

The Internet and Terrorism
April 2005
James A. Lewis
Center for Strategic and International Studies

The final version of this article was published in the *Proceedings* of the 99th Annual Meeting of the American Society for International Law

Terrorists take advantage of commercial networks for communications, finance, and transportation to act on a global rather than national or regional scale. These networks allow them to maintain a presence and to coordinate and mount operations that would have been beyond their capabilities before 1990. The Internet is one of these commercial networks. It is a vital resource for global terrorism. An initial reaction to the statement that the internet is a vital resource for terrorism might be to urge that we seek to restrict their use of it. This reactive approach should not be the principle guide for government policy.

Islamic groups were not the first terrorist organizations to turn to the Internet, but they quickly learned the value of the new technology. Chechen rebels were the “early adapters” among Islamic groups. Pakistan has become a primary center for Internet talent (from groups such as Lashkar-e-Taiba) for the fundamentalists. Internet use is one of the characteristics of fundamentalist terrorism.

The Internet enables global terrorism in several ways. It is an organizational tool, and provides a basis for planning, command, control, communication among diffuse groups with little hierarchy or infrastructure. It is a tool for intelligence gathering, providing access to a broad range of material on potential targets, from simple maps to aerial photographs. One of its most valuable uses is for propaganda, to relay the messages, images and ideas that motivate the terrorist groups. Terrorist groups can use websites, email and chatrooms for fundraising by soliciting donations from supporters and by engaging in cybercrime (chiefly fraud or the theft of financial data, such as credit card numbers).

However, the Internet is not a weapon that appeals to terrorists. A desire to inflict “Electronic Pearl Harbors” is not the source of their interest in the Internet. There have been many terrorist attacks, but none has involved cyber weapons. Cyber weapons are less effective and less attractive than other arms in the terrorist arsenal. Terrorist seek violence and bloodshed. Above all, terrorists prefer explosives. An Al Qaeda training manual, “Military Studies in the Jihad Against the Tyrants” states that explosives are the preferred weapon because “explosives strike the enemy with sheer terror and fright.” In their actions, terrorists want to make a political statement, and to inflict psychological and physical damage not only on their victims but on the larger civil society. Cyber attacks would not have the dramatic and political effect that meets the psychological needs of terrorists to commit violent acts. Finally, the vulnerability of potential targets to cyber attack is overstated. Cyber-terrorism has really been cyber-graffiti.

Cybercrime is potentially a greater concern for terrorist use of the Internet than cyber-terrorism. There is some evidence that terrorist groups are making increased use of the internet to commit cybercrimes. Cybercrime is an attractive replacement to the bank

robberies or hijackings that terrorists used in the past to finance their operations because it holds very little risk. Cybercrime is an increasing problem, but our response to cybercrime should be the same regardless of whether the perpetrator is a terrorist or a criminal. An effective response to cybercrime lies outside of counterterrorism and would emphasize network security measures such as better authentication, the use of encryption for stored data, and strong intrusion and reliability measures. Above all, it would emphasize a robust law enforcement response in this new arena for crime.

The primary use of the internet by terrorist involves information: obtaining it, disseminating it, and using it to advance their goals. While email and chatrooms are crucial organizational and communications tools, the website is the primary informational 'weapon.' Websites are used for propaganda, recruitment, and fundraising. They provide terrorist groups with an audience for their message many times larger than they could reach before the advent of a cheap, decentralized global communications network.

Terrorist websites use the imagery and symbols of victimization and empowerment to spread their message. These displays are effective in arousing the emotions of supporters and potential supporters. The West (particularly the U.S.) victimizes the Muslim world, and the website imagery shows innocent Muslim wounded and dead, destruction of homes, Jerusalem, Abu Gharaib. The response to these 'outrages' lies in terrorism (or, in the view of the authors, the defense of Islam) and there are images of AK-47s, knives, U.S. casualties and the September 11 attack on New York. Terrorists portray themselves as the defenders of fundamentalist Islam and the Arab cause. The symbolism is of a Muslim world that is under attack by the nonbelievers (led by the U.S.), where only the terrorists can resist and overcome these opponents. The classic splash page for a terrorist website would show an F-15 in the upper right corner angling down in attack and Osama, clutching an AK-47 and gazing or pointing confidently upward in response.

There are hundreds, and possibly thousands, of websites maintained by terrorist groups and their supporters. The ability to use an announcement or imagery on a website to gain the attention of global news networks reinforces and multiplies the effect of Internet use. Estimates range from 700 to 4000. These websites play an essential role in creating a global presence. The location of the websites is ephemeral. A July 2004 survey of terrorist websites found them to be located in Iran, Canada, the U.S., the Netherlands, Lebanon, Russia, Hong Kong, and the UK. Terrorist websites are a global phenomenon. In most cases, the hosting ISP does not know the nature of the website. Terrorist webmasters have also demonstrated an ability to use poorly secured sites as unwitting host – in one example the State of Arkansas's Transportation Department provided hosting for a terrorist website for a period of weeks.

One of the characteristics of terrorist websites is their ability to manage rapid changes of internet address. When authorities force a site to move, informal networks based on chatrooms or email inform the group's supporters of the new network address. This "word of mouth" system to distribute new addresses to audience is very effective. It reinforces a sense of inclusion in the group and of success in defying the authorities. It also raises the question as to whether we are better off knowing an address or forcing a website to move and then having to hunt for them.

In only a few instances, does the temporary disruption of forcing a website to change its address actually degrade terrorist performance. In considering a policy framework for terrorist use of the internet, we may want to ask what activities should we tolerate and what should we try to restrict; where efforts at restricting terrorist use of the Internet can be effective; whether the cost of restriction outweigh the benefits, and what alternatives to restriction are available. Some activities are clear targets for law enforcement or other actions aimed at restricting terrorist use of the Internet. These include fundraising, recruitment, the provision of training materials or “how to” manuals, criminal activities or hate crimes (although difference between the international and U.S. definitions of what comprise a ‘hate crime’ can complicate this – the U.S. standard is more careful in protecting speech). Official support for a terrorist website by a government should be a cause of immediate action.

However, the flexibility provided by the Internet makes countermeasures difficult. Shutting down a press or radio station is easy compared to shutting down a website, as the website requires little equipment or facilities, can purchase hosting services from thousands of providers around the world, and these service providers could be located in another country or another continent. The key to effective countermeasures is to monitor email and chatrooms, but this has posed a particular problem because of civil liberties concerns, a lack of analysts capable of reading Arabic, and because of technological difficulties with surveillance.

The risk of overreaction should also be a constraint on any reaction to terrorist use of the Internet. It is important to remember that we gain more from openness, in political legitimacy and economic creativity than we lose from allowing terrorists to have access to information. Efforts to remove information from the Internet may do more damage to democracies than to the terrorists. Similarly, restrictions on speech and debate on the internet must also be carefully limited, just as the ability of law enforcement or security forces to constrain free speech (in telephone conversations or in publishing) is limited. Censorship is not a tool of democracies and eavesdropping is tightly regulated to avoid abuse by governments. The same approach should apply to the Internet.

The measure for responses to terrorist use of the internet should be to gage which tactic is more likely to degrade enemy performance. These tactics fall into two general categories: suppression and engagement. When people think of responding to terrorist use of the Internet, suppression is often the first thought (shutting down websites, banning chatrooms, closing email accounts, et cetera) but we should not assume that suppression is the most effective tactic. Terrorists exploit the openness and commitment to civil liberties found in western societies, but when they use the Internet, they are using a technology where we have an advantage, both in terms of technology and in terms of being more open to debate. Counterterrorism efforts need to ask how best to exploit the home field advantage.

Exploitation has two meanings. The first is to make terrorist use of the internet a tool to gather information on these groups and to disrupt their activities through intelligence operations. These could include ‘false flag’ operations to provide misinformation, identify supporters and members of terrorist groups, and to divert funds. This is primarily an intelligence function. The second meaning is to exploit terrorist dependency on the Internet as a communications tool to engage them in the battle of ideas. One of the reasons

that terrorist use of the Internet is seen as a problem is that U.S. efforts at public diplomacy efforts are feeble. Our goal should be to win this battle not by suppressing the terrorists' ideas but by exposing their idiocy. Saudi Arabia, not usually a leader in free speech on the internet, took the step of having clerics go into chatrooms and debate them in order to undercut the terrorists' legitimacy and support. The internet provides terrorists with an avenue into the minds of their supporters and the unconvinced; this same opening is also vulnerability for them in the battle of ideas.

The Internet is an enabler of global terrorism. This cannot be undone. The internet is, however, a creation of the west that the terrorist so strongly detest. It should not be beyond our means to use the Internet against them more effectively than they use it against us. To design effective policies for countering terrorist use of the internet requires a focus on two simple goals: exploit the home field advantage, and win the debate rather than try to suppress it.