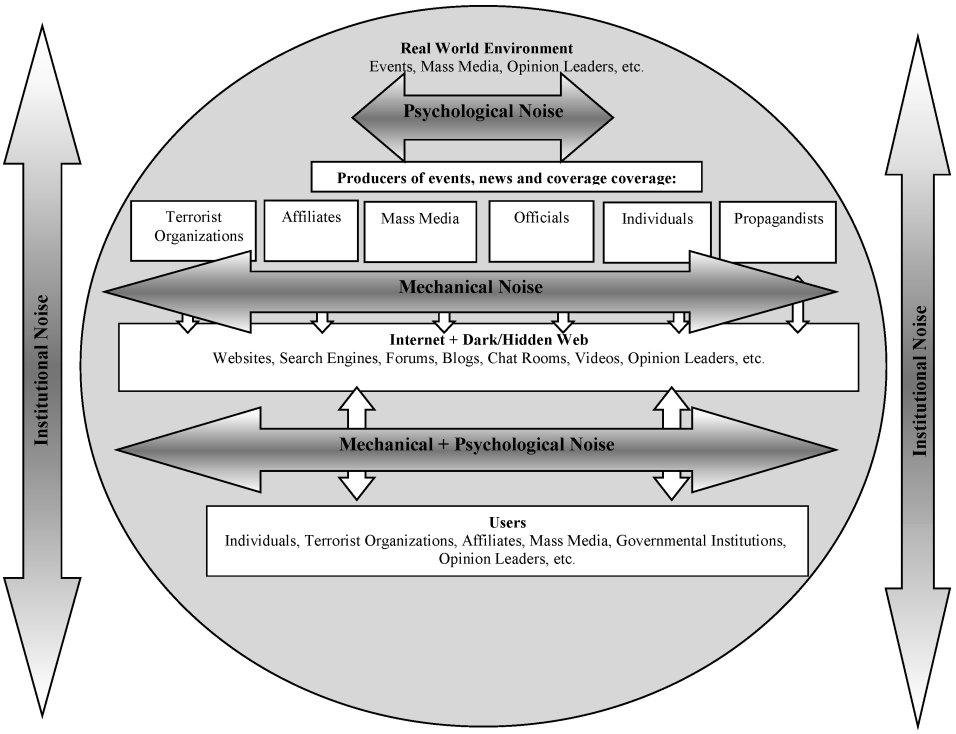

Figure 1. Using "noises" to counter terrorist online communication.

top 10 vulnerabilities" and suggest a hacking strategy using each of these vulnerabilities. Most of the exploits make use of program bugs, of which the majority is stack overflow vulnerabilities. They also argue that none of the attacks is stopped by encryption and not all of them by firewalls.

Another common attack is known as *smurfing*. This exploits the *Internet Control Message Protocol* (ICMP), which enables users to send an echo packet to a remote host to check whether it's alive. A collection of hosts at a broadcast address that responds in this way is called a *smurf amplifier*. The attack is to construct a packet with the source address forged to be that of the victim, and send it to a number of smurf amplifiers. The machines there will each respond (if alive) by sending a packet to the target and this can swamp the target with more packets than it can cope with. Smurfing is typically used by someone who wants to take over an *Internet relay chat* (IRC) server, so they can assume control of the chatroom. The innovation was to automatically harness a large number of "innocent" machines on the network to attack the target.

A more common assault is the *distributed denial of service* (DDoS) attack. The attacker subverts a large number of machines over a period of time, and installs custom attack software in them. At a predetermined time, or on a given signal, these machines all start to bombard the target site with messages. So far, DDoS attacks have been launched at a number of high-profile websites, including Amazon and Yahoo! but they can easily be turned against terrorist sites. Some of the preceding ideas can be combined into *spoofing attacks*. A spoofing attack occurs when one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Say that Charlie

knows that Osama and Ayman are hosts on the target LAN, and wants to masquerade as Osama to Ayman. He can take Osama down with a service denial attack of some kind, and then initiate a new connection with Ayman. A simple way of guessing the sequence number of Ayman, which worked for a long time, was for Charlie to make a real connection to Osama shortly beforehand, and use the fact that the value of Ayman changed in a predictable way between one connection and the next. Modern stacks use random number generators and other techniques to avoid this predictability, but random number generators are often less random than expected—a source of large numbers of security failures. If sequence number guessing is feasible, then Charlie will be able to send messages to Ayman, which Ayman will believe come from Osama.

Another option is the use of *routing attacks*. These attacks have three forms: An attack using a subverted router, when a router is taken over by the attacker and used to gain further control over the hacked network; an attack using a rogue router when an unauthorized router is deployed by an attacker on the network. If a routing updates authentication mechanism is absent or bypassed, such a router can participate in the routing process on the network and alter it in accordance with the attacker's needs; and an attack using a masquerading router that spoofs a legitimate router's identity to gain access to the routing domain. This can be done to bypass access lists and may involve source routing attacks. The end result of any routing attack is the redirection of traffic on the network. Thus, the basic routing attack involves Charlie telling Osama and Ayman that a convenient route between their sites passes through his and in fact take control of the online traffic between the two and all their networks.

There is also the optional use of *Trojan Horses*, *viruses,* and *worms*. Computer security experts have long been aware of the threat from malicious code, or *malware* but various forms of malware can be used against online terrorists. The common distinction among the three is that a Trojan horse is a program that does something malicious when run by an unsuspecting user; a worm is something that replicates; and a virus is a worm that replicates by attaching itself to other programs. A virus or worm will typically have two components: a replication mechanism and a payload. The replication by a worm or virus is simply making a copy of itself somewhere else usually by breaking into another system or by mailing itself as an attachment. The second component is the payload. This will usually be activated by a trigger, such as a date, and may then do one or more of these damages: make selective or random changes to the computer's protection; make selective or random changes to user data (e.g., trash the disk); lock the network (e.g., by replicating at maximum speed); steal resources or steal data; and even take over the infected system.

Finally, there is the option of *identity theft.* In the United States, about half a million people are the victims of this kind of fraud each year. The most common form of identity theft is credit card fraud. Terrorists use this crime to fund their activities and disguise the identities of their operatives. According to Judith Collins from the Michigan State University Identity Theft Crime and Research Lab, "All acts of terrorism enacted against the United States have been facilitated with the use of a fake or stolen Identity."[28] Collins indicates that 5 percent of all identity thieves are connected to terrorism and 2 percent, specifically to Al Qaeda. In fact, the Al Qaeda terrorists involved in the 11 September 2001 attacks had opened 14 bank accounts using several different names, all of which were fake or stolen. If criminals can steal someone's identity, counterterrorists can do the same. Fraudulently making a video- or audiotape as Osama bin Laden and passing it to Al-Jazeera or faking articles and videos to be placed on Al Qaeda's websites, should not be that difficult. Such attacks can create confusion among the terrorists' followers and supporters, harm the credibility of their websites and messages, and lower these sites' exposure and attraction.

Psychological/Social Noises

The tactics included in this category involve various psychological and social operations and counter-propaganda. Different terms relate to Psychological/Social Noise: Information Warfare, Information Operation (IO), and Psychological Operation (PSYOP). There are numerous definitions of these terms.[29] Information Warfare is simply the use of information to achieve national objectives: "The target of information warfare, then, are the human minds that make decisions of war and peace and, from the military perspective, those minds that make the key decisions on if, when and how to employ the assets and capabilities embedded in their strategic structures."[30] Information Warfare consists of a broad variety of information operations (IOs). The focus of IO is on the decision maker and the information environment in order to affect decision making and thinking processes, knowledge, and understanding of the situation. Thus, for instance Psychological actions or operations (PSYOP) are a part of Information Operations.

As defined, "PSYOP are operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."[31] As a communication medium and vehicle of influence, the Internet is a powerful tool for psychological campaigns. Consequently, the realm of military psychological operations (PSYOP) must be expanded to include the Internet: "Although current international law restricts many aspects of PSYOP either through ambiguity or noncurrency, there is ample legal room for both the U.S. and others to conduct PSYOP using modern technology and media such as the Internet."[32] Today, in order to remain relevant, "PSYOP must demonstrably influence audiences in an increasingly sophisticated international information environment. . . . Without a fundamental change in the way PSYOP forces are permitted to conduct day-to-day functions, they can never co-opt the information cycle of a sophisticated adversary."[33] Whether used offensively or defensively, it is clear that the Internet is an important tool for PSYOP and can bring tremendous capabilities and informational advantage to forces employing this medium.

The crises in Serbia and Kosovo are good examples of the importance of PSYOP campaigns. The IOs used during these crises integrated the elements of counter-propaganda, PSYOP, civil affairs, and public affairs with the actions of maneuver forces to influence and modify the attitudes, perceptions, and behaviors of key decision makers and groups.[34] After NATO bombed Serb media outlets considered a source of Milosevic propaganda, the U.S. government decided not to cut off Serb Internet sites. The decision was based on the assumption that "full and open access to the Internet can only help the Serbian people know the ugly truth about the atrocities and crimes against humanity being perpetrated in Kosovo by the Milosevic regime."[35] However, as noted by many analysts, at the start of the conflict, Serbia maintained information superiority over the minds of its citizens and, to a lesser extent, outside Serbia. The Serbs also used the Internet to spread various campaign themes. In this way, Milosevic was able to asymmetrically respond to U.S. and NATO actions.

Given the strategic opportunities afforded by the Internet, there are several options for employing this medium in PSYOP. Counterterrorism agencies in particular could use the Internet offensively to help achieve unconventional warfare objectives, as well as to address and counter adversarial propaganda, disinformation, and incitement. In addition to websites, preempting messages and developing Internet products such as streaming audio/video, online video games, mediated newsgroups, and ad banners can also be leveraged for their strategic value and reach. The Defense Science Board report on PSYOP also suggested

some less obvious potential tools using emerging media technologies, such as chat rooms and instant messaging services that could be used for "guided discussions" to influence how various groups and audiences think about certain topics.[36]

Some of these tactics are rooted in the evolving domain of political Internet campaigns. Moveon.org (http://www.moveon.org) is a prominent example of a Web-based political campaign. In many ways terrorists launch their online campaigns in the same way legitimate political campaigns use the Internet. Both attempt to attract the users, to seduce them by engaging them in a sensory experience, trying to manipulate their needs, suggesting the fulfilment of a goal, and inspiring and guiding the users to make a choice by providing a higher-level motivation. Captivation occurs on the fulfilment of the goal, and the function at this point is to facilitate the formation of a relational bond between the user and the party/candidate/group/organization. Thus, there are lessons to be learned from the online campaigns and counter- campaigns in the political arena: they can serve as pivotal experiments to guide counterterrorist campaigns. Political campaigns are in fact a series of actions and appeals involving resource mobilization. The communicators are trying to mobilize the predisposed, demobilize hostile voters, convince the undecided, and convert the initially hostile. They must do so by designing persuasive messages, communicating these messages, monitoring the responses, and facilitating the desired behavior.[37] Campaigning via the interactive Internet often provides social bonding and replicates feelings of personal contact.[38] These elements, frequent also in terrorist websites, can also be used in counter campaigns. However, before such campaigns are launched, the agencies involved should know the psychographic profiles of those susceptible to recruitment, and secondly, the messages that affect them. They also need to understand how these individuals are influenced: what channels are meaningful to them, whom they listen to, the effect of peer networks, and how to reach them most effectively.

To run such a strategy, a political Internet campaign against terrorism must use tactics that have proven successful and that can be applied to the counterterrorism arena. One illustrative example may be the use of "opinion leaders" or "influentials." Scholars at the *Institute for the Internet and Democracy* at George Washington University found in their research that 69 percent of individuals who accessed the website of a political party or candidate from 26 November to 31 December 2003 were "influentials."[39] They are those individuals, comprising about 10 percent of the population who influence others and mediate messages from the mass media to their followers in a process termed as two-step flow of communication. Decades of social science research have demonstrated that there is a group of people in any community to whom others look to help them to form opinions on various issues and matters. Whether called "opinion leaders" or "influentials," these people literally *lead* the formation of attitudes, public knowledge, and opinions. In the classic book, *Personal Influence*, opinion leadership is defined as: "... leadership at its simplest: it is casually exercised, sometimes unwitting and unbeknown, within the smallest groupings of friends, family members, and neighbors. It is not leadership on the high level of Churchill, nor of a local politico; it is the almost invisible, certainly inconspicuous form of leadership at the person-to-person level of ordinary, intimate, informal, everyday contact."[40] Since the introduction of the opinion leadership conceptualization, both practitioners and academics have been keenly interested in its applicability in modern society. Hundreds of studies have been conducted to identify potential opinion leaders, learn of the characteristics distinguishing them from their "followers," and understand how they exert their personal influence to change opinions and behaviors of the masses.[41]

The two-step flow of communication hypothesis asserts that information from the media moves in two distinct stages. First, individuals (opinion leaders) who pay close

attention to the mass media and its messages receive the information. These opinion leaders then pass on their own interpretations in addition to the actual media content. Opinion leaders are quite influential in getting people to change their attitudes and behaviors, and are quite similar to those they influence. The two-step flow theory has improved our understanding of how the mass media influence decision making. The theory has refined our ability to predict the influence of media messages on audience behaviour, and it has helped to explain why certain media campaigns may have failed to alter audience attitudes and behavior. It is probably accurate enough to assume that the influentials among Islamist and extremist groups and societies similarly visit radical websites, and seduce and persuade their friends to share the given ideas and views. If this is the case, it is even more important for the West in general to develop an online strategy to challenge these opinion leaders, to harm their credibility, to substitute them, to slow if not to block their flow of influence and to weaken their status by online counter-campaigns.

Institutional Noise: Many Noises Make One Big Noise

A crucial part in this strategy plays the institutionalization of a Web-focused, multinational counterterrorism campaign. Institutional noise is required to coordinate the mechanical and psychological noises, to allocate proper resources and most importantly to maximize its efficiency, reach, and impact. No international security threat has facilitated intergovernmental cooperation on the levels of politics, intelligence and law enforcement to the extent terrorism has. The United Nations, the European Union, OSCE, and NATO have proven to be successful platforms for harmonizing counterterrorism policies.

The EU has implemented the first steps towards institutionalization of joint Web-based counterterrorism. It has recognized the threat of how terrorists are using the Internet for their purposes and proposed strategy and action plan for combating online radicalization and recruitment by terrorists. The EU called for measures to combat terrorist use of the Internet: "We need to spot such behaviour by, for example, community policing, and effective monitoring of the Internet and travel to conflict zones. (. . .) And we will examine ways to impede terrorist recruitment using the Internet."[42] The EU also emphasized the activities required to prevent the misuse of the Internet for terrorist purposes while at the same time observing fundamental rights and principles: "The European Council calls for the implementation of the action plans agreed under the EU Counter Terrorism Strategy, including the strategy against radicalization and recruitment, to be accelerated. The European Council awaits the Commission's first programme in this connection as well as concrete proposals on detection technologies. The Council and the Commission are also invited to develop measures to combat the misuse of the Internet for terrorist purposes while respecting fundamental rights and principles."[43] The EU member states and Europol are already actively monitoring and evaluating terrorist websites. The Council supports the initiative "Check the Web," which aims at strengthening cooperation and sharing the task of monitoring and evaluating open Internet sources on a voluntary basis.[44] The Interpol, Europol, and shadowy organizations like the Club of Berne or the Security Alliance in Paris are examples that show that, in the face of the threat of terrorism, the institutionalization of functional cooperation and information-sharing on the level of law enforcement and intelligence is possible. However, the required global institutionalization of mechanical and psychological noises should be organized as an international network, a counter-network to terrorist online networks.

The concept of the hierarchy of governmental security institutions is built on three assumptions: the environment is stable, the processes are bureaucratic, and the output

is definable and more or less predictable. Obviously, these assumptions no longer apply to terrorism. Governmental organizations are controlled by hierarchies, and the counterterrorism departments should be linked according to a paradigm, articulated by the Linux Project.[45] This project relies on open and adaptive systems that promote learning, co-operation, and flexibility, and that takes the form of networks of governmental analysts, artificial intelligence labs, and research institutions instead of individuals. Inspired by the Linux Project, the suggested system should be based on open source analyses, should focus on tactical and strategic issues using participation and empowerment, team accountability, matrix arrangements (flexible positions and responsibilities based on the abilities of the participating institutions), information networking, and initiatives for improvements should emanate from all directions on a regular basis.

Such online processes are known in different communities of software developers as well as open-source communities. The most well-known open-source community is Wikipedia. The strength of Wikipedia is not the technology, but the massively collaborative effort of thousands of decentralized contributors joined by a global online communication network. These communities practice an ongoing collective learning process and collective intelligence. Based on the fact that most of radical terrorists' information is available online, a considerable amount of this valuable data can be collected and stored in the Internet (websites, open communication platforms), and relevant analysis can be generated just using this database. The new tools of U.S. Intelligence include a federated search engine called Oogle[46] and Intellipedia, a controversial intelligence data-sharing tool based on Wiki social software technology.[47] Intellipedia uses MediaWiki, the same software used by the Wikipedia free-content encyclopedia project.

The key factor may be the creation of an access for consuming and providing open source material and analyses that enables a common computing and communications infrastructure. The heart of this system might be a technological platform including collaborative Terrorism Data Fusion Center with analytical tools and databases of open source data. The challenging factors are trust and symmetry. An infrastructure in which all parties have symmetrical rights might be useful to avoid political domination. For this reason the institution might be virtually and physically led by a committee consisting of representatives of the participating institutions or a rotation system. To avoid a situation where a participating country just consumes the data provided by other participants, a sort of credit point system should be established. This system should guarantee that the parties are allowed to consume as much data in the quality as they have provided.

A useful illustration for such a system might be the concept of openflows: "An openflow is a cluster of initiatives, people and computers who create platforms, projects and concepts for the development of Open Source Intelligence or OSINT."[48] The technologies of the Internet allow for the development of new ways of collaboration, ways that are more open, more collaborative, less hierarchical, and, also, more efficient. The open flow aims to help address these challenges in terms of its technological aspects, its organizational and conceptual dimensions, its valuable resources, and its efficiency and effectiveness.[49]

Conclusion

The Internet may be the most perfect embodiment of the democratic ideals of free speech, open communication, and the "marketplace of ideas" that has ever existed. As the American Supreme Court has written, online "any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox." Unfortunately, freedom on the Internet is far from secure—in fact, it is under challenge from numerous radical

groups and terrorist organizations. Modern terrorism and especially *jihadist* groups use the Internet for various functions, from communicative purposes such as propaganda and distribution of information to instrumental uses such as recruitment or virtual training. Many violent groups with a long record of victimization, bloodshed, and destruction have entered the Internet. Their sophisticated, effective, and growing use of this liberal, free, easy-to-access medium is indeed frightening.

Due to the growing reliance of terrorists on the Internet, the virtual war between terrorists and counterterrorism forces and agencies is certainly a crucial one. However, counterterrorism on the Net is certainly lingering behind the terrorists' manipulative use of this medium. It is indeed a startling paradox that the worst enemies of Western modernity and technology are using the most advanced Western technology of communication, the Internet, for their destructive campaigns. Moreover, the online terrorists never invented or advanced any online technology, they simply adapted the existing platforms and software. Thus, it seems odd that those who invented, advanced, and maintain the medium are victimized by the "late comers" into cyberspace. There are several reasons for this alarming fact: beside the legal and practical issues, counterterrorism on the Net suffers from the lack of strategic thinking. Various measures have been suggested, applied, replaced, changed, and debated. Yet, there was never an attempt to propose a general model of online counterterrorism strategy. This article argues that the answer to terrorist use of the Internet lies not in censorship of the Internet, but in a more sophisticated and complicated strategy, relying on the theoretical notion of "noise" in communication process theory.

To understand the communication process of terrorists and its countermeasures the following model might be useful. Various producers present, post, and promote radical message in various forms (videos, games, postings, online publications, and websites) on the Net and in the Dark Web. Target audiences such as potential followers, radicals, terrorist organizations, journalists, governmental agencies, and NGOs receive these messages directly or indirectly, through exposure, interpersonal diffusion, or search engines. The understanding of this communication process enables one to identify the potential targets of a counterstrategy or the activation of noise. The following model presents the terrorist communication process and the placement of various "noises" that may hinder, slow down, damage, or disrupt the terrorist abuse on the Net.

No longer merely an undesirable element to be eliminated, noise can be regarded as a more complex and even desired element under certain circumstances. When it comes to terrorist communication, the concept of noise can serve as a key conceptual and theoretical foundation in the strategy of countering terrorism online. As demonstrated by this article, various "noises" can be used to harm the flow, the decoding, the communicator's credibility and reputation, the signal's clarity, the channel's reach, the receivers' trust and more. Creating and using mechanical/technological or social/psychological noises may illustrate the potential of a rich variety of countermeasures and organize them in a strategic framework.

Rephrasing von Clausewitz, the Internet should be regarded as "an increasing continuation of war by other means." The new arena, cyberspace, presents new challenges and requires dramatic shifts in strategic thinking regarding national security and countering terrorism.

Notes

1. Brian Jenkins, *International Terrorism* (Los Angeles: Crescent Publication, 1975), p. 4.

2. Gabriel Weimann and Conrad Winn, *The Theater of Terror: Mass Media and International Terrorism* (New York: Longman, 1994).

3. Brigitte Nacos, *Mass-Mediated Terrorism* (Oxford: Rowman and Littlefield, 2002); Brigitte Nacos, "The Terrorist Calculus Behind 9–11: A Model For Future Terrorism?," *Studies in Conflict & Terrorism,* 26 (2003), pp. 1–16.

4. The quotes are taken from the translations of a videotape, presumably made in mid-November 2001 in Afghanistan. Available at http://www.washingtonpost.com/wp-srv/nation/specials

5. Bruce Hoffman, "Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment," *Studies in Conflict and Terrorism,* 26 (2003), pp. 427–440; Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008).

6. John Arquilla and David Ronfeldt, "The Advent of Netwar (revisited)," in *Networks and Netwars,* John Arquilla and David Ronfeldt, eds. (Santa Monica: RAND Corporation, 2001); John Arquilla and David Ronfeldt, "Networks, Netwars, and the Fight for the Future," *First Monday* (25 October 2003), pp. 1–25; John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar and Information-Age Terrorism," in *Countering the New Terrorism*, Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, eds. (Santa Monica: RAND Corporation).

7. Cited by Jack Kelly, "Militants Wire Web with Links to Jihad," *USA TODAY* (10 July 2002), available at http://www.usatoday.com/news/world/2002/07/10/web-terror-cover.htm

8. Rita Katz and Josh Devon, "WWW.J I H A D.COM: E-Groups Abused by Jihadists," *National Review Online* (2003), available at http://www.nationalreview.com/comment/comment-katz-devon071403.asp

9. Marc Rogers, "The Psychology of Cyber-terrorism," in *Terrorist, Victims and Society*, Andrew Silke, ed. (Chichester: John Wiley & Sons, 2003), pp. 77–92.

10. Gabriel Weimann, *How Modern Terrorism Uses the Internet* (Washington, DC: United States Institute of Peace, Special Report 116, 2004), available at http://www.usip.org/pubs/specialreports/sr116.pdf; Gabriel Weimann, *Terror on the Internet* (Washington, DC: United States Institute of Peace Press, 2006); Bruce Hoffman, "The Use of the Internet by Islamic Extremists," Testimony before the House Permanent Select Committee on Intelligence (Rand Corporation, CT-262–1, 4 May 2006), available at http://www.au.af.mil/au/awc/awcgate/congress/hoffman_testimony4may06.pdf

11. Stephen Coll and Susan B. Glasser, "Terrorists Turn to the Web as Base of Operations," *The Washington Post* (7 August 2005),p. A01, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html; Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday* (November 2002), available at http://www.firstmonday.org/issues/issue7_11/conway/; Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back" (September 2005), available at http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura_conway.pdf; Audrey Kurth Cronin, "Cyber-Mobilization: The New *Levee en Masse*," *Parameters* (Summer 2006), pp. 77–87, available at at:http://www.carlisle.army.mil/usawc/Parameters/06summer/cronin.htm; Susan B. Glasser and Stephen Coll, "The Web as a Weapon," *The Washington Post* (9 August 2005), p. A01, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html; Nadya Labi, "Jihad 2.0," *The Atlantic Monthly* (July/August 2006), available at http://www.theatlantic.com/doc/prem/200607/online-jihad; Marc Lynch, "Al-Qaeda's Media Strategies," *The National Interest* (Spring 2006); Hanna Rogan, "Jihadism Online: A Study of how al-Qaida and Radical Islamist Groups use the Internet for Terrorist Purposes" (Norwegian Defense Research Establishment, FFI/RAPPORT-2006/00915, 2006), available at http://rapporter.ffi.no/rapporter/2006/00915.pdf; Jon Swartz, "Terrorists' use of Internet Spreads," *USA Today* (20 February 2005), available at http://www.usatoday.com/money/industries/technology/2005–02-20-cyber-terror-usat_x.htm; David Talbot, "Terror's Server," *Technology Review* (Massachusetts Institute of Technology, February 2005), pp. 46–52; Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters* (Spring 2003), pp. 112–123, available at http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm; Weimann, *How Modern Terrorism Uses the Internet*; Weimann, *Terror on the Internet*; Michael Vatis, *Cyber Attacks During The War on*

Terrorism: A Predictive Analysis (Institute for Security Technology Studies, Dartmouth College, 22 September 2001), available at http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf

12. Cited in ADL report "Terrorist Activities On the Net," available at http://www.adl.org/terror/focus/16_focus_a.asp

13. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning.'"

14. Weimann, *How Modern Terrorism Uses the Internet*; Weimann, *Terror on the Internet*.

15. Jody R. Westby, "Countering Terrorism with Cyber Security," paper for the 36th Session of World Federation of Scientists, International Seminars on Planetary Emergencies (18–26 August 2006, Erice, Italy).

16. Tor Anonymity Online, available at http://www.torproject.org/index.html.en (accessed 12 October 2007).

17. Bruce Hoffman, cited in Les Blumenthal, "U.S. Seeks to Counter Terrorists' use of the Internet" (2007), available at http://www.kansascity.com/news/world/story/287013.html

18. Clause Shannon and Warren Weaver, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1949).

19. Boaz Ganor, Katharina von Knop, and Carlos Duarte, *Hypermedia Seduction for Terrorist Recruiting*, B. Ganor, K. Von Knop, C. Duarte, eds. (Washington, DC: NATO Science for Peace and Security Series, 2007); Sageman, *Leaderless Jihad*; Gabriel Weimann, "Using the Internet for Terrorist Recruitment and Mobilization," in *Hypermedia Seduction for Terrorist Recruiting* (Washington, DC: NATO Science for Peace and Security Series, 2007), pp. 47–58.

20. Daniel Benjamin and Steven Simon, *The Next Attack: The Failure of the War on Terror and a Strategy for Getting It Right* (New York: Henry Holt and Company, 2005); Christine Fair, "Militant Recruitment in Pakistan: Implications for Al Qaeda and Other Organizations," *Studies in Conflict & Terrorism,* 27(6) (2007), pp. 489– 504; Bruce Hoffman, William Rosenau, Andrew Curiel, and Doron Zimmermann, *The Radicalization of Diasporas and Terrorism* (Santa Monica, CA : RAND National Security Research Division, 2007); Sageman, *Leaderless Jihad*.

21. Frank Bolz, Kenneth Dudonis, and David Schulz, *The Counterterrorism Handbook: Tactics, Procedures, and Techniques* (Boca Raton: CRC Press, 2002); Richard Halloran, "Strategic Communication," *Parameters* (Autumn 2007), pp. 4–14.

22. Joseph S. Nye, *Power in the Global Information Age, from Realism to Globalization* (London: Routledge, 2004).

23. Joseph S. Nye, "Soft Power and American Foreign Policy," *Political Science Quarterly,* 119(2) (2004), p. 256.

24. Joseph S. Nye, "The Power of Persuasion, Dual Components of US Leadership," *Harvard International Review,* 24(4) (2003), p. 46.

25. Gabriel Weimann, "Virtual Disputes: The Use of the Internet for Terrorist Debates," *Studies in Conflict and Terrorism,* 29(7) (2006), pp. 623–639; Gabriel Weimann, "When Fatwas Clash Online: Terrorist Debates on the Internet," in *Information Warfare 2.0: How States and Armed Groups Compete for Strategic Influence*, James J. F. Forest, ed. (Westport, CT: Praeger, 2008).

26. Cited by Karen deYoung, "Spy Agencies Iraq War Hurting U.S. Terror Fight," *Washington Post* (24 September 2006), available at http://www.washingtonpost.com/wp-dyn/content/article/2006/09/23/AR2006092301130.html

27. Roger Needham and Butler Lampson, "Network Attack and Defense," available at http://www.cl.cam.ac.uk/∼rja14/Papers/SE-18.pdf (accessed 1 January 2008).

28. From "Terrorist Groups Relying on Identity Theft for Funding and Operations," *About.Com*, available at http://idtheft.about.com/od/useofstolenidentity/p/IDTheftTerror.htm

29. Arnulf Kopeinig, "Information Warfare" (Österreichische Militärzeitschrift, vol. 1, 1999), p. 23.

30. George S. Stein, "Information Warfare," *Airpower Journal* (Spring 1995), p. 32.

31. Joint Chiefs of Staff, *Joint Psychological Operations*, Joint Pub 3–53 (Washington, DC: GPO, 10 July 1996), p. I-1.

32. Angela Maria Lungu, "War.com: The Internet and Psychological Operations," paper submitted to the Faculty of the Naval War College (2001), p. 3.

33. Steven Collins, "Army PSYOP in Bosnia: Capabilities and Constraints," *Parameters,* 29 (1999), p. 57.

34. Timothy LaBahn, "Information Operations in Bosnia," *FA Journal* (November–December 2001), p. 32.

35. DOS spokesman James Rubin, quoted in Jon Swartz, "Administration Drops Idea of Blocking Serb Net Sites," *The San Francisco Chronicle* (15 May 1999).

36. Defense Science Board, *Information in Support of Psychological Operations*, quoted by Lungu, "War.com: The Internet and Psychological Operations."

37. Stephen E. Frantzich, *Political Parties on the Technological Age* (New York: Longman, 1989); Judith S. Trent and Robert Friedenberg, *Political Campaign Communication: Principles and Practises*, 3rd ed. (Wesport, CT: Praeger, 1995).

38. Gary Selnow, *Electronic Whistle-Stops: The Impact of the Internet on American Politics* (Westport, CT: Praeger, 1998).

39. Montague Kern, "Web and Mass Media Campaigns by Political Candidates: MoveOn.org and the Democratic Party in 2003–2004 Presidential Primaries," in *Elections on the Horizon: Marketing Politics to the Electorate in the USA and UK* (London: The British Library, 2004), available at http://sherpa.bl.uk/2/01/PMKern.pdf, Paper presented at the conference 'Elections on the Horizon: Marketing Politics to the Electorate in the USA and UK,' 15 March 2004, The British Library, London.

40. Elihu Katz and Paul Lazarsfeld, *Personal Influence* (New York: Free Press, 1955).

41. For a review, see Gabriel Weimann, *The Influentials: People who Influence People* (New York: SUNY Press, 2000).

42. Council of the European Union, doc. 14781/1/05, subject: The European Union Strategy for Combating Radicalization and Recruitment to Terrorism, 24 November 2005, p. 3.

43. Council of the European Union, subject: Presidency Conclusions, doc. 10633/06, p. 5.

44. Council of the European Union, subject: Council Conclusions on Cooperation to Combat Terrorist use of the Internet, doc. 8457/2/07, p. 3.

45. George Dafermos, "Management and Virtual Decentralized Networks: The Linux Project," *First Monday* 6 (11), available at http://www.firstmonday.org/issues/issue6_11/dafermos/

46. Google also provided its hardware and software system, which includes proprietary algorithms that intelligence IT managers praise highly, to the Army, the Energy Department, and other agencies in the intelligence world.

47. Stew Magnuson, "Wikipedia for Intel Officers Proves Useful, National Defense Magazine," *National Defense* (November 2006), available at http://www.nationaldefensemagazine.org/issues/2006/November/SecurityBeat.htm#

48. Felix Stadler and Jesse Hirsh, "Open Source Intelligence," available at http://subsol.c3.hu/subsol_2/contributors2/stalder-hirshtext.html

49. On the use of virtual and physical open source intelligence counterterrorism system, see Katharina von Knop, "Institutionalization of a Web-focused, Multinational Counter-Terrorism Campaign: Building a Collective Open Source Intelligence System," in *Response to Cyber-Terrorism* (Washington, DC: NATO IOS Press, 2008).