

Threats posed by Cyber Terror and Possible Responses of the United Nations

Jonas Böttler

Delegation of Canada
First Committee on Disarmament and International Security
UNISCA

12 December 2002

Contents

Introduction	3
What is Cyber Terror?	4
Incidents related to Cyber Terror in recent history	6
Possible Scenarios of Cyber Terror	9
The United Nations and Cyber Terror	12
Conclusion	13
Bibliography	15

Introduction

The time after the fall of the “Iron Curtain” and the end of the Cold War has been called the post-industrial era, but even more used is the term of the Information Age. And indeed if the amount of information that travels around the globe today is taken into account, this term is not exaggerated. The interconnectivity of the world’s computer networks has seen a breathtaking increase in the last decade. Every year there are more and more people, private enterprises and international organizations using the internet as well as other means of information technology. The world’s telecommunication, businesses, stock-markets, international traffic systems, nearly everything is run with the help of information technology. The benefits that are provided by the growing interconnectivity are numerous and omnipresent alike, and will very probably change the way we run our daily lives drastically in the years to come.

But the Information Age has also its odds. The growth of computer networks in recent years has led to an immense dependence on these systems. Very many things that we use every day and take for granted, for example water supply, electric energy, heating-systems, oil- and gas supply, television, radio programs, telecommunication, banking systems, emergency services, traffic control, public administration and so on and so forth, function based on this technology. The more developed a country is, the more it depends on the correct and safe work of all these systems. Any intrusion, manipulation, sabotage, disruption or even destruction on one of these networks or systems will have effects which go far beyond the affection of only the attacked system itself.

The events on September 11th have put the issue of international terrorism and especially the fight against it on top of the world’s political agenda. The world learned shortly after the attacks that the terrorists had used the internet to communicate secretly in order to plan and coordinate their attacks. This increased the salience of the question about the skills and abilities of terrorist groups to misuse information technology not only for communication purposes but also with the intention to cause terror, more specifically: cyber terror.

This work is going to take a closer view on this issue. First of all the great variety of unlawful acts connected to information technology is going to be presented drawing attention to the question of what actually defines cyber terror. Then there will be a look back in recent history to examine some attacks on the internet or specified parts of it. Once some examples were given, an outlook to the future is taken to demonstrate some of the possible scenarios and their possible effects.

Finally, the work of the United Nations on this issue is taken into account, trying to identify which parts of the work on this issue have to be improved.

Last but not least the question what has to be done to deal with the threats will be addressed and which role the United Nations could play on this issue.

What is cyber terror?

The problem of defining cyber terrorism is a difficult one, perhaps even more difficult than defining “conventional” terrorism. Certainly there were many attacks on the internet in general as well as on certain special websites of private enterprises and national or international government sites, but can all of them be labeled cyber terror? What is necessary for an attack on computer networks or systems to be called an act of cyber terror?

When a closer look at “unlawful” acts in cyberspace is taken, one can distinguish basically between three different categories of attacks. Unlawful acts by states, such as espionage and all measures of state let information/digital warfare are not taken into account for this survey, the focus lies on non-state actors.

1. The first one are being launched by single persons or small groups of people, named “hackers”. They search for leaks in security systems and lock themselves into websites, databases and other sorts of networks. Once they gained access, they often just “take a look around” or post messages like: “This website was hacked by (name of the hacker or hacker group). Have a nice day”. These people hack into systems like other people do puzzles, just because they like the challenge. Sometimes these people also hack for political purposes, for example because they want to unveil information, since it is the philosophy of many hackers that all information should be freely accessible for all people. Another example are the “Electrohippies”, a group of “hacktivists”, who conducted Web sit-ins against the WTO site during their summit in Seattle in late 1999.¹ Attacks like these cause nuisance and may even result in financial losses for the attacked actor, but are not acts of terror, because they are not supposed to cause physical damage to people or create fear.

¹ Dorothy E. Denning: Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

2. Another category is the group of cyber criminals, who use their knowledge about information technology for financial gains. These groups or single actors for example hack into commercial websites where clients use their credit cards to pay their orders. They intercept the relevant data of the credit cards and use it to pay large bills and to take money out of cash dispensers. Another aspect of this kind of crime is hacking the security systems of for instance telephone cards in order to forge them and to sell them on a large scale. These kind of deeds come in a big number and are definitely cause a lot of financial losses, although it is very difficult to state how big these losses really are, since only approximately five percent of all these computer related crimes are reported to the law enforcement authorities.² Regardless of this fact these are “regular” criminal acts and no acts of terrorism.
3. The third category is the one most difficult to define, because it contains all possible unlawful acts not addressed in paragraph 1 or 2. Of special importance for this category though are all the attacks that are intended to cause as much damage and destruction as possible independent from the reasons of the attacks. One examples for this was the determined denial-of-service attack³ of February 2000 that struck CNN, Yahoo and eBay causing an estimated loss of one billion \$⁴. Another one the “Code Red” worm⁵ that struck about a million servers in July and August 2001 this time causing about 2,6 billion \$ financial damage.⁶ It is this category that also acts of cyber terror would fit in. The possible scenarios of cyber terror attacks are going to be addressed later.

There are several attempts on how cyber terror can be defined but so far there was no official definition found, which everybody could agree to. Dorothy E. Denning’s is known as a specialist on this field of study, and her definition seems to address all the important aspects of cyber terror.

According to her cyber terror is:

“generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a

² International review of criminal policy – United Nations Manual on the prevention and control of computer related crime, chapter The extent of crime and losses, <http://www.uncjin.org/documents/eighthcongress.html>

³ Denial-of-service attacks are attacks were hackers use hundreds or even thousands other computers and/or servers as „zombies“, manipulating them to send at a certain time or on at special signal a series of questions to a specific target (mostly server), causing an overload and nearly always a breakdown of the system attacked.

⁴ Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, 2000, p. 40, <http://www.techlawjournal.com/security/20001214.asp>

⁵ A computer worm is a program designed to infect other computers and/or server secretly, reproducing itself and sending itself via email to other computers/server erasing and/or manipulating files or sending them around randomly

⁶ Dorothy E. Denning: Is Cyber Terror next?, Social Science Research Council, 2001

government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.”⁷

Yet also this definition has its drawbacks. It is very difficult to draw a line between some acts that are a costly nuisance and acts of cyber terror. For example if the banking or stock exchange system are being attacked the loss of money on a big scale would be inevitable but one would probably not call this an act of terror. On the other hand is attacks like are being made on a big scale undermining people’s confidence in these system this would be identified as an act of terror. The problem though is that in the last years many attacks just occurred and the population would only seldom know who had been responsible for the attacks and what the intention of the perpetrators were. Still, a definition, even if it is not a totally exact one is necessary to define what is meant generally when the term cyber terror is used.

Incidents related to Cyber Terror in recent history

Unlike terror attacks in the real world it is very difficult to clearly identify acts of cyber terror. There is no explosive device that blew up or had to be dismantled by the police, or no cartridge cases being found. Even worse, with the growing interconnectivity in the world’s computer networks a terrorist can commit his deeds being thousands of kilometers away from his target. The more knowledge a perpetrator possesses the better he will be able to cover his traces and mislead the prosecuting authorities. As long as an attacker does not identify himself it is nearly impossible, even for a highly sophisticated intelligence agency like the American NSA, to track him and to bring him down.

But still we are able to clearly identify several acts related to cyber terror. It is interesting to know that acts of cyber terrorism are often committed responsive to events in the real world.

⁷ Dorothy E. Denning: Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

During the bombing campaign conducted by NATO against Serbia in 1999 for example, NATO web servers were subject to sustained attacks during which all of NATO's approximately one hundred web servers, hosting NATO's international website and e-mail traffic, were bombarded with thousands of e-mails, many containing damaging viruses as well as several denial-of-service attacks. The attacks managed to bring NATO servers to a standstill for several days causing serious disruptions in both internal and external communications and services.⁸

Another example from the middle east: On October 6th, three Israeli soldier were kidnapped by Palestinian terrorist. As a response, pro-Israeli hackers were launching sustained denial-of-service attacks against sites of the Palestinian Authority, of Hezbollah and Hamas.

Pro-Palestinian hackers on the other hand retaliated by taking down sites belonging to the Israeli Parliament, the Israeli Defense Forces, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and others.⁹

The sophistication, coordination and volume of these attacks are increasing tremendously. The Palestinian attacks, are even pursuing a strategy of phased escalation. According to one of the participating groups, UNITY: Phase 1 targeted Israeli government sites; Phase 2 directed attacks against Israeli economic services (like the Bank of Israel for instance); Phase 3 consists of hitting the communication infrastructure, like Israel's main Internet service provider (ISP); Phase 4 calls for a further escalation, including foreign targets.¹⁰

A very alarming incident was reported from Russia. This example also demonstrates quite impressively the threat posed by infiltration of a computer network by the help of insiders.

The Russian state-run gas monopoly, Gazprom, which is the world's largest natural gas producer and the largest gas supplier to Western Europe had been hit by hackers who collaborated with an insider from Gazprom. The hackers were said to have used a Trojan horse to gain control of the central switchboard which controls gas flows in pipelines. Although this report was made by former Russia's Interior Ministry Col. Konstantin Machabeli the company denied that this was actually true.¹¹

The USA were facing a similar problem in their own country. Over a period of several years, a series of intrusions, collectively known as Moonlight Maze, struck the USA affecting the

⁸ Michael A. Vatis: Cyber attacks during the war on terrorism, a predictive analysis, 2001

⁹ Michael A. Vatis: Cyber attacks during the war on terrorism, a predictive analysis, 2001

¹⁰ Michael A. Vatis: Cyber attacks during the war on terrorism, a predictive analysis, 2001

¹¹ Dorothy E. Denning: Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

Department of Defense, the Department of Energy, the NASA and other governmental agencies. Although officials still insist that no classified information were lost, it is undisputed that vast quantities of technical defense research were downloaded illegally.¹²

Not only insiders within a system can help terrorists to get access to key data or access to important systems. In March 2000 Japan's Metropolitan Police Department reported that a software system they had procured to track their police vehicles, including unmarked cars, had been developed by the Aum Shinryko cult. The same group was responsible for the sarin gas attack on the Tokyo subway system in 1995, during which 12 people died and more than 6.000 were injured.

At the time that this discovery was made, the Aum Shinryko cult had received classified tracking data on 115 vehicles. Furthermore, the cult had developed software for at least 80 different Japanese firms and 10 government agencies. They worked as subcontractors to other firms, making it almost impossible for the organizations to know who was actually developing their software. There is a real threat that, being a subcontractor, the Aum Shinryko cult could have installed Trojan horses. This would enable this organization to launch or facilitate cyber terrorist attacks at a later date.¹³

Learning of all these different sorts of attacks, intrusions and manipulation one can easily forget the threat which exists even when there are no such attempts. Terrorist group make use of the internet as best as they possibly can, that includes the use of the internet as a mean for recruiting new terrorists. According to US officials there were 155 to 200 Jihad sites on the Web which offer everything that is need for terrorism, including instructions on how to become a jihad warrior, prepare explosives, avoid security personnel and get discount travel flights for terrorist training camp sites. Some of these sites even provide databases showing where one can buy arms, including ammunition, along with their prices. Some sited offer bibliographies on articles dealing with guerrilla warfare and low-intensity conflict, while others report about terrorist activity and ask for donations.¹⁴

¹² Michael A. Vatis: Cyber attacks during the war on terrorism, a predictive analysis, 2001,

¹³ Dorothy E. Denning: Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

¹⁴ US Makes Cyberwar On Bin Laden, article of NewsMax.com, published 2001-02-09,

Possible Scenarios of Cyber Terror

As far as we know, there has not been a cyber terror attack that actually led to violence, injury or even death of persons up to today. This does not mean to much though, since before the attacks of September 11th nobody could have really expected or imagined that civilian aircrafts could be used as such dreadful weapons. Can the information technology be used against the population and are similar devastating results imaginable? This question is going to be addressed in this paragraph.

There are alarming signs though, especially when it comes to the Al Qaeda organization, probably the world's most dangerous terrorist network of our time. According to General Mike Hayden, head of the NSA, Osama bin Laden has better technology at hand than the NSA. He stated that: "Osama bin Laden has at his disposal the wealth of a \$3 trillion a year telecommunications industry that he can rely on. We are behind the curve in keeping up with the global telecommunications revolution."¹⁵ Although a lot has happened since this article was published, especially on the field of draining the financial sources of terrorism, the attacks on the synagogue on Djerba and on the discotheque in Bali in 2002 showed that the Al Qaeda network is able to communicate and, even worse, still able to conduct terrorist operations.

The Institute Director of the System Administration, Networking, and Security Institute (SANS), Alan Paller, is also of the opinion that there is a serious threat: „We are not ready to withstand a major attack.“¹⁶ This was proven by the NSA itself in January 2000. Being the most important US organization for the protection of information infrastructure, they suffered from a computer breakdown in the NSA Head Quarter, leaving the virtually the whole country unprotected for three and a half days.¹⁷ Whether this crash was caused by an exterior attack or not, the NSA would not say.

The possible variety of attacks against the information infrastructure and/or certain points is huge, so that only a few scenarios can be presented here.

1. Coordinated bomb attacks: cyber terrorists will place a number of computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb

¹⁵ Bin Laden Is Higher Tech Than US Says NSA Chief, article in pc-world, published 2001-02-13, <http://www.pcworld.com/news/article/0,aid,41329,00.asp>

¹⁶ Internet Vulnerabilities to Cyberterrorism Exposed, article in pc-world, published 2002-10-01, <http://www.pcworld.com/news/article/0,aid,64224,00.asp>

¹⁷ Bin Laden Is Higher Tech Than US Says NSA Chief, article in pc-world, published 2001-02-13, <http://www.pcworld.com/news/article/0,aid,41329,00.asp>

receiving each other's pattern. If bomb one stops transmitting, all the bombs detonate simultaneously. The advantage: the terrorist will be able to conduct large scale destruction on several places at the exact same time, causing fear among the population.

2. Manipulation of banking and financial systems: cyber terrorists will try to disrupt the banks, insurances, international financial transactions and the stock exchanges. If attacks like these are conducted on a larger scale, it is likely that the people of a country or a group of countries will lose all their confidence in the economic system, resulting in uncountable financial losses, perhaps even affecting the world's economic situation
3. Manipulation of pharmaceutical industry. Cyber terrorist will remotely try to get access to the formulas of medication at pharmaceutical manufacturers to alter them. If such an attack remains undetected for small amount of time, the loss of human life in a large scale will be inevitable.
4. Manipulation of traffic control systems: cyber terrorists will try to manipulate air traffic control systems, to provoke collisions between civilian aircrafts. This scenario is also imaginable for railway traffic where terrorists would try to provoke train collisions.
5. Manipulation of civilian infrastructure: cyber terrorist may try to remotely change the pressure in the gas lines, causing a valve failure and eventually resulting in large explosion and fires. Also the electrical grid is becoming steadily more vulnerable to possible attacks. They might also try to attack the telecommunication systems to disrupt communication as well as the main internet service provider (ISP) to paralyze all internet traffic.
6. Manipulation of nuclear power plants: cyber terrorist will try to get access to the control of nuclear power plants. If they manage to disrupt the cooling system this could finally result in a meltdown of the reactor's core. The effects of such a meltdown are known from the incidents in Chernobyl in the year 1986.

As already stated, these are but a few examples of possible targets for cyber terror. One has difficulties to anticipate the thinking and the mindset of terrorist, so it will stay a very important challenge to predict terrorist moves. One can predict though that terrorists, especially group like Al Qaeda will desperately try to cause as much destruction and horror as possible. That makes it very likely that they will seek a combination of physical and virtual terror. Combining these two tools would make an incredibly powerful weapon of terror.

Take the events of September 11th as an example. If the terrorists would had the ability, they would have manipulated the New York traffic control system at first to create chaos on the streets in order to make it even more difficult for rescue forces to make their way to the scene. Directly after the attack they would have attacked the local electrical power system to cut the city of from electrical supply. Right after this they would have turned of telecommunication and the internet. The result of a scenario like this would most probably be total chaos at least for several hours if not days.

This scenario may sound unrealistic and exaggerated but before September 11th also nobody would have expected terrorists to take down skyscrapers using large civilian aircraft. It is obvious that such an attack would require tremendous skills, highly sophisticated knowledge of information technology, a lot of planning efforts and also a lot of financial means making it very hard to carry out such a coordinated multi-level attack. Although it would be very hard to carry out such an attack it cannot be called impossible. Considering Bin Laden's financial background it seems at least imaginable that he could be able to hire the required specialists to launch such an attack.

The events of September 11th as they happened were a shock for Americans and people all over the world alike. Being asked later, people who were not even directly affected by these attacks often described a feeling of being helpless. This had strong negative effects on the American economy. People were just afraid to spend their money on consuming goods and were instead saving it, this also affected the world's economic situation. The international air traffic industry still suffers from these attacks, just because there are still many people who are just afraid to fly. It was only this week that United Airlines, the world's second largest aviation company had to confess their bankruptcy.¹⁸

The anthrax attacks that hit the US in the end of 2001 show another important aspect of this issue. Although only very few were actually hit by these attacks, the extensive media coverage created a climate of uncertainty and fear affecting nearly a whole country. So one could argue that the media coverage of these attacks had more effects on the public than the attacks itself. These are exactly the terrorist's intentions. Terrorism can only use its full power when after the shockwave of the attack itself a media "shockwave" covers the issue. It is sad that several persons had to die because of the anthrax attacks but these casualties were nothing compared to the hype produced

¹⁸ United Airlines reported this for the first time on Saturday, 2002-12-07. Of course the terrorist attacks were not the only for United Airlines failure, but they played definitely an important role.

by the media. The media often draws a false picture. One has only to think of how many casualties traffic accidents produce each year, with no media coverage at all. Although the media often draws incorrect and exaggerated pictures, the effects of the media coverage on terrorist attacks have to be kept in mind. This is important because it is sure that the terrorists know their business also when it comes on how to deal with the media. The media policy of Al Qaeda, were new tapes with Bin Laden's or Al Zawahiri's voice are just accidentally "found", demonstrates this. The immense interest of the media on acts of cyber terror makes it even more likely that attacks on this field will occur.¹⁹

Taking all the mentioned aspects into account it is virtually impossible to imagine all the effects that a major attack combining virtual and physical elements like the mentioned case of an "improved September 11th" could possibly have. The country being attacked would most likely be paralyzed, but for how long, nobody really knows.

The United Nations and Cyber Terror

As stated in Chapter I, Article 1, first sentence in the Charter of the United Nations, its main purposes are: "To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace."

Especially after September 11th nobody would seriously doubt that the phenomenon of international terrorism is a threat to international peace and security and that acts of cyber terrorism, as shown in the last chapter, could be too.

So it seems indeed strange, that the United Nations have not yet addressed the issue of cyber terrorism. They are aware though that information technology could be used for evil purposes in the context of computer related crime. To deal with crime in general, the UN established the Commission on Crime Prevention and Criminal Justice in 1992. The task of this commission is mainly the international action to combat national and international crime, like organized crime, economic crime, money laundering and so on.²⁰ That means the UN are mainly focusing on the deeds mentioned in the second category, concentrating on crimes committed for financial gain.

¹⁹ Dorothy E. Denning: Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

²⁰ The Commission on Crime Prevention and Criminal Justice, 2002, http://www.undcp.org/odccp/crime_cicp_commission.html

And even on this commission the issue of crime related to information technology is but a small one.

The General Assembly has also dealt with this issue and passed two Resolutions on “Combating the criminal misuse of information technologies” The first Resolution dates from the beginning of 2001²¹, the second one from the beginning of 2002²². The fact that these Resolutions were both adopted on the reports of the Third Committee shows that the aspect of international terrorism was not the most important concern when these Resolutions were passed. In fact the issue of cyber terrorism is not mentioned in any of those two Resolutions.

Only in the United Nations Manual on the prevention and control of computer related crime a very small reference to cyber terrorist can be found. In the chapter that deals with common types of computer crime the manual says: “Computer sabotage can be the vehicle....for promoting the illegal activities of ideologically motivated terrorists....”²³

That is not really much when all the mentioned threats are taken into account.

Conclusion

So far the work of the United Nations concerning the issue of cyber terror can only be called insufficient, if existing at all. On the other hand, this could turn out to be an advantage at the same time.

Since there were no casualties or physical destruction because of a cyber terrorist attack up to this point this is one of the very few occasions where the UN could act instead of being only forced to react. This is even more important when the fact that a major cyber terrorist attack *will* affect more than only one country is considered.

As proposed by the Resolution on Digital Warfare by the General Assembly of the UNISCA session 2002 the UN could (and should) install a committee on digital warfare. This would have several advantages.

First of all, it is obvious that the more countries participate in such an effort, the more information they can share. The more information is available the better can the protection the international computer networks be organized. We do not know which changes information

²¹ General Assembly Resolution A/RES/55/63

²² General Assembly Resolution A/RES/56/121

²³ International review of criminal policy – United Nations Manual on the prevention and control of computer related crime, chapter Common types of computer crime, <http://www.uncjin.org/documents/eighthcongress.html>

technology will bring in the future, but this makes it even more important to take the possible risks into account.

This mentioned committee could be a central point to gather information from national intelligence services and authorities as well as from non-state actors such as “good” hacker groups or private enterprises. A think tank within this committee could start working then, constructing possible scenarios of cyber terror attacks as well as their countermeasures.

This think tank should also formulate certain standards to make sure that all networks that are being used have at least a common minimum security standard. This is very important, because most people do not know that a quite small number of vulnerabilities is used over and over again in the attacks on information infrastructure.²⁴

Another important aspect of this committee would be a United Nations led Computer Emergency Response Team. This team would be operational 24 hours a day during 7 days a week. In case of any attack, they could start countermeasures to contain possible damage.

The producers of software product have to be given certain security standards as well, because there is no such thing as security rules for software sold around the globe.

In the days when the United Nations were founded, information or digital warfare was unknown. It is not surprising that these issues are not at all addressed at the United Nations Charter, that has to be changed as well. Cyber warfare and cyber terror has to be given a legal framework.

Taken all these proposed measures together, they will probably not be able to prevent all possible cyber terror attacks but they will make it harder for potential perpetrators to reach their goal. And even more important: provide better protection for the world’s population in order to serve the United Nations very purposes: To maintain international peace and security.

²⁴ Internet Vulnerabilities to Cyberterrorism Exposed, article in pc-world, published 2002-10-01, <http://www.pcworld.com/news/article/0,aid,64224,00.asp>

Bibliography:

- Devost, Houghton & Pollard: Organizing for Information warfare: The truth is Out There, 1997, www.terrorism.com
- Devost, Houghton & Pollard: Information terrorism: Can You Trust Your Toaster?, 1996, www.terrorism.com
- Arquilla, Ronfeldt & Zanini: Networks, Netwar, and Information-age Terrorism, from: The Changing Role of Information in Warfare, 1999
- Denning: Is Cyber Terror Next?, Social Science Research Council, 2001
- Denning: Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, <http://www.terrorism.com/documents/denning-infoterrorism.html>
- Denning: Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000, <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>
- Vatis: Cyber Attacks During The War On Terrorism: A Predictive Analysis, 2001
- NewsMax.com Wires: US Makes Cyberwar On Bin Laden, 2001-02-09, <http://www.newsmax.com/archives/articles/2001/2/8/221142.shtml>
- Politt: Cyberterrorism: Fact or Fancy?, 1998, <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>
- Collin: The Future Of Cyberterrorism: Where the Physical and Virtual Worlds Converge, 1997, <http://afgen.com/terrorism1.html>
- National Infrastructure Protection Center: Highlights: *A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.*, 2001, <http://www.iwar.org.uk/cip/resources/nipc-highlights/2001/highlight-01-06.pdf>
- Advisory Panel to Asses Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction: Second Annual Report, 2000, <http://www.techlawjournal.com/security/20001214.asp>
- PC-World: Bin Laden Is Higher Tech Than US Says NSA Chief, 2001-02-13, <http://www.pcworld.com/news/article/0,aid,41329,00.asp>

- PC-World: Internet Vulnerabilities to Cyberterrorism Exposed, 2002-10-01,
<http://www.pcworld.com/news/article/0,aid,64224,00.asp>
- International review of criminal policy – United Nations Manual on the prevention and control of computer related crime, <http://www.uncjin.org/documents/eighthcongress.html>
- www.un.org