symantec

Cyberterrorism?

by Sarah Gordon

Senior Research Fellow
Symantec Security Response

and Richard Ford, Ph.D.
Independent Consultant

INSIDE

INSIDE

Contents

Abstract

The term cyberterrorism is becoming increasingly common in the popular culture, yet a solid definition of the word seems hard to come by. While the phrase is loosely defined, there is a large amount of subjectivity in what exactly constitutes cyberterrorism. In the aftermath of the September 11th attacks, this is somewhat disconcerting.

In an attempt to define cyberterrorism more logically, a study is made of definitions and attributes of terrorism and terrorist events. From these attributes a list of attributes for traditional terrorism is developed. This attribute list is then examined in detail with the addition of the computer and the Internet considered for each attribute. Using this methodology, the online world and terrorism is synthesized to produce a broader but more useful assessment of the potential impact of computer-savvy terrorists. Most importantly, the concept of 'traditional' cyberterrorism, which features the computer as the target or the tool is determined to be only a limited part of the true risk faced.

Finally, the authors discuss the impact this new view of cyberterrorism has on the way in which one should build one's defenses. In particular, the breadth of the issue poses significant questions for those who argue for vertical solutions to what is certainly a horizontal problem. Thus, the validity of special cyberterrorism task forces that are disconnected or loosely connected with other agencies responsible for fighting the general problem of terrorism is questioned, and a broader, more inclusive method suggested. Keywords: cyberterrorism, terrorism, computer security

Introduction

If you ask 10 people what 'cyberterrorism' is, you will get at least nine different answers! When those 10 people are computer security experts, whose task it is to create various forms of protection against 'cyberterrorism', this discrepancy moves from comedic to rather worrisome. When these 10 people represent varied factions of the governmental agencies tasked with protecting our national infrastructure and assets, it becomes a critical issue. However, given the lack of documented scientific support to incorporate various aspects of computer-related crime into the genre 'cyberterrorism', this situation should not be surprising.

Despite copious media attention, there is no consensus methodology by which various actions may be placed under the nomenclature 'cyberterrorism', yet the term clearly exists in common usage. The term, first coined in the 1980s by Barry Collin (Collin, 1997), has blossomed in the last several years: "Protect yourself from the cyberterrorist"; "Insure yourself against cyberterrorism"; "Funding forthcoming to fight cyberterrorism" (Hamblen, 1999; Luening, 2000).

All of these sound nice, but the reality is that the reader, solution provider, or defender is often left to his own devices as to what the term actually means and thus what solutions should be created (or implemented). *When a government's or corporation's entire infrastructure may be at stake, subjectivity is useful but may not be the best evaluative tool.*

At the same time, research of this phenomenon shows that cyberterrorism cannot easily be defined. This creates a Catch-22 situation: the thing cannot be defined — yet without defining it, one cannot 'know' what it is one is fighting and hence come up with a good solution. Furthermore, even when there is an operational agreement on terms, if an attack/security event does not fit into one of the (often narrowly defined) categories, funding (and consequently investigation or technical remedy) may not be forthcoming.

For example, recently terrorists used a computer in Delray Beach, Florida to make their travel plans and purchase tickets, as well as using public library computers in the same town (Holland, 2001). How large the role computers played in the organization and execution of the attacks is, at this point, unclear, but the conclusion is obvious: computers and, in particular, the Internet, played a key role in the execution of the September 11th attacks. This concept is critical in evaluating the true problem we face in the virtual world: the use of computers in terrorist acts. While there are possible technical solutions that would have made this particular scenario more difficult, this task does not currently fall under the auspices of any government agency tasked with fighting cyberterrorism. Furthermore, as each of the actions cited above was not necessarily illegal prior to the attack, detection and prevention is made all the more difficult.

The most widely cited paper on the issue of Cyberterrorism is Denning's Testimony before the Special Oversight Panel on Terrorism (Denning, 2000). Here, she makes the following statement:

> *Cyberterrorism is the convergence of terrorism and cyberspace. It 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 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.*

While Denning's definition is solid, it also raises some interesting issues. First, she points out that this definition is usually limited to issues where the attack is against "computers, networks, and the information storied therein", which we would argue is 'pure Cyberterrorism'. Indeed, we believe that the true impact of her opening statement ("the convergence of terrorism and cyberspace") is realized not only when the attack is launched against computers, but when many of the other factors and abilities of the virtual world are leveraged by the terrorist in order to complete his mission, whatever that may be. Thus, only one aspect of this convergence is generally considered in any discussion of cyberterrorism — an oversight that could be costly. Second, it is very different from the definition that appears to be operationally held by the media and the public at large.

Given the Augean task of attempting to define cyberterrorism, one way we might approach the task of understanding it is to throw away the very idea of defining it at all, and instead begin by breaking it down into its fundamental elements — each of which can be examined and used as a foundation for developing solutions which may be technical, legal, social, educational, or policy driven. After all, a word is meaningless in and of itself — it is only the relational concepts that the word conveys that imbue the utterance with meaning.

As 'cyberterrorism' relates to 'terrorism' a logical first step might be to look at the functional elements present in some operational definitions of 'terrorism'[1].

The United States Federal Bureau of Investigation (FBI) defines terrorism as, "The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (FBI, 2002).

The United States Department of Defense (DOD) defines terrorism using a slightly broader brush, calling it "the unlawful use of, or threatened use, of force or violence against individuals or property, to coerce and intimidate governments or societies, often to achieve political, religious or ideological objectives" (DOD, 2002).

The United States Department of State (DOS) definition states that terrorism is "premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents" (DOS, 2002).

These varied operational definitions exist as a function of the individual organizational roles and tasks which are assigned to employees/agents. Thus, as these roles and tasks vary, the concepts of terrorism continue to vary.

The terrorism matrix

When terrorism is examined in view of these definitions, there are some pervasive elements: people (or groups), locations (of perpetrators, facilitators, victims), methods/modes of action; tools, targets, affiliations, and motivations[2]. Examples are shown in Figure 1, using two groups designated as terrorist groups by the United States government: The Liberation Tigers of Tamil Eelam (LTTE) and the Aum.

	LTTE	AUM
Perpetrator	Group	Group
Place	Sri Lanka	Japan
Action	Threats/Violence	Violence
Tool	Kidnapping/Harassment	Nerve Gas
Target	Government Officials/Recruits	!=AUM
Affiliation	Actual/Claimed	Actual/Claimed
Motivation	Social/Political Change	World Domination

Figure 1: Terrorism matrix by group and attribute.

When we examine the elements in these categories in terms of the definitions provided by the government agencies, we see there is congruence between the terrorism event and the definitions used by the various agencies tasked with providing protection. This congruence is a good thing, as it results in people tasked with defense being able to determine that certain functional tasks (building blocks of modeling solutions) fit within the definitions used within their agencies/organizations.

For example, as mentioned above, the United States Department of State (DOS) defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents". Thus, the activities of both of these groups fit the DOS criteria for 'terrorism'.

Integrating the computer into the matrix of their traditional terrorism introduces some interesting effects and problems, as we see when we consider two groups, the LTTE and Aum referenced in Figure 2. Note how the scope of 'terrorism' changes within each cell due to the addition of the computer.

1. It is worth noting that there are over 100 definitions; examining them all is beyond the scope of this paper.
2. Note that desired and actual outcome play a role as well. Future 'performance' in the theatre of terrorism is likely to be based to some degree on 'audience reaction'. This is integral to the discussion, but beyond the scope of this short paper.

	LTTE	AUM
Perpetrator	Group/Individual	Group/Individual
Place	Sri Lanka/London/Australia/ Worldwide	Japan/US/Worldwide
Action	Threats/Violence/Recruitment/ Education/Strategies	Violence/Recruitment/ Education/Strategies
Tool	Kidnapping/Harassment/ Propaganda/Education	Nerve Gas/Education
Target	Government Officials/Recruits	!=AUM
Affiliation	Actual/Claimed	Actual/Claimed
Motivation	Social/Political Change	World Domination

Figure 2: Matrix of terrorism with inclusion of the computer.

In this model, not all of the elements are congruent with functional tasks assigned to given agencies. Thus, 'terrorism' can take place within these same groups that is not within the scope of investigation, etc. This is clearly a major problem, and one that merits further investigation. Therefore, let us look very briefly at the various sorts of issues the inclusion of computers introduce to the concept of terrorism. This is obviously an extremely complex task; each area will be considered in depth in future research, and as part of the IFIP World Computer Congress workshop on Cyberterrorism (WCC, 2002).

PERPETRATOR

Interactions between human beings are complex; while the obvious solutions gravitate toward monitoring, we are concerned with virtualization of interactions, which can lead to relative anonymity and desensitization. Topics of interest include methods to measure and diminish the impact of computer-mediated interactions on potential recruits and the ability for defenders to use virtual identities to influence intra- and inter-group dynamics (dissension, 'behind the scenes' communication and destabilization).

PLACE

Location exists as an element, but is not a 'required' element in traditional terrorism in that an event does not have to occur in a particular location. Thus, whether an act is virtual/virtual, virtual/real world or real world/virtual is of interest only as factor in modeling solutions. In addition, the Internet has introduced globalization of the environments.

Actions that take place in virtual environments have demonstrably had real world consequences. An April Fool's Day hoax posted to Usenet demonstrated this when claims of the resignation of Canadian Finance Minister Paul Martin resulted in the decrease in value of the Canadian dollar (Reuters, 2002).

ACTION

In traditional scenarios, terrorist scenarios typically are violent or involve threats of violence. While there have been many studies of violence in the physical world, more research is called for in terms of 'violence' as a virtual phenomenon. Violence in virtual environments is a relatively new field, with many unanswered questions. These open issues include the psychological effects of traditional real-world violence portrayed in virtual environments, possible behavior modification resulting from

violence in virtual environments, physical trauma from virtual violence and the use of virtual violence in military training (Stone, 1993; Whiteback, 1993). However, despite the prevalence of traditional violence portrayed in virtual environments, 'cyberviolence' is still very much an unknown quantity. For example, destruction of someone's computer with a hammer constitutes a violent act. Should destruction of the data on that machine by a virus also be considered 'violence'? Perhaps violence should be considered in terms of hostile action, or threat thereof?

TOOL

There are an almost uncountable number of ways that the terrorist can use the computer as a tool. Facilitating identity theft, computer viruses, hacking, use of malware, destruction or manipulation of data all fall under this category.

These uses of the computer, when combined with 'computer as target' form the 'traditional' picture of cyberterrorism. These will be discussed in more detail later in the section Computers: The Weapon of the Cyberterrorist.

TARGET

There are a large number of potential targets that involve, either directly or indirectly, computers. Consider, for example, the impact of Personal Identity Theft. While the incidence of identity theft is comparatively low, the impact of theft upon the unfortunate soul whose ID is stolen can be large: terrorists could use the stolen identity to mask their work, carrying out certain operations under their target's name, not their own.

This would help evade detection by authorities, as well as potentially acting as a 'signal' that an identity or operation had been compromised. The Internet, especially the essentially useless authentication provided by email, provides the perfect breeding ground for identity theft.

Another interesting twist on this scenario is that of 'virtual' identity theft. For example, many users have multiple online personalities or profiles. Conceptually, there may be reasons why a terrorist would benefit from stealing a user's online identity. Attacks could be as trivial as exploiting trust relationships with other users when logged in as the stolen identity, to planting of Trojans etc., via 'trusted' email.

Similarly, the rise of online stock trading and stock message boards has created an environment in which it is possible to deliberately manipulate a stock price (perhaps via a stolen identity). A terrorist could use such techniques as a funding source, or even attempt to move the markets towards chaos. Thus, a well organized virtual attack upon a bank or corporation's stock rather than the bank or corporation itself, could in fact prove to be highly effective.

In the opinion of the authors, all of the attacks mentioned above are more likely to be successful when carried out against individual users or corporations rather than governments. However, governmental control currently relies heavily on the stability of the overall economy; thus economic destabilization is a viable attack against a government as well as the attacked third-party entity.

Using the terrorism matrix, effective solutions for computer as 'target' can be conceptualized and designed — but these will be useless overall unless problems (technical, social, legal) arising from the interaction of computer with every cell of the terrorism matrix is addressed. If I can buy a ticket for an unknown 'friend' in Bulgaria to fly to London and blow up the London Eye, antivirus software on the computer controlling the London Eye is of little relevance.

AFFILIATION

It is possible for a person to read all about a given cause and chat with proponents of the cause without ever leaving the safety of his or her own home. New recruits can thus become affiliated with a terrorist group, commit to carrying out given actions, all without ever actually coming into contact with another human being. At the same time, these loose affiliations can complicate investigations and confuse media reports. Additionally, the introduction of computing technology facilitates alliances between groups with similar agendas; this type of affiliation can result in strengthening of the individual organizations as they can immediately acquire access to the information resources of their allies.

MOTIVATION

Political, social, and economic changes are the motivations present in real-world terrorism. Combining a dependence on Internet-connected systems for banking and Ecommerce with the ability of anyone with a desire and readily available tool to disrupt these areas, results in a situation that is all too clear: unless steps are taken to significantly reduce risks, disaster is inevitable. Even with the best risk reduction, there are still likely to be problems.

Pure cyberterrorism

The concept of 'pure' cyberterrorism — that is, terrorism activities that are carried out entirely (or primarily) — in the virtual world is an interesting one. The Internet provides many different ways of anonymously meeting with 'like minded' individuals in a (comparatively) safe way. Furthermore, a successful cyberterrorism event could require no more prerequisite than knowledge — something that is essentially free to the owner once acquired, and an asset that can be used over and over again. Thus, it would be possible that such an environment could facilitate the creation of entirely new terrorist groups — no monies would be required for actions, and members could organize themselves quickly and easily in the anonymity of cyberspace. This is very different from certain examples given above, where the computer can aid the task of the terrorist, but 'real' resources are still required to execute the plan. It is this pure cyberterrorism that most writers mean when they discuss the dangers posed by the cyberterrorist, and this compartmentalization poses a significant barrier to our ability to protect ourselves.

One question that has not been adequately addressed in the literature is what might this terrorism look like. At this time, there is much confusion, based largely upon lack of agreement in definitions. However, using 'traditional' terrorism models should help make the situation more suited to analysis, and this is certainly a topic for future research.

Terrorism as theater?

Within the terrorism literature, a common metaphor is that of terrorist incidents as theater. Those concerned with terrorism and the media frequently find the staging of incidents, the publicity sought, and the manipulation of the audience primary themes in their analyses. To this end, WWW sites can bring publicity, and this is indeed a growing trend. Additionally, currently almost half of the 30 groups on the State Department's list of terrorist organizations have their own websites, which can be used to solicit money for their various causes or disseminate coded messages, either explicitly or steganographically.

The functional tasks of the group having a WWW presence may be distributed among several sites; it is relatively easy for a terrorist organization to solicit funds for operations via the WWW (the ultimate penetration of Ecommerce?), promote their cause, as well as recruit would-be operatives while maintaining somewhat of a perceptual distance between the tasks. Finally, the relative anonymity provided to those accessing information via the WWW also helps distance those sympathetic with the cause from those actively fighting for the cause in ways that may be objectionable to the sympathizers.

The new terrorism

New terrorist organizations are highly funded, technologically articulate groups capable of inflicting devastating damage to a wide range of targets. While most published work in the computer industry has focused on the impact of the computer as target (pure cyberterrorism) it is our belief that the real danger posed by the synthesis of computers and terrorism is not only the insertion of computer as target in the terrorism matrix, but in many of the other areas, too.

The current narrowness of focus poses a significant risk to US infrastructure. By being too concerned about one particular part of the matrix, we are apt to let our guard down in areas which may be more critical. A forward-looking approach to terrorism that involves computers is highly contextual in its basis. Traditional antiterrorism defenses must be deployed, but these countermeasures must fully take into account many of the virtual factors that we have outlined in this paper.

If the events of September 11th teach us one thing, it is that we should always consider the 'big picture' of the overall terrorist threat, rather than view one aspect in isolation. The 'cyber' aspects of the puzzle must be woven throughout the picture, not simply confined to one cell. To view a problem with too narrow a perspective is to invite anarchy into our lives.

Computers — the weapons of the cyberterrorist

Following on from the discussions above, it becomes obvious that the most likely 'weapon' of the cyberterrorist is the computer. Thus, one might ask, are we arguing that one should restrict access to computers, just as access to explosives is restricted? Not quite, but close. We believe that the stockpile of connected computers needs to be protected. There are many laws that define how one should protect a firearm from illegal/dangerous use. The mandatory use of trigger locks, though controversial, has been put forward to prevent danger should the gun end up in the wrong hands. Similarly, powerful explosives like C4 are not simply sold over the counter at the corner store.

Explosives and guns are certainly not entirely analogous to computers. A better analogy might stem from the concept of an 'attractive nuisance'. For example, a homeowner shares some responsibility for injury caused by a pool on his property — it is deemed an attractive nuisance, and as such, the innocent should be prevented from simply being attracted and harmed.

Thus, there are many instances of laws which already discuss damage done by/to a third party from the intentional/unintentional misuse of a piece of corporate/personal property. The application of these laws or the definition of 'misuse' with respect to computers seems unclear. However, there is a need for clear laws and standards which require operators of large networks of Internet-connected computers to exercise appropriate due diligence in their upkeep and security.

To this end, we believe that there is an urgent need for definition of a minimum standard of security for computer networks. The definition of such a standard has far reaching implications not only for the usability of America's technology foundation, but the security of corporations and indeed of the nation itself. By formalizing an industry best practice guideline, companies will have a clear understanding of what must be carried out.

Clearly, such a guideline is a moving target, but its inception would allow the structuring of a valid and robust posture against both terrorist threats and other hostile entities. Such a set of minimum standards would have to be easily and affordably supported by the security/application vendors themselves, rather than relying on individual users needs/requirements to drive the best practice guidelines.

This is not exactly a novel concept. International standards have been developed in other areas where safety and security are a concern. Consider the airline industry. There are international guidelines for airport safety; in cases where these standards are not met, consequences range from warnings to prohibited travel. The needs for such changes, and how a due diligence standard could be created are subjects of future research. However, it seems clear that such standards are urgently needed.

FUTURE RESEARCH

Certainly there are many unanswered questions. Most people, governments included, consider cyberterrorism primarily as the premeditated, politically motivated attack against information, computer systems, computer programs, and data by sub national groups or clandestine agents.

However, as we have seen, the real impact of the computer on the terrorism matrix is considerably wider. By limiting our understanding of cyberterrorism to the traditional 'computer as target' viewpoint, we leave our nation open to attacks that rely on the computer for other aspects of the operation.

Even when considering the purely virtual impact of cyberterrorism, the approach is not adequately thought out. For example, consider an act that incorporated a desire for political change with the release of an otherwise benign computer virus within which an antigovernment message is embedded. For example, if the Melissa virus had contained the message "The Clinton regime must be defeated", would it have been the act of a terrorist instead of a misguided computer programmer — and would the ultimate punishment really fit the crime if that programmer were meted out the same punishment as the terrorists responsible for blowing up a US embassy?

What role does incitement to violence play? A swastika emblazed on the WWW site of UK politician John Major may constitute some violation of a law, but probably does not constitute terrorism. But what if swastikas were digitally painted on the WWW sites of every Jewish organization in the country? What if a message was included inciting people to violence against their Jewish neighbors? Would these acts fall under the domain of 'using violence'? What if these images and messages were put there by a known terrorist organization? Would the act take on the characteristic of the perpetrator? Would these acts be hate crimes or cyberterrorism? Whence falls 'jurisdiction'?

Given the lack of physical boundaries in the virtual community, does a group's physical location have any bearing on whether or not they may be considered a sub-national group? What is a 'national group' in cyberspace anyway? Which government agency deals with *that?*

What constitutes combatant targets in virtual environments? Consider the 1998 response by the Pentagon to civilian target computers as a response to Floodnet protests (McKay, 1998). Is the system that automatically strikes back considered combatant? Are its owners moved from 'non-combatant' to 'combatant' based on an auto-response? Is the response perhaps engaging in 'violence'?

Some claim "terrorists and activists have bombed more than 600 computer facilities". What specific components may be considered an element of a cyber system; what differentiates these incidents from conventional terrorism? Physical property, civil disorder and economic harm are easily understood in the physical world; however, are there virtual equivalents that could lead to a broadening of the concept of cyberterrorism?

Defending against the new terrorism

Defending against terrorism where a computer or the Internet plays an important part in the terrorism matrix is very similar to defending against terrorism that does not. The regular practices (deterrence, law, defense, negotiations, diplomacy, etc.) are still effective, except that the scope of certain elements is expanded. For example, traditional strikes against military bases, targeting of key leaders, and collective punishment have been effective in traditional terrorism (Whitelaw, 1998) and certainly have potential for dealing with some aspects of cyberterrorism. These techniques are often presented, and can be to be updated to include their 'virtual' counterparts. It should be noted, however, that differences in international law and culture could make this process a complex task.

Crenshaw (Crenshaw, 1999) presented here at length, examines a summary of traditional counter-terrorist techniques:

DETERRENCE

Governments can use their coercive capacity to make terrorism too costly for those who seek to use it. They can do this by military strikes against terrorist bases, assassinations of key leaders, collective punishment, or other methods. There are several drawbacks to this approach, however. On the one hand, it can lead to unacceptable human rights violations. In addition, groups may not come to government attention until movements are so well developed that efforts to contain them through deterrent methods are insufficient.

CRIMINAL JUSTICE

Governments can treat terrorism primarily as a crime and therefore pursue the extradition, prosecution, and incarceration of suspects. One drawback to this approach is that the prosecution of terrorists in a court of law can compromise government efforts to gather intelligence on terrorist organizations. In addition, criminal justice efforts (like deterrent efforts) are deployed mostly after terrorists have struck, meaning that significant damage and loss of life may have already occurred.

ENHANCED DEFENSE

Governments can make targets harder to attack, and they can use intelligence capabilities to gain advance knowledge of when attacks may take place. As targets are hardened, however, some terrorist groups may shift their sights to softer targets. An example is the targeting of US embassies in Kenya and Tanzania in August 1998 by truck bombs. Although the attacks are believed to have been coordinated by individuals with Middle Eastern ties, targets in Africa were chosen because of their relatively lax security compared with targets in the Middle East.

NEGOTIATIONS

Governments can elect to enter into negotiations with terrorist groups and make concessions in exchange for the groups' renunciation of violence. While governments are often reluctant to do so at the beginning of terror campaigns, negotiations may be the only way to resolve some long-standing disputes.

For example, data gathering and monitoring operations of terrorist communications has typically applied to signal intelligence and fieldwork. In a virtual environment, the ability to gather information from various sources is eminently achievable in a somewhat automated manner. Specific groups can be watched easily, and computers are comparatively simple to 'bug'. All contacts that a particular user interacts with could then be tracked, and the network of communication mapped. Furthermore, much of this surveillance can be carried out over the very same network that the terrorists intend to use to facilitate their plot.

This extension, however, must be carried out with care. Consider, for example, the original US export regulations on the export of 'strong encryption' (ITAR). Under such regulations, certain encryption products were classified as munitions. While ITAR has since been replaced, the revamped 'Export Administration Regulations' (DOC, 2002), while somewhat more relaxed, continue to blacklist several countries from receiving encryption products, despite the fact that strong encryption technology is freely available via the Internet. While this law seems to be aimed at preventing the use of strong encryption by other potentially hostile governments and terrorist entities, strong encryption algorithms and implementations remain trivially available to pretty much anyone.

This classification of knowledge as munitions seems to be the ultimate (and flawed) extension of traditional anti-terrorist tactics into the virtual realm. Clearly, it is not sufficient to quickly draw analogies that are not, in fact, correct. A far better approach is to carefully consider the impact of the computer in the different cells of the terrorism matrix. For example, banning the export of encryption from just America is akin to banning the sale of C4 only on weekdays — the asset would be hardly even an inconvenience to the would be terrorist. A far better solution is to consider the safeguard in the context of the virtual world. When examined in this aspect, for example, it is reasonably clear that the original classification of encryption products as munitions is not likely to be effective. Similarly, while the use of export grade encryption can (and has) resulted in the ability of officials to read some terrorist communiqués, a restrictive "export to here, not here" ban is unlikely to succeed in any meaningful way.

A forward-looking approach to terrorism that involves computers is therefore highly contextual in its basis. Traditional antiterrorism defenses must be deployed, but these countermeasures must fully take into account the virtual factors that we have outlined in this paper.

Conclusion

The Internet was developed primarily as an unregulated, open architecture. Not only are we observing a predictable backlash to the 'corporatization' of the network, where the tools of destruction can easily be placed in the hands of the dissatisfied or malevolent people, we must also deal with the fact that the infrastructure is ideally suited to criminal activities. Some of these activities are being promoted as cyberterrorism; however, the loose use of the term is actually undermining the defense capabilities of the very corporations and governments who are at risk.

Events can be analyzed in terms of their critical factors, and only if these factors all exist can the event legitimately be called terrorism. However, that does not mean if all these factors do not exist that a corporation is 'safe'. Unfortunately, corporations are built around the premise that people will do the right thing. The fact, as we have seen, is that this is not necessarily the case.

We do not use the term 'ice pick terrorism' to define bombings of ice-pick factories, nor would we use it to define terrorism carried out with ice picks. Thus, we question the use of the term cyberterrorism to describe just any sort of threat or crime carried out with or against computers in general. At the same time, those who do insist on treating only 'pure cyberterrorism' as cyberterrorism are completely missing the true threat posed by the addition of acts in the virtual world to the terrorists' playbook. Finally, the nascent danger in the term cyberterrorism is that cyberterrorism will somehow be dealt with separately to regular terrorism. This artificial fragmentation of our defenses is likely to provide the terrorist with a significant advantage in any campaign against a nation state, and is to be avoided at all costs.

This brings us to the final point of this study: turning the tables on terrorism. As we have shown, computers can play an enormous role in terrorism. At the same time they can provide perhaps our biggest defense against terrorism if used to our advantage. However, just like as we need to understand the integration of computers with terrorism, we must examine how computers can assist in defense broadly.

This begins with the re-examination of basic beliefs about 'cyberterrorism' which must take place within academia, industry, government and defense sectors. This re-examination is, however, only the first step in combating terrorism.

Information at each level of analysis must be shared, collated and redistributed across federal, state and local government boundaries, as well as amongst industry and academia, and in some cases, the private citizenry.

Obviously, this type of endeavor is information technology intensive. In the United States alone there are over 87 000 different jurisdictions (HLS, 2002); combined with information from industry, academia and the private citizenry, this amount will increase many times over. Fortunately, one of the things computers are good at is processing information. By developing an information technology architecture that would sort, correlate and facilitate the most effective use of that information, information could be shared in a timely manner amongst these groups, some of which historically have had little, if any, communication.

While specification of design or administration of such a project is beyond the scope of this paper, we believe that using a publish and subscribe model, with a meta-information standard such as XML, data from law enforcement, government, defense and industry could be analyzed, correlated, filtered and redistributed quickly to those who need it most.This cross-disciplinary sharing of information could help practitioners create complementary defensive solutions and policies, building on shared expertise and innovation.

Additionally, a well-designed technical solution can circumvent some of the cultural problems inherent in cross-sector information sharing, by eliminating the need for the actual data to do the correlation. Some technologies have been developed which would appear to lend themselves particularly well to this sort of implementation, but practical tests are required before any conclusion can be reached (Legion, 2002).

Aside from the role of computers in defense, we must attempt to re-educate policy makers, defusing the latent danger of vertical 'cyberterrorism' defenses and replacing them with a well-rounded, integrated approach to a problem that is extremely broad. From a corporate and governmental perspective this requires a careful examination of the 'messaging' that is broadcast. How do we portray the fusion of computers with terrorism? Can the messaging be made more productive so that we can shape the mindset of our audience to one that is synergistic with a broad view of cyberterrorism?

Finally, it is impossible to neglect to mention the fact that the rapid increase in connectivity and the ultimate frailty of our national IT infrastructure coupled with the astonishing homogeneity of our computing base is a matter of grave concern. Continued focus must be put on increasing the public demand for computer security as well as the corporate awareness of the issue: whereas security flaws in widely used applications were once perceived as personal risks, we must begin to recognize the potentially global consequences of such issues in balance with the more general problems posed by the integration of computing with terrorism.

The lack of understanding of cyberterrorism, and the overall insecurity of America's networks have allowed a situation to develop which is not in the best interests of the country or computer users. The need to protect computing resources, making the job of a cyberterrorist more difficult is obvious. However, this can only be accomplished by re-examining commonly held beliefs about the very nature of computer systems and of cyberterrorism itself.

References

Collin, B., 1997. *The Future of Cyberterrorism,* Crime and Justice International, March 1997, pp.15-18.

Crenshaw, M . 1999. *How Terrorism Ends.* US Institute of Peace working group report, May 1999.

Denning, D., *"Cyberterrorism",* Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000. (http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html)

DOC, 2002. *US Department of Commerce, Export Administration Regulations* (EAR), 15 C.F.R. Parts 730-774. Sections 740.13, 740.17 and 742.15 are the principal references for the export of encryption items.

DOD, 2002. *Department of Defense Education Activity Internal Physical Security.* Department of Defense. DoDEA Regulation 4700.2

DOS, 2002. United States Code. Title 22, Section 2656f.

FBI, 2002. *Code of Federal.Regulations.* 28 CFR. Section 0.85 on Judicial Administration. July 2001.

Hamblen, *M. Clinton commits $1.46B to fight cyberterrorism* http://www.cnn.com/TECH/computing/9901/26/clinton.idg , 26 January 1999.

HLS, 2002. *National Strategy for Homeland Security.* Office of Homeland Security. July 2002.

Holland, J. 2001. *Investigators look into how library computers may have linked terrorists.* South Florida Sun-Sentineel. Miami, FL.

Legion, 2002. http://legion.virginia.edu Retrieved from the World Wide Web, August 2002.

Luening, E. 2000. *Clinton launches plan to protect IT infrastructure.* CNET, 7 January 2000.

McKay, N. 1998. *Pentagon Deflects Web Assault.* Wired, September 1998.

Reuters, 2000. *Canadian dollar in for a ride with Martin Firing.* http://biz.yahoo.com/rf/020602/canada_economy_dollar_2 .html.

Stone, V. 1993. *Social interaction and social development in virtual environments .* Teleoperators and Virtual Environments, Vol. 2. pp. 153-161.

Whiteback, C. 1993. *Virtual environments: Ethical issues and significant confusions.* Teleoperators and Virtual Environments, Vol. 2. pp. 147-152.

Whitelaw, K. 1998. *Terrorists on the Web: Electronic 'Safe Haven'.* US News & World Report, Vol.124, p. 46.

WCC, 2002. *IFIP World Computer Congress Workshop.* IFIP World Computer Congress. Montreal, Quebec, Canada. August 2002.

This article first appeared in 'Elsevier Science Computers and Security Journal'.
For more information please visit www.compseconline.com.

About the Authors

Sarah is Senior Research Fellow at Symantec Security Response. Her current research areas include testing and standards for antivirus and security software, privacy issues, cyberterrorism and psychological aspects of human/computer interaction.

She has been featured in diverse publications such as IEEE Monitor, The Wall Street Journal, and Time Digital, and profiled by PBS, ITN, and CNN International. Her work has appeared in publications such as Information Security News and Virus Bulletin; she has won several awards for her work in technology. She is a highly sought-after speaker, having presented at conferences ranging from DEFCON to Govsec.

She was recently appointed to the Editorial Board for Elsevier Science Computers and Security Journal. She is on the Advisory Board of Virus Bulletin, and is co-founder and board member of The WildList Organization International. She is Technical Director of The European Institute for Computer Antivirus Research – where she also serves on the Board of Directors and Conference Program Committee. She is a member of SRI's cyberadversary working group.

Sarah was responsible for security testing and recommendation for The United Nations, and participates in various initiatives for Homeland Security and Infrastructure Protection. She was chosen to represent the security industry in "Facts on File: Careers for Kids who Like Adventure", and is a reviewer for various technical security book publishers including Wiley publications. Her work in ethics, technology and profiling computer criminals is required coursework in various academic information security programs. She is committed to excellence in information security education, guest lecturing at Universities world-wide on topics ranging from virus writers and hackers to the truth about cyberterrorism.

Sarah graduated from Indiana University with special projects in both UNIX system security and ethical issues in technology. She is a member of the American Association for the Advancement of Science, The American Counseling Association, and the Association for Family Therapy and Systemic Practice in the UK. Prior to joining Symantec, she worked with the Massively Distributed Systems Group at IBM's Thomas J. Watson Research Laboratory in New York in the AntiVirus Research and Development Team. She may be reached at sgordon@symantec.com.

Dr. Richard Ford is one of the nation's top Internet architecture experts and an internationally acknowledged computer security specialist. Ford has lectured worldwide on the subject of computer security, and holds editorial positions for several virus and security related journals. He holds one patent and is widely published in the areas of both computer security and physics. Dr. Ford has served as Director of Research for the National Computer Security Association. He also spent two years at IBM Research's prestigious T.J. Watson Research Center, working in the Massively Distributed Systems group's High Integrity Computing Laboratory. Before being appointed Chief Technology Officer for Cenetec Ventures, Dr. Ford was the Director of Technology at Verio in Boca Raton. There he served as senior architect for the world's largest web hosting platform and was also responsible for the security of more than 200,000 web sites. He is currently working as a consultant on various projects related to computer security and e-commerce.

Dr. Ford was educated at Oxford in his native England and holds a Bachelors Degree and a Masters in Physics from that university. He went on to complete his doctorate at Oxford in Low Temperature Semiconductor Physics. He began work immediately after as an executive editor of Virus Bulletin, the world's foremost technical publication on computer viruses and malicious software.

Now an independent consultant, Ford resides in Boca Raton with his wife Sarah.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product information
In the U.S. call toll-free
800.745.6054

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.