Malicious Internet Use and Homeland Security

Wolfgang W. Bein
University of Nevada
Howard R. Hughes College of Engineering,
School of Computer Science
Las Vegas, Nevada 89154, USA
E-mail: bein@cs.unlv.edu

Abstract

The advantages of speed, security and connectivity, which Information Technology brings to businesses and government, are increasingly empowering international terrorist groups. Tools previously only available to national security agencies are increasingly at the disposal of terrorist cells and rogue nations. Powerful encryption methods are now widely available. Anonymizers, which remove the computer's identifying information so that IP addresses are hidden and cookies and scripts are blocked, represent a new advance in Internet technology. These developments raise important questions about the risks of privacy. The Internet offers terrorists an intelligence and reconnaissance tool, giving wide access to logistical data, and - as part of the globalization aspect of the Internet - cultural resources can benefit terrorist activity, teaching customs and mannerisms of the target society.

1. Introduction

There is great enthusiasm about our new digital world; perhaps very much similar to the excitement experienced over nuclear energy throughout society during the middle part of the previous century. Much has been made of the possibility of terrorists using Information Technology for cyber attacks of various kinds, including malicious denial of service attacks through viruses and worms, which could indeed cause societal harm [1]. As much as such cyber warfare does indeed present a clear and present danger, a different dark aspect of cyberspace has received much less attention.

Traditionally, computer scientists have tended to view the quest for Internet privacy as an indisputable goal. Computer and network security tools in tandem with powerful encryption methods are now widely available to the public. Anonymizers represent a new advance in Internet technology: Such anonymizers are used to remove the computer's identifying information so that IP addresses are hidden and cookies and scripts are blocked. As a result terrorist organizations can operate with the knowledge that their communications are entirely protected.

Many of the tools that were previously only available to legitimate governments are now accessible to terrorist cells and rouge nations. Certainly, since the events of September 11, it has become apparent that Information Technology has the potential to serve as a conduit for terrorist conspiracies.

But beyond the technical there is a profound societal and cultural aspect: The Internet has redefined the meaning of neighborhood, enabling terrorist cells to communicate over long distances, setting up communities of interest, and maintaining terrorist networks that function much like the Internet itself. The digital world gives a new sense of place, where borders play a lesser role; cultural context is weakened, making it easier for foreign terrorist groups to act in their targeted countries.

2. Anonymation and Encryption

Privacy refers to the ability of individuals to protect information about them. *Anonymity* is the privacy of identity and it can be:

> Persistent anonymity (or pseudonymity), where the user maintains a persistent online persona ("nym") which is not

connected with the user's physical identity ("true name"), or

One-time anonymity, where an online persona lasts for just one use.

The key concept here is that of linkability: With a nym, one may send a number of messages that are all linked together but cannot be linked to the sender's true name. By using one-time anonymity for each message, none of the messages can be linked to each other or to the user's physical identity.

Some of the more routine uses of persistent anonymity are in message-oriented services, such as email and newsgroup postings. Here, the two major categories are those of sender-anonymity, where the originator of a message wishes to keep his identity private, and of recipient-anonymity, where the recipient desires to enable replies to a persistent persona.

Anonymizers as third party proxies, usually remove identifying information, hide host names and IP addresses, and block cookies and scripts. Such anonymizers are made even more effective by the use of distributed networks of intermediate servers (named Mixes based on David Chaum's Mix-net concept [2]) on the way to the final destination on the Internet. Along these networks powerful encryption methods are employed including the Data Encryption Standard (56-bit key, or higher) or the more recent Advanced Encryption Standard. There is extensive software available using numerous servers all over the globe, suffice it to mention here the open source European JAP project [3]. Many other schemes and software packages are available, e.g., see [4], [5], as well as Figure 1.

Somewhat more exotic, but as readily available, are steganographic programs, which are used to hide data in picture files. Often messages are first encrypted before embedding. Such embedded and encrypted information is extremely hard to find and decrypt; it thus offers ample opportunity for mischievous use.

Figure 1. A Russian site displaying servers which can be used as proxies

3. Socio-Economic and Cultural Factors

Information Technology is most often associated with the vibrant economies of the first world, most notably the economies of North America and Western Europe, and perhaps Japan, and Hong Kong. It is indeed counterintuitive to acknowledge how much the World Wide Web has impacted the infrastructure of third world countries as well as countries with emerging economies.

This trend, however, is illustrated by how fast wireless technologies have leapfrogged outdated phone systems in Eastern Europe. India and Pakistan's economic progress over the last decade was largely enabled through the emergence of software industries, which relied on fast Internet access. Recently, the country of Afghanistan joined cyberspace by gaining legal and technical control of the "dot-af" domain for Afghan web sites and e-mail addresses.

Thus it comes as no surprise that the Internet and its countless web sites provide a platform for communications and propaganda of radical movements throughout the third world. It well established [6] that Chechnyan radical groups have posted their propaganda on various sites in Russian and English. (See also Figure 2.) Throughout the third world so-called "Internet-cafés" are proliferating, thereby offering ready access that is hard to trace by legitimate intelligence services.

There is a surprising extra dimension in the issue of Information Technology and terror - the

dimension of cultural side effects. As recently as twenty years ago, a foreign terrorist group would have found it substantially harder to carry out an operation such as the attacks of September 11. The 19 attackers were not residents of the United States; they were foreign intruders. And yet they were able to blend in with American society quite effectively, able to rent a car, able to lease an apartment, able to successfully get into flight school.

The Internet-generated information abundance of today was very much reserved to intelligence agencies of legitimate governments in pre-Internet times. From airline schedules to event schedules, from city maps to building floor plans, the Internet offers immediate access to detailed information. In fact, only very recently have government agencies and large corporations begun to sift through their web pages, and started the tedious process of deleting or editing sensitive information. Terrorists could take the use of Information Technology one step further, and use digital imaging to carry out surveillance of their targets well in advance and remotely.

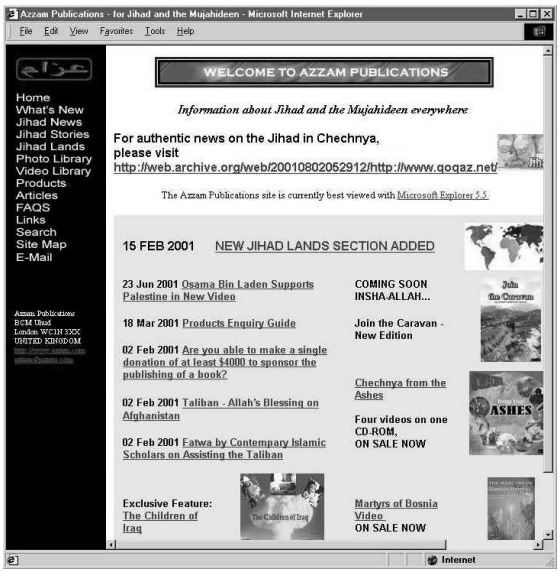

Figure 2. A pre September 11 jihad propaganda site, cached by the Internet Archive on July 20, 2001

And yet it is not such technical capability alone that makes the Internet an enabling technology. It is the power of the medium itself. Indeed, the abundance of web sites makes global culture ubiquitous. Foreign attackers can avoid cultural pitfalls of the targeted county, prepare themselves for mannerisms and local customs.

There is loss of a sense of place widely acknowledged in the literature, where the "persistence" and "gravity" of place [7] are replaced by mobility and 'an unbearable lightness of being.' Negroponte [8] foresaw this trend about a decade ago (albeit as a positive thing) when he proclaimed that the change from atoms to bits wold be irrevocable and unstoppable.

The kind of homogeneity that the Internet brings to many interactions de-emphasizes local context and culture, and thus rather benefits a foreign attacker. The Internet globalization has been beneficial in many ways, but has become discomforting when viewed in the context of terrorism.

4. Conclusions for Homeland Security

What, then, are the ramifications for Homeland Security? The answers can be categorized roughly as technical, legal, and attitudinal.

In the area of technology and research, the National Research Council [9] developed the following recommendations:

- Develop more effective machine-learning algorithms for data mining, especially across the entire plane of multi-media file types.
- Explore new methods to combine data from multiple sources.
- Create better automated tools to handle natural languages.
- Improve algorithms for image interpretation, speech recognition, and interpretation of other mixed media, including image and video processing.
- Improve tools for reasoning under uncertainty.
- Create better tools for data visualization.

Project Echelon, which is operated by the National Security Agency, is a classified reconnaissance project, designed to intercept electronic communications globally. In a recent State Department Report [10] it was pointed out that both the intelligence community leadership, as well as congressional committees have expressed determination to enhance analytical capabilities. Unfortunately, given the advances in cryptography and anonymization, a solution based entirely on technology might not be forthcoming, and in addition to signals intelligence and imagery intelligence, human intelligence will likely have to play a larger role.

In the legal arena, France, and more importantly the United States, have seen the need to regulate export of encryption software. In France, for example, the use of products with a key length of more than 128 bits requires registration with a trusted third party. In the United States export controls were put in place, which have been subsequently loosened to routinely allow export of 56-bit key DES encryption. As discussed in Section 2, some of the restrictions are merely academic by now, as encryption is widely available over the Internet.

Returning to the issue of intelligence, a number of legal obstacles to effective surveillance of terrorist groups were removed in the aftermath of September 11. The USA Patriot Act of 2001 gives law enforcement agencies greater flexibility in obtaining court orders for intercepts when foreign terrorist communication is suspected. It was also designed to facilitate greater sharing of information between law enforcement agencies and intelligence agencies. In fact, the Department of Homeland Security will soon have an Information Analysis and Infrastructure Protection division that will be responsible for analyzing information provided by law enforcement and intelligence agencies. In the future, legislation should accommodate workable solutions in a post cold war world. This might mean:

- Public privacy concerns will have to be balanced with public security concerns.
- Legitimate Security and Intelligence Agencies have to be given the proper legal tools to use Information Technology effectively.

The real change, however, might be a shift in societal attitudes towards issues of privacy. Recent events have shown that there is a distinctly dark side to encryption and anonymization. In the past, privacy has been considered a prime objective in Information Technology, and privacy pursuits have been especially strong among Information Technology professional, and most notably among computer scientists. Could it be that our concern might shift to acknowledge the risks of global privacy?

5. References

[1] C.P Pfleeger, S.L Pfleeger, *Security in Computing*, 3rd Edition, Prentice Hall, Upper Saddle River, 2003.

[2] D. Chaum. "Untraceable electronic mail return Addresses, and Digital Pseudonyms", *Communications of the ACM*, 24(2), 1981, pp. 84-88.

[3] JAP Anonymity and Privacy, http://anon.inf.tu-dresden.de/index.html.

[4] O. Berthold, H. Federrath, and M Kohntopp, "Anonymity and Unobservability on the Internet". In *Proceedings of the 10th Conference on Computers, Freedom and Privacy, ACM,* 2000, pp. 57-68.

[5] M.J. Freedman and R. Morris, "Tarzan: A Peer-to-Peer Anonymizing Network Layer". In *Proceedings of the 9th ACM Conference on Computer and Communications Security,* Washington, 2002, pp. 44-54.

[6] R. Jacquard, *In the Name of Osama Bin Laden*, Duke University Press, Durham and London, 2002.

[7] R. DeGrandpre, *Digitopia, The Look of the New Digital You*, AtRandom.com Books, New York, 2001.

[8] N. Negroponte, *Being Digital*, Vintage Books, New York, 1995.

[9] National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, The National Academic Press, Washington, 2002.

[10] R.A. Best, Jr., Intelligence Issues for Congress, Foreign Affairs, Defense, and Trade Division, Department of State, 2003.