16. Defending against cyber terrorism: preserving the legitimate economy

Olivia Bosch

I. Introduction

The main thesis of this chapter is that the means used to defend against the many commonly occurring cyber incidents can provide a strong foundation for dealing with the effects of the less frequent acts of cyber terrorism. Daily cyber security 'housekeeping' by businesses, government departments and individuals will not prevent cyber incidents, but good information security policies and business continuity plans (BCPs) for disaster recovery can mitigate the effects when such incidents do occur. Further research is required to determine how much the state, which has both the responsibility and the tools to address national security issues, can protect information assets beyond those that are owned directly by government.

This chapter examines what is meant by cyber *terrorism* and how it compares with other cyber *incidents*, how issues of attribution and BCPs could be addressed, and what kind of information security vulnerabilities are arising from new developments in the activities of business and others in the private sector.

In the latter half of the 1990s, when widespread use of the Internet and computer connectivity were still relatively new, minor computer disruptions were often deemed to be acts of cyber terrorism or the result of hacker attacks when they were not. Today, computer disruptions occur so frequently that reactions have shifted towards the other extreme, of treating them as routine occurrences and responding to them in a blasé or lax manner. These reactions often confuse or complicate analysis of what has happened and distort judgements on the choice of policies for the protection of electronic information assets.

II. Cyber terrorism

Cyber terrorism can be defined as the actual use of, or the threat to use, attacks by and on computers and related electronic information networks to intimidate or kill civilians or to cause large-scale disruption or destruction for primarily political objectives. This form of terrorism includes the use of computers and related equipment to cause mass disruption in the flow of information or services, with intent to induce fear or undermine public confidence in essential

public services and critical national infrastructure.[1] This definition of cyber terrorism is primarily derived from the definition of terrorism in general. Although there is no commonly agreed definition of terrorism, it is often described as the intentional use, or threat to use, violence to intimidate or kill civilians or incur large-scale destruction for political purposes.[2] Examining some of the characteristics of terrorism can provide insights, leading to a better understanding of the context in which cyber terrorism might occur. Unlike traditional terrorism, however, cyber terrorism has occurred so infrequently that Richard Clarke, US Special Advisor for Cyberspace Security, stated that he prefers not to use the term, favouring instead a focus on the broader concept of 'information security' or 'cyberspace security'.[3]

Concerns evoked by cyber terrorism are based on an assumption that its targets are most likely to be a state's critical information infrastructure: that is, assets which the state has a strategic responsibility to protect. Critical infrastructure consists of the essential human-built assets related to energy, communications and water supply that underpin a state's survival and well-being.[4] Critical *information* infrastructure consists of the electronic information network components of these essential assets as well as their connectivity with other essential industry and service sectors, such as transport and banking.[5]

Non-cyber terrorists have traditionally relied on the use of conventional weaponry, primarily explosives, guns and mortars. These instruments tend to have familiar and calculable effects that are readily reported by the media. As the number of media outlets has increased worldwide and with the increased span and immediacy of reporting since the late 1990s, these acts have received more public attention. Media scrutiny has not, however, prevented non-state groups, such as al-Qaeda, from carrying out terrorist acts. Nor has media attention hindered them from finding effective ways to evade counter-terrorist operations: through changing their goals and alliances (including partnerships or links with criminal groups), by creating leaderless cell structures and—since the mid- to late 1990s—by taking advantage of Internet communication and the alienating effects of globalization.[6]

[1] See, e.g., Soo Hoo, K., Goodman, S. and Greenberg, L., 'Information technology and the terrorist threat', *Survival*, vol. 39, no. 3 (autumn 1997), pp. 135–55.

[2] There is an extensive literature on terrorism. See, e.g., Hoffman, B., *Inside Terrorism* (Columbia University Press: New York, 1998); Slater, R. O. and Stohl, M. (eds.), *Current Perspectives on International Terrorism* (Macmillan Press: Basingstoke, 1988); Wardlaw, G., *Political Terrorism: Theory, Tactics, and Counter-measures*, 2nd edn (Cambridge University Press: Cambridge, 1989); and Wilkinson, P., *Terrorism and the Liberal State*, 2nd edn (Macmillan Press: Basingstoke, 1986).

[3] Clarke, R., 'Administrative oversight: are we ready for a cyberterror attack?', Briefing to the Senate Judiciary Committee Subcommittee on Administrative Oversight and the Courts, 13 Feb. 2002, reported in US Department of State, International Information Programs, Wynne, J., 'White House advisor Richard Clarke briefs Senate panel on cybersecurity', 13 Feb. 2002, URL <http://usinfo.state.gov/topical/pol/terror/02021409.htm>.

[4] On critical infrastructure protection see chapter 17 in this volume, and on critical energy system infrastructure see chapter 18.

[5] On banking see also chapter 8 in this volume.

[6] Stern, J., 'The protean enemy', *Foreign Affairs*, vol. 82, no. 4 (July/Aug. 2003), pp. 28–35.

If cyber-terrorist attacks were to occur and result in large numbers of casualties or mass disruption and destruction, they would not go unnoticed by the media. Attempted cyber-terrorist acts that have been thwarted through successful intelligence, on the other hand, would normally not be reported.

Traditional, politically motivated terrorists have tried to conduct their destructive activities on a scale that is large enough to draw media attention to their goals and to induce overreaction by governments, but not so large as to undermine any public support their group may enjoy or to provoke destructive retaliation. Terrorism is seldom the main mode of operation, but rather a tactic used in support of broader operations.[7] The scale of casualties has varied, however, depending on such factors as the objectives and conduct of the terrorist operations. For example, some cults or apocalyptic groups and groups which carry out suicide bombings may have organizational goals that require them to aim at inflicting particularly high casualties. Where cyber terrorism lies in the spectrum of the more commonly occurring types of terrorist attack is still an open question. Given the low frequency of cyber terrorism so far, it is suggested that types of electronic attack that are not obviously terrorist in intent might be used instead to *support* the more commonly occurring conventional terrorist attacks, or indeed other forms of violent conflict.

Types of cyber incident

The objective of this chapter is not to show that cyber terrorism will not occur or has not been attempted, but rather to place this relatively low-probability (albeit high-impact) event into better perspective vis-à-vis the great majority of computer and network incidents that occur from other causes. As cyber terrorism has been infrequent, it is worth noting the main causes of computer incidents. The following is a general breakdown of various types of 'incident', a term that is neutral as to cause. Further research is needed to produce a more exact breakdown which would facilitate the understanding of the dynamics of cyber incidents.

At least half of all computer incidents are not caused deliberately. These include not only accidents but also the unintentional effects of vulnerabilities arising from the mismanaged configuration of networks, software flaws (which also open the way for computer viruses), improper or poor technical or administrative implementation of information security policies (e.g., failing to update anti-virus protection or software patches), inadequately trained computer users and human error. About 75 per cent of all large information technology (IT) projects are delayed, run over budget and do not work as intended, indicating the high degree to which inadequate IT project management is likely to contribute to inadequate IT security.

[7] On terrorism as a mode of operation in violent conflicts see Stepanova, E., *Anti-terrorism and Peace-building During and After Conflict,* SIPRI Policy Paper no. 2 (SIPRI: Stockholm, June 2003), available at URL <http://editors.sipri.se/recpubs.html>.

The remaining incidents are caused by individuals with malicious, criminal or political intent, the great majority of whom are disgruntled employees—in this context also called 'insiders'.[8] Many policy and corporate decision makers or directors either do not admit to having many cyber incidents or describe a computer network disruption as the result of cyber terrorism when it is not.[9] While this may be more convenient than acknowledging the existence of bad management and consequent dissatisfied employees, it causes confusion and misguided perceptions of what is required to improve information security.

A small proportion of malicious activity is carried out by cyber criminals seeking to steal or manipulate data directly for financial gain. They rely on the critical information infrastructure being intact so as to be able to conduct their activities without risk of detection. It can also be expected that some malicious cyber activities will aim to cause disruption in support of other criminal objectives, such as extortion and blackmail (which is sometimes considered a form of terrorism, depending on the definition chosen). Violence and intimidation are increasingly being used to recruit hackers or to obtain computer passwords from employees.[10] In these cases, terrorism is, and is treated as, a criminal act.

There is also a smaller group of 'hactivists' (who conduct civil protest online) and hackers (who obtain unauthorized access to networks primarily for the sake of intellectual challenge). These groups exploit the Internet to attract media or other public attention. Unlike cyber terrorists, who also seek media attention, their intention is not to kill or cause severe damage in the pursuit of their activist or civil protest goals.[11]

The term 'cyber warfare' describes cases in which electronic computer attacks are the means used to cause disruption, destruction or casualties in time of armed conflict. However, these actions would be subject to the laws of armed conflict, which include observing the principles of non-combatant dis-

[8] See, e.g., the annual Computer Crime and Security Surveys of the US Computer Security Institute (CSI), with the participation of the San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad. They report that 60–80% of incidents have been caused by employees. For information on the 2003 edition of *Computer Crime and Security Survey* see URL <http://www.gocsi.com>. On lax employees and security, see chapter 15 in this volume. Recent CSI–FBI surveys show a rise in computer attacks from outside enterprises. Such attacks have become more numerous as connectivity to the Internet has increased and 'attack' tools have become automated. The number of incidents caused by insiders has not necessarily declined and may become more significant as 'insider knowledge' of networks is acquired by outsiders with malicious intent.

[9] Computer incidents known to result from cyber terrorism are reported to be *c.* 1% of all incidents. See Saita, A., 'Searching for cyberterrorism', Aug. 2002, at URL <http://infosecuritymag.techtarget.com/2002/aug/news.shtml>, which refers to Belcher, T. (co-author), *Internet Security Threat Report,* Symantec/Riptech, June 2002, available at URL <http://www.riptech.com>.

[10] Bell, R. E., 'The prosecution of computer crime', *Journal of Financial Crime*, vol. 9, no. 4 (Apr. 2002), pp. 309–10.

[11] Denning, D. E., 'Activism, hactivism, and cyber terrorism: the Internet as a tool for influencing foreign policy', Paper for the Workshop on the Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking, Nautilus Institute and World Affairs Council of Northern California, 10 Dec. 1999, San Francisco, Calif., available at URL <http://www.nautilus.org/info-policy/workshop/papers/denning.html>.

crimination, proportionality of force used to achieve military objectives, and other related norms.[12]

An adequate understanding of cyber terrorism requires interaction between computer programmers, who have not hitherto needed to be experts on terrorism; experts in such fields as explosives and law enforcement; and security analysts, who have not hitherto required knowledge of the intricacies of computer software programming and electronic information networks. At some organizational or policy level, different disciplines need to share insights when analysing the impact of cyber terrorism in relation to other types of cyber incident.

III. Attribution and business continuity planning

Because many types of threat may arise and many types of vulnerability become apparent when a computer incident occurs, it is often difficult to pinpoint, or attribute, its cause or origin. Sabotage by a disgruntled employee, a wire gnawed through by a rodent, a dislocated plug-in, certain weather conditions and cyber criminals are all examples of different sources or causes of the same type of outage or incident. An analogy might be made with a simplified description of an aircraft accident investigation process. There may be up to four types of team that visit the scene of such an incident: one team is sent by a manufacturer to assess a component defect in the case of liability claims; one team comes from a law-enforcement agency to investigate whether a criminal act has been committed; one team might be sent from intelligence agencies to assess whether the incident was a terrorist act; and alongside them a team from the emergency services works to rescue casualties and restore local order, sometimes disturbing or inadvertently destroying evidence that might be useful to the other teams. Although they may all be doing their professional best, the cause of the accident may be difficult to discover in a timely manner. The efforts made to avert and monitor computer breakdowns at the time of the turn of the millennium provided a dry run of the various processes available to distinguish 'millennium bug' incidents from those arising from hacking or other causes.

The mis-labelling of cyber incidents as cyber terrorism distorts the assessment of policies which should be pursued for anticipating and managing the disruptions that occur. Assuming that terrorists, and hence also cyber terrorists, seek or require media attention in order to publicize their cause, it is log-

[12] The laws of armed conflict—a body of international law with a history dating back to the past century—basically stipulate 'that weapons and war tactics must, in their application, be confined to military targets; that they must be proportional to their military objectives as well as reasonably necessary for the attainment of these objectives; and that they should not cause unnecessary suffering to the victims or harm human beings and property in neutral countries'. Goldblat, J., SIPRI and International Peace Research Institute, Oslo (PRIO), *Arms Control: The New Guide to Negotiations and Agreements* (SAGE Publications: London, 2002), chapter 17, 'Restrictions on the methods of warfare', pp. 279–98. For a list and the texts of agreements from the 1860s to the 1990s see University of Minnesota, Human Rights Library, 'Law of armed conflict', URL <http://www1.umn.edu/humanrts/instree/auoy.htm>.

ical to assume that incidents caused by cyber terrorists would be relatively likely to be brought to public attention. If terrorists repeat such incidents, the perpetrators and their method of attack could thus eventually be determined. Critical information infrastructure can be expected to be a likely target for cyber terrorists since it comprises the related national energy and communications assets that underpin state survival, the ultimate protection of which lies with government, whose policies, in turn, terrorists aim to influence.

The degree to which potential terrorist incidents can be identified beforehand should be a function of the work of the intelligence community, an asset of the state which contributes to maintaining national security. In the past, knowledge of threats to the security of a nation's infrastructure, particularly in times of crisis or conflict, would have been conveyed informally by government to the owners and operators of energy and communications infrastructure, who in turn could take precautionary protection measures. The degree to which such an information flow should now be institutionalized or made more formal is still an open question, especially if cyber terrorist acts remain relatively infrequent within the wide range of computer incidents that occur. It can be expected that the state has computer assets and technologies designed to try to thwart potential cyber terrorists, in the same way as the state has assets to try to prevent other types of terrorist incidents. Further research is needed to assess how these assets might be made available to, or developed in association with, the private sector with a view to predicting cyber incidents or at least being able to monitor them in real time.

Since it is not possible to prevent all types of terrorism or the many other types of computer incident that occur, and given that attribution of the cause or origin of a cyber incident may be delayed or difficult, business continuity plans and their implementation are a means by which to mitigate the effects of cyber incidents. As an aspect of senior management functions, BCPs could be prepared in advance and then implemented upon notice of, during or after an incident to restore essential corporate or government services. Mechanisms for early warning and detection of incidents can be part of BCPs in order to minimize the time between detection, incident and reaction. Computer emergency response teams (CERTs) are already in place to monitor and report incidents, such as those caused by computer viruses and their potentially worldwide propagation.[13]

Through setting in place early-warning mechanisms for triggering BCPs, methods to assess the origins, type and development of incidents, and plans to restore essential services until fuller recovery occurs, local authorities and central government can put themselves in a better position to respond and recover not only from the less newsworthy and more commonly occurring computer incidents but also from a cyber terrorist act. Governments, however, have the additional responsibility of dealing with the injuries and accidents which result from the public panic that a terrorist act is intended to create.

[13] On CERTs see also chapters 2 and 15 in this volume.

The design and implementation of BCPs, including early-warning and information-sharing mechanisms, present their own difficulties and risks. These include shortages of skilled staff who are already struggling to perform basic services; poor installation and maintenance of large computer projects, making it difficult to locate the problem; and the need to deal with data and services that have been outsourced abroad. The potential effects of cyber incidents, moreover, vary in different parts of a country, or across regions of the world, in part because of variable standards of living and emergency services support as well as the diversity of geographical circumstances (e.g., locations susceptible to particular natural disasters or sites of critical infrastructure assets). Small and medium-sized enterprises and many developing countries with a lack of resources often do not have BCPs and instead rely on an often implicit strategy of reacting to an incident after it has occurred.

At the corporate board or senior government policy level, security management can be linked to business continuity planning, especially when dealing with critical infrastructure. Companies and governments need to assess not only threats but also vulnerabilities arising from connectivity and interdependencies. One of the most important interdependencies is that between the communications and utilities sectors, recognized most acutely at the millennium shift. The degree of interconnectedness, however, can also be viewed as an asset. For example, the utilities' transmission and distribution systems in mainland Europe are highly integrated, enabling arrangements for alternative provision when one country faces an outage. In Asia, however, historical and geographical factors have forced countries to rely solely on national means of electricity provision. These two different sets of circumstances are illustrative of the varying requirements for business continuity planning, not only among companies within the energy sector which have to provide services, but also among users whose BCPs need to cover the choice of alternative supply.

A holistic approach in both business continuity planning and security management is required. It must include protection of not only information and services but also the infrastructure on which data and services are transmitted, and vetting of the personnel handling sensitive employee or proprietary data. IT security issues can no longer be dealt with solely by a technical person in a back office or within a compartmentalized subdivision of management.

IV. Globalization and the role of business in cyber security

The rhetoric about cyber terrorism galvanizes awareness of the need for information protection, but this rhetoric can also have a distorting effect. When companies ask government to advise them on the severity of the cyber terrorism threat and receive a nebulous response, corporate decision makers may then argue that they do not need to pay for more security. Yet, as the business sector becomes more aware of the causes of non-cyber terrorist incidents, business can no longer afford to delay in implementing information security

measures. It can be expected that the corporate sector, including infrastructure owners, should pay for security measures to deal with the risks which they know may affect their sector—now including those arising from IT projects and networks.

As owners of infrastructure become aware of these new risks, they can budget for the protection of their information as well as for the implementation of BCPs in the event of a cyber incident. Corporate liability and responsibility are gradually becoming codified and institutionalized for dealing with these relatively new security requirements, and are increasingly becoming a corporate budget line-item. In the UK, the 1999 Turnbull Report provides guidance to directors and other managers of companies listed on the London Stock Exchange for their requirement to identify, evaluate and manage their significant risks. They must review on a regular basis reports on the effectiveness of the system of internal control in managing key risks and make annual assessments.[14] Such types of guidance and international standards for IT security management, such as ISO 17799,[15] enable more widespread and consistent implementation of IT security policies, facilitating more secure economic transactions, which in turn stimulates business and commerce.

While regulations and standards have roles in promoting good IT security, the uncertainty about the economics of IT and networks worldwide also strengthens the impetus for business to implement IT security management processes, as these uncertainties lie beyond any one entity's local corporate control.[16] Internet-based remote access to sites for routine maintenance may reduce personnel costs, but these systems also give rise to opportunities for interception and data manipulation. Internet-based or -accessible products or services may stimulate new revenue streams, but if improperly implemented or secured they may also lead to security incidents and potential loss of reputation. Many companies, including those in the financial services sector, write off a considerable amount of their losses from computer incidents, whatever the cause, because this is cheaper than improving management and staff satisfaction or hiring and training skilled personnel to implement adequate information security policies. BCPs often include mechanisms for reputation management, which may be cheaper than overhauling an IT security system.

Within the context of globalization and the spread of IT, new vulnerabilities have arisen. While the spread of new technologies is not new in itself, concerns arise from the rate at which new IT technologies and applications have appeared over the past decades and from the unevenness of the global spread of IT, often referred to as the 'digital divide'. However, the digital divide

[14] Institute of Chartered Accountants in England & Wales, 'Internal control: guidance for directors on the Combined Code (The Turnbull Report)', Sep. 1999, available on the Institute's Internet site, URL <http://www.icaew.co.uk>.

[15] International Organization for Standardization, 'The ISO 17799 Service & Software Directory', URL <http://www.iso17799software.com/index.htm>. See also the ISO Internet site at URL <http://www.iso.org>.

[16] Frye, E., 'Information-sharing hang-ups: is antitrust just a cover?', *CIP Report*, vol. 1, no. 8 (Feb. 2003), p. 7, available at URL <http://techcenter.gmu.edu/programs/cipp/cip_report.html>.

encompasses more than just uneven IT spread or absorption: it also reflects more deep-rooted disparities in a country's income distribution and in its education and employment opportunities. Understanding the new vulnerabilities in IT for any given environment thus requires knowledge of a country's overall infrastructure. Because much technology spreads via the corporate, commercial or business sector, not by governmental routes, uncertainties about its use abound.

Three trends concerning globalization and business developments can be identified to help provide a wider context for IT security concerns. One perception of globalization is that the largest companies in the world, which tend to be firms in the United States, are destined to remain in control of advances in IT technology. While some anti-globalization protesters dislike this perception of control, the spread of IT by multinational companies can bring with it the spread of common IT infrastructure, and along with it the spread of 'good practice' in the fields of IT project development and cyber security. Second, globalization raises awareness of 'the local'. Given that about 60–80 per cent of the gross national product of most countries is derived from small and medium-sized enterprises, the spread of IT means that more local and regional businesses are stimulated and encouraged as new ideas and processes come into the region. However, these opportunities are sometimes opposed by strong vested interests which see technology as reducing both jobs and the scope for the corruption that some regard as a necessary 'enhancement' of their otherwise meagre incomes. IT security concerns may be greatest in such cases if a lack of resources necessitates reactive rather than proactive approaches to BCPs and security management. Third, globalization has resulted in the creation of 'virtual companies', based on highly integrated information networks that bring together and then distribute knowledge, skills, labour resources and production facilities—wherever and whenever they are required. This process highlights the business drivers and the pressure for new sources and streams of business revenue, but it also points to the new security risks arising from bringing together people and networks with varying degrees of IT capability and knowledge of security. These three modes of IT transfer and absorption represent a dynamic range of business or economic developments that require strategic thinking about how best to devise security management in the face of international IT vulnerabilities and threats.

V. Conclusions

Further research needs to be carried out on the extent to which a potential terrorist would choose cyber means rather than explosives to achieve the large or spectacular impact associated with terrorism. The complexities of the often proprietary electronic networks of critical information infrastructure, and the increasingly strong authentication procedures for access, suggest that it is very difficult for those outside a large corporate enterprise to launch a successful

cyber attack on it without 'insider' knowledge of its networks. Outside the critical infrastructure sectors, however, the fact that so many businesses are not yet properly implementing even the most basic security policies implies that anyone, including a cyber terrorist, could have an opportunity to manipulate data or bring down a network without insider knowledge.

Putting into place protection and intrusion-detection systems, minimizing technical vulnerabilities, assessing computer connectivity with the Internet and implementing good management of IT projects, including software upgrades and contingency and recovery plans, would all contribute either to the prevention of cyber incidents in general or to better emergency response action. They would also go a long way towards protecting against or mitigating the impact of cyber-terrorist acts. This is not to argue for complacency on matters of cyber terrorism, but rather to place into better perspective the questions of what types of security effort are required and where.

The degree to which the private and public sectors cooperate on critical infrastructure protection and how they do so are important. Most analysts agree on the need for more information sharing between the public and private sector, but the more debatable issue is how and where this cooperation might be institutionalized or codified. Given the importance of ensuring that critical infrastructure provides a reliable service, governments have traditionally shared relevant intelligence information about impending threats to such infrastructure with owners and operators, albeit on an informal basis.

The strategic impact on issues of cyber security of new technologies and their global spread requires further analysis. The 1990s brought new developments in IT which companies, governments and individuals throughout the world understandably were keen to use. New communications and computing technologies were introduced into daily operations to reap the benefits of reducing operational costs, facilitating remote access and processing, and enabling new business models, such as electronic commerce, to produce new revenue streams. However, more research is needed on how global developments in commerce and business, such as outsourcing, may give rise to uncertainties which require a greater focus on data and infrastructure protection measures.