

Panel on “Cyber terrorism and international cooperation”

**“Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection”**

by Olivia Bosch  
International Institute for Strategic Studies  
21 May 2002

All too often a major computer disruption is described as an act of “cyber terrorism” when it is not, and this has confused discussion on what policies are required to protect electronic information assets, particularly those related to critical infrastructure. This paper discusses concerns evoked by “cyber terrorism” and the assumption that targets of cyber terrorism will include a state’s critical information infrastructure. Critical infrastructure includes the essential human-built assets related to energy, communications and water supply that underpin a state’s survival and well-being. Critical *information* infrastructure is defined here as the electronic information network components of these essential assets and their connectivity with other major industrial sectors such as banking and transportation. This paper will highlight:

1. what “cyber terrorism” means;
2. the link between critical information infrastructure and “cyber terrorism”; and
3. the role of the private sector in protecting critical information infrastructure with reference to the mechanisms used, for example, during the Year 2000 experience, for global monitoring of computer disruptions.

**Definition of “cyber terrorism”**

A commonly accepted definition of “cyber terrorism”<sup>1</sup> has been as elusive as that of “terrorism” generally. It is helpful, however, to refer to the extensive literature on terrorism, often in the context of guerrilla warfare and associated negotiations for conflict resolution. In this literature, “terrorism” is frequently defined as the intentional use, or threat to use, violence to intimidate or kill civilians or incur large-scale destruction for political purposes.<sup>2</sup> A terrorist attack is a tactic that is part of a larger political-military campaign by organised non-state groups or sometimes states in pursuit of their objectives.<sup>3</sup> Throughout history,

terrorism has infrequently been the sole means or strategy for such an organisation to further its goals;<sup>4</sup> and often terror is not even the main mode of operation. Terrorists have traditionally relied upon the use of conventional weaponry, primarily explosives, guns and mortars, and techniques such as kidnapping and, in the last few decades, hijacking. The widespread reporting of terrorist acts gives rise to a perception that terrorism is more prevalent than it is; this reporting is facilitated by the obvious results of using conventional weaponry and by the increasing number of media outlets world wide, particularly since the late 1990s.

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-scale as to undermine any public support for their group or provoke retaliation that might destroy it. The scale of casualties has varied, however, depending on such factors as how successfully the operation is conducted and what the objectives are. For example, some cults or apocalyptic groups may have goals that require aiming for high casualties,<sup>5</sup> and some analysts since the attacks of 11 September 2001 on the World Trade Center and Pentagon argue that the new terrorism is the ability to cause heavy casualties and thus focus on terror as a form of expression rather than as the means of conveying a message for political purpose.

“Cyber terrorism” can be defined, therefore, as the use, or threat to use, attacks by and on computers and related electronic networks and information to intimidate or kill civilians or incur large-scale destruction or disruption for political purposes. This would include the use of computers and related tools to cause “mass disruption” in information or service flows intended to induce fear or undermine public confidence in essential public services. While the term “cyber terrorism” is often used, however, security analysts argue the low degree of its occurrence.<sup>6</sup> Richard Clarke, Special Advisor to the US President for Cyberspace Security, prefers that the term not be used and instead wants to focus on information security.<sup>7</sup> If cyber-terror attacks resulting in large numbers of casualties or mass disruption and destruction were to occur, they would be unlikely to go unnoticed by the media. Alleged cyber-terrorist acts that have been attempted but thwarted would be difficult to count, as intelligence successes are reported less frequently than intelligence failures. This paper, however, is not claiming that cyber terrorism will not occur or has not yet been attempted, but seeks to place into better perspective what it would entail compared to the great majority of computer and network “incidents” with other causes.

As cyber terrorism appears to be so infrequent, it is worth noting what is giving rise to computer “incidents” – a term neutral as to cause. At least half of all computer incidents are the result of non-malicious events such as accidents or unintentional effects of vulnerabilities arising from mismanaged configuration of networks, software flaws (which also facilitate viruses), improper technical or administrative implementation of information security policies, inadequately trained users and human error. That about 75% of large information technology (IT) projects are delayed, are over budget and do not work as intended indicates the high degree to which good IT project management is a pre-requisite for good IT security.

The remaining number of incidents are primarily caused by persons with malicious, criminal or political intent, the majority of these being disgruntled employees – also known as “insiders”.<sup>8</sup> Many policy and corporate decision makers either do not admit to having many cyber incidents or ascribe a computer or network disruption to cyber terrorism when it was not; while this may be easier than admitting bad management giving rise to dissatisfied employees, it can be misleading in the context of improving information security. Other malicious activity is undertaken by cyber criminals who seek to steal or manipulate data for financial gain and try to do so without being discovered. Additionally, there are “hactivists” (who conduct civil protest on-line) and hackers (who obtain unauthorised network access for intellectual challenge) most of whom seek media or other forms of attention, but unlike cyber terrorists do not intend to kill or cause large-scale destruction in the pursuit of their activist or civil protest goals.<sup>9</sup>

It can be expected that malicious cyber activities aim to cause disruption in support of other criminal objectives, such as extortion and blackmail. Recent cases of such action include, for example, attacks against a corporate business server or database with the perpetrator threatening to advertise the system’s vulnerability, and hence undermine corporate reputation, if a ransom is not paid. It is noted that such activities might in turn be undertaken to finance terrorist or other criminal activities, and “[t]he potential use of violence and intimidation either to recruit hackers or to obtain computer passwords from employees should not be underestimated”.<sup>10</sup> Intimidation, killing of civilians and causing large-scale destruction are already proscribed by national and international criminal laws, such as those dealing with murder, conspiracy to murder, and hijacking, and criminal prosecution might be conducted against the perpetrators.<sup>11</sup> Attacks on or by computers and electronic networks and information are increasingly also becoming subject to specific legislation, with examples including the U.K. Computer Misuse Act 1990 (and Amendment 2002),<sup>12</sup> the U.S. Computer Fraud and Abuse Act 1984 and its updates including the National Information Infrastructure

Protection Act of 1996,<sup>13</sup> and the November 2001 Council of Europe's Convention on Cybercrime. While law enforcement is particularly involved in developing forensic computer science, all electronic computer crimes need not have computer-based evidence for prosecution.<sup>14</sup>

Understanding cyber terrorism requires a new multi-disciplinary approach among communities that have not usually interacted. Computer programmers have not needed to be experts on terrorist groups, explosives and law enforcement, especially as at most levels terrorism is, and is treated as, a criminal act. Analysts studying terrorism have not required knowledge of the intricacies of computer software programming and electronic information networks and related legal norms. No one is suggesting that each must now become expert in the other's field, but, at some organisational or policy level, the different skill- and mind-sets need to share insights when analysing cyber terrorism. Given the potential threat, this is essential.

### **Link to critical information infrastructure**

Critical information infrastructure is seen as a likely target for cyber terrorists since it comprises assets, primarily related to national energy requirements and communications that underlie state survival, whose ultimate protection is a responsibility of governments whose policies terrorists may aim to influence. One recent report presented case studies of cyber attacks on critical information infrastructure during conflicts underway at the time. The types of "attacks" presented were primarily website defacements, distributed denial-of-service activities and viruses that did not appear to result in casualties or large-scale disruption or destruction.<sup>15</sup> While these were not labelled as cyber terrorism, it was not certain either what link the perpetrators had with the conflict other than wanting to indicate protest or use the opportunity for a hacking challenge. Further research is needed on that link and the degree to which in future more disruptive hacker activity might be supported by states. If electronic computer attacks were intended to cause mass disruption, large-scale destruction or casualties as a means of warfare during armed conflict, then those actions would be subject to the well known principles of non-combatant discrimination, proportionality of force used to achieve military objectives, and other norms according to the laws of armed conflict.<sup>16</sup>

This tendency to mis-label incidents as cyber terrorist distorts the debate on the best policies for dealing with the disruptions that do occur. This debate is not new. In the past, knowledge of threats to the assets of a nation's infrastructure, particularly in times of crisis or conflict, is likely to have been conveyed informally by an intelligence or other appropriate governmental

agency to infrastructure owners and operators, so that defensive and contingency plans were prepared. The energy, communications, air traffic/airline and financial sectors have decades of experience of drawing up emergency plans for protecting their physical assets, normally for commercial and safety reasons. They know a great deal about the vulnerabilities of their infrastructure to physical attack and the necessary precautions to take. The question is what additional costs must be incurred to counter the small part of overall risk ascribable to terrorism.

While infrastructure owners have decades of experience of protecting physical assets, the protection of information, while also not a new demand, requires new approaches as governments, infrastructure owners and operators, along with many other business sectors, increasingly incorporate new and cheaper information technologies into their daily operations. It follows, therefore, that as they implement these new technologies, including access to the Internet, they become responsible for protecting the electronic data or digitally controlled services, such as electricity or currency exchanges, flowing through their physical assets. This means learning the new risks and implications arising from the new technologies, including matters of liability. Many common types of vulnerabilities and threats are already well known. Assuming that cyber-terrorist acts have been infrequent, then nearly all “incidents” affecting critical information infrastructure to date are likely to have resulted from a combination of the accidents, software flaws, improper implementation of IT projects and security policies, as well as dissatisfied employees, criminals and hackers mentioned earlier.

Infrastructure owners, now aware of these risks, would be expected to budget for the protection of their information and the electronic network infrastructure upon which it relies. Corporate liability and responsibility are gradually becoming codified and institutionalised with respect to these relatively new security requirements and increasingly they are a budget line-item.<sup>17</sup> Putting into place protection and intrusion detection systems, minimising technical vulnerabilities, assessing which computers should not be linked to the Internet, and having good management of IT projects including software upgrades as well as of contingency and recovery plans, all contribute to dealing with incidents and will thus go a long way to protecting against or mitigating possible acts of cyber terrorism. This is not to argue for complacency on matters of cyber terrorism but to place into better perspective where and what types of security effort are required.

Further research is still to be conducted 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 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. However, that so many businesses do not (yet) properly implement even the most basic security policies implies that the computer “front doors” are wide open for anyone, including a cyber terrorist, to launch an attack.

Also for future research is the degree to which cyber terrorists would seek media attention and the extent to which there is proof of their actions. Perpetrators of computer incidents are deemed difficult to trace, but cyber terrorists would want to make themselves known in some way and thus the source of attacks might be more easily attributable. A terrorist’s approach to media attention would differ fundamentally from that of a cyber *criminal* whose activities are conducted in such a way to minimise detection and thus attribution. Situations where a perpetrator has a political motive require input from intelligence sources to gauge the seriousness of the threat so preventive measures can be taken. Contrary to popular perception, however, intelligence information is usually not directly useful for purposes of prosecution.<sup>18</sup>

### **Private sector protection of critical information infrastructure**

The degree to which the private and public sectors cooperate to protect critical infrastructure and how they do so is important. Most analysts agree the need for more information sharing between the public and private sector, but the more debatable issue is how institutionalised or codified this cooperation might be. 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 its owners and operators, but on an informal basis.

While government agencies may discuss external threats with infrastructure owners on a need-to-know basis, governments now want to know more about electronic information attacks carried out within the private sector so they can gauge the level and type of potential threats to national security. Threat assessments will benefit from having winnowed out the great majority of incidents that is not directly related to national security. The private sector, however, has been reluctant to provide such data, in part due to fear of damage to company

reputation if the details became known to the public, for example, through a request under the Freedom of Information Act (FOIA) in the United States. Given the number of industry and computer security surveys over the past few years that indicate a high level of insider-caused incidents, however, managements would find it difficult to acknowledge the management failures leading to disgruntled employees bent on vengeance or fraud, or poor technical and administrative implementation of IT security policies. Many companies, including in the financial services sector, write off a considerable amount of the losses from computer incidents whatever the cause, which is cheaper than improving implementation of information security policies. For critical infrastructure sectors, in which public safety and national security are involved, write-offs are not acceptable.

While rhetoric about cyber terrorism might galvanise attention for the need for information protection, this rhetoric can also have a distorting effect. There is a need to take into account both threats and vulnerabilities, as cyber security is implemented across a wide spectrum with all the different users and owners taking responsibility for their particular aspects. This spectrum of responsibility ranges from the end-user, through the Internet Service Providers (ISPs), infrastructure hardware vendors, communications carriers and software programmers, to threat and risk analysts and senior management or policy decision makers. A new multi-disciplinary approach is needed, not only to gain a better understanding of cyber terrorism, but also to deal with the wide-ranging requirements for IT security generally. Corporate Chief Executive Officers (CEOs) must take into account the role IT plays in their business strategy, and not perceive its security solely as a technical issue to be dealt with by “computer geeks in the back room”.

The Year 2000 (Y2K) experience gave rise to new ways in which governments and critical infrastructure sectors could share information, not only to try to prevent cyber incidents, but also to monitor incidents as they arose.<sup>19</sup> As most of the industrial and commercial sectors involved in critical infrastructure are increasingly reliant upon the (tele)communications sector to deliver information and services, it is appropriate for the International Telecommunication Union (ITU), unique as an international organisation having both states and corporate entities as members, to consider how to achieve a better understanding of the interdependencies across sectors and their related network security issues. Many mechanisms for sharing information about electronic incidents in various sectors are becoming institutionalised. These can be seen to occur at three levels: technical, operational and strategic policy.

At the technical level, knowledge about the vulnerabilities of information technology hardware and software, such as software flaws, is shared among manufacturers, computer programmers and communications engineers. This vulnerability-oriented technical information along with reports of computer incidents is shared worldwide among specialised computer response teams, most notably the CERT Coordination Center (CERT is now the trademark of Computer Emergency Response Team) and the Forum of Incident Response and Security Teams (FIRST), and among the major hardware and software vendor alliances and industry associations such as the Information Technology Association of America (ITAA) – the worldwide organisation is the World Information Technology and Services Alliance (WITSA) – and the Business Software Alliance (BSA).

At the operational level, while technical information is shared as above, there is also specialised knowledge specific to a commercial or financial sector that tends to be shared more easily within that sector but not outside it. Such operational information includes ways in which manufacturers' specifications may have been modified or made proprietary to suit a particular sector's needs, as well as differences between types of information in terms of requirements for ease of access. For example, sectors vary on the extent to which they rely on data transmitted in real time which has security requirements that differ from archived stored data. In 1997, the information sharing and analysis center (ISAC)<sup>20</sup> was conceived in the United States as a mechanism for distributing incident information among primarily corporate members of a critical infrastructure sector. ISACs operate on a continuous basis and members share information in a way that preserves their anonymity while providing an overview of cyber incidents within their sector not otherwise obtained individually. Among the ISACs to date are the Financial Services ISAC primarily of US institutions; the World Wide ISAC, which is predominantly European; an Energy/ISAC established as a result of the 11 September 2001 attacks on the World Trade Center and Pentagon; and ISACs for transportation and the information technology industries.

In addition to ISACs, there are longer-standing information sharing mechanisms in infrastructure sectors where a safety culture is particularly important, such as air traffic control and civil nuclear power. As these sectors already monitor incidents giving rise to public-safety issues, processes to monitor unauthorised access to digital process controls and other operationally significant information-related processes can thus be added to these existing mechanisms. This was the case when monitoring the Year 2000 problem in sectors such as air traffic control and civil nuclear power worldwide. The global monitoring was facilitated or coordinated by international governmental organisations, which already had a

regulatory responsibility for spreading best safety practices globally. The international governmental and industry organisations notable for establishing mechanisms for global monitoring of Y2K incidents affecting critical infrastructure sectors included the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA), and the International Atomic Energy Agency (IAEA) and the World Association of Nuclear Operators (WANO). The International Telecommunication Union (ITU) was crucial in setting up a global monitoring process to deal with repercussions of the Year 2000 problem in communications worldwide, though these arose more from congestion than from the specifications problem of Y2K itself. While the international financial institutions such as SWIFT and the Bank for International Settlements (BIS) tend not to confront problems threatening life and limb, potential major disruptions of financial flows were perceived as sufficiently destabilising to warrant establishing global monitoring mechanisms. Whether in the form of ISACs as initially conceived since 1997 or of pre-existing information-sharing mechanisms, there has been a tendency to share operational information more easily within a sector than across sectors. Such information sharing within sectors is essential to improving analysis of cyber incidents so that it is possible to distinguish whether a cyber attack is meant to target a sector or a particular enterprise within a sector.

At the strategic policy level, sharing intelligence about threats and risks as well as about vulnerabilities may need to become institutionalised, not only bilaterally between a CEO and a government representative as mentioned earlier, but also more strategically among CEOs across sectors and among government officials across regulatory and intelligence agencies. Additionally, while this multilateral approach may take account of interdependencies between sectors at the national level, mechanisms are also required at the international level. The international organisations mentioned above dealt effectively with the Year 2000 problem at the sectoral level, and they obviously were also instrumental in expanding their existing monitoring mechanisms to deal with computer incidents internationally. The extent to which mechanisms used for monitoring Y2K incidents in critical infrastructure subsequently remained in place, however, depended in part on an assessment of costs relative to benefits. In the absence of explicit potential or actual threats as faced during the Cold War, many businesses, especially small- and medium-sized ones, are less willing to spend on security from potential and unknown cyber terrorist activity. Furthermore, many companies write off losses until they exceed the cost of making security improvements.

Critical infrastructure owners, however, cannot afford to write-off a loss if governments' responsibilities for national security include adequately protecting energy and communications assets. This strategic assessment, however, varies across the globe as many developing countries have learned to live with energy brown-outs and other disruptions to critical services, which are considered "normal". This varying expectation of quality service delivery was a lesson learned from the Year 2000 experience, and another was the extent to which countries see information technology as essential to improving their economies. Making electronic banking and financial services more secure thus becomes a factor in improving economic and political stability. The need for information security applies not only to the international payment systems such as SWIFT, which rely on both communications and electricity infrastructure, but also to mechanisms such as the Financial Action Task Force on Money Laundering (FATF), which rely on critical communications infrastructure to be able to fulfil their objectives. Created by the G-7 Summit in 1989, and having to cope with the more problematical aspects of new payment technologies adopted by the financial and banking sectors since its inception, the FATF, too, used the Y2K experience to develop further mechanisms for monitoring progress towards its objectives worldwide. In October 2001, the FATF extended its mandate to include measures to control terrorist financing. Regarding other activities of cybercrime, Interpol has increased its information sharing-capability globally in accordance with the rise in "hi-tech" transnational crime. Though Interpol does not have investigatory powers, national law enforcement agencies have a mechanism for sharing relevant information and intelligence at the international level.

## **Conclusion**

While cyber terrorism has not occurred on a noticeable scale, it is important to distinguish it from other types of attacks by or on electronic information technology networks, communications and data. The intent to intimidate or kill people or cause mass disruption or destruction for political purposes applies to terrorism however conducted. And whether an attack on a nation's critical information infrastructure might be more effective using traditional terrorist means rather than cyber means is still to be determined. Information infrastructure, including delivery of services reliant upon it, and data are already required to be protected to a large extent for commercial and safety reasons. The owners – whether private- or public-sector – of critical infrastructure thus must give similar priority to protecting information-based assets as previously given to protecting physical assets, not least of which in the past has been communications hardware.

The information security mechanisms and management policies necessary to deal with the many common and well known causes of computer incidents, such as viruses and disgruntled employees, will go most of the way to also dealing with potential cyber-terrorist attacks. In effect, this means harnessing the enlightened self-interest of the owners and operators of the critical infrastructure in maintaining reliable and safe service delivery. The Year 2000 problem revealed many existing incident reporting mechanisms, particularly at the international organisational level, onto which could be added the reporting and sharing of computer incidents, including that from Y2K. Subsequent institutionalising of those mechanisms to share information about the technical, operational and strategic aspects of attacks by and on electronic computer and communications networks can provide that additional information needed to distinguish more clearly between types of attacks, including those arising from cyber terrorism. Minimising the many known network vulnerabilities and reducing IT project management failures that result in the majority of costly nuisance-level computer incidents means more attention can then be focused on potential national and international security threats such as cyber terrorism, particularly resulting in mass disruption. Awareness of the need for improving critical information network security has been heightened by the 11 September 2001 attacks on the World Trade Center and Pentagon, and thus mechanisms for sharing intelligence or reporting incidents involving valuable information related to critical information infrastructure are likely to become more institutionalised, within each important industry sector, between these sectors and related government agencies, and internationally.

## Endnotes

---

<sup>1</sup> A good analysis is in Kevin Soo Hoo, Seymour Goodman and Lawrence Greenberg, "Information Technology and the Terrorist Threat", *Survival*, Vol. 39, No. 3 (Autumn 1997), pp. 135-155.

<sup>2</sup> For analyses of terrorism see Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998); Robert O. Slater and Michael Stohl (eds.), *Current Perspectives on International Terrorism* (Basingstoke: Macmillan Press, 1988); Grant Wardlaw, *Political Terrorism: Theory, tactics, and counter-measures* (Cambridge: Cambridge University Press, 2<sup>nd</sup> ed., 1989); and Paul Wilkinson, *Terrorism and the Liberal State* (Basingstoke: Macmillan Press, 2<sup>nd</sup> ed., 1986).

<sup>3</sup> The focus in this presentation is on terrorism as might be conducted by non-state groups, rather than by states, which generally, though significantly not invariably, have more information technology resources for conducting cyber-terrorist attacks.

<sup>4</sup> For example, the Baader-Meinhof group active in Germany during the 1970s relied primarily on terrorism to try to achieve its goals.

<sup>5</sup> Some cults pursue objectives resulting in internal terror rather than by terrorising the public, for example, the Jonestown mass-murder suicide in November 1978, and suicides among members of the Order of the Solar Temple, and Branch Davidian sects such as during the events at Waco, Texas

---

between February and April 1993. While large-scale casualties may occur, and for a number of reasons, these incidents are not considered terrorist in the sense defined in this paper.

<sup>6</sup> Dorothy Denning, "Activism, Hactivism and Cyber terrorism: The Internet as a Tool for Influencing Foreign Policy", The Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, at Nautilus Institute (10 December 1999) at <http://www.nautilus.org/info-policy/workshop/papers/denning.html>. Though at the strategic rather than tactical level, Greg Rattray argues that international actors, with the many cyber tools and techniques already available, have yet to employ digital force to win conflicts; see his *Strategic Warfare in Cyberspace* (London: MIT Press, 2001), p. 141.

<sup>7</sup> Richard Clarke, briefing on "Administrative Oversight: Are We Ready for a CyberTerror Attack?", Senate Judiciary Committee Subcommittee on Administrative Oversight and the Courts, 13 February 2002, reported in US State Department Electronic Communications, 14 February 2002, at <http://usinfo.state.gov/topical/global/ecom/02021401.htm>.

<sup>8</sup> See for example Computer Security Institute-FBI annual computer security surveys; their early surveys and other surveys indicate that 60-80% of incidents are caused by employees. See also *Internet Security Threat Report: Attack Trends for Q3 and Q4 2001*, Riptech, January 2002, from [www.riptide.com](http://www.riptide.com). The more recent CSI-FBI surveys indicate a rise in computer attacks from outside an enterprise. Such attacks have become more numerous as connectivity to the Internet increases and "attack" tools have become automated. The number of incidents caused by insiders is not likely to have declined.

<sup>9</sup> Dorothy Denning, "Activism, Hactivism and Cyber terrorism: The Internet as a Tool for Influencing Foreign Policy", at <http://www.nautilus.org/info-policy/workshop/papers/denning.html>.

<sup>10</sup> R.E. Bell, "The Prosecution of Computer Crime", *Journal of Financial Crime*, Vol. 9, No. 4 (April 2002), pp. 309-310.

<sup>11</sup> Mary Jo White, "Prosecuting Terrorism in New York", *Middle East Quarterly*, Vol. VIII, No. 2 (Spring 2001), p. 14.

<sup>12</sup> Activities made offences under the Computer Misuse Act 1990 are: unauthorised access to computer material; unauthorised access with intent to commit or facilitate commission of further offences; unauthorised modification of computer material. The 1990 Act was amended in 2002 to include activities against computerised systems which give rise to denial of service.

<sup>13</sup> For a good analysis of aspects of computer crime as discussed in US legislation since the Computer Fraud and Abuse Act (1984), see The Computer Crime and Intellectual Property Section, United States Department of Justice, *National Information Infrastructure Protection Act of 1996: Legislative Analysis*, at [http://www.usdoj.gov/criminal/cybercrime/1030\\_anal.html](http://www.usdoj.gov/criminal/cybercrime/1030_anal.html), updated June 10, 1998.

<sup>14</sup> R.E. Bell, "The Prosecution of Computer Crime", *Journal of Financial Crime*, Vol. 9, No. 4 (April 2002), p. 313.

<sup>15</sup> *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, Institute for Security Technology Studies, Dartmouth College (September 22, 2001) at [http://www.ists.dartmouth.edu/ISTS/couonterterrorism/cyber\\_attacks.htm](http://www.ists.dartmouth.edu/ISTS/couonterterrorism/cyber_attacks.htm); the case studies in this report are the Kashmir, Israeli-Palestinian, and Kosovo conflicts, and the mid-air collision of US and Chinese aircraft on 1 April 2001.

<sup>16</sup> For commentary on international law with respect to terrorism and counter-terrorism since 11 September 2001, see Christopher Greenwood, "International law and the 'war against terrorism' ", *International Affairs*, Vol. 78, No. 2 (April 2002), pp. 301-317, and Adam Roberts, "Counter-terrorism, Armed Force and the Laws of War", *Survival*, Vol. 44, No. 1 (Spring 2002), pp. 7-32.

---

<sup>17</sup> *The Turnbull Report* (September 1999) requires directors of companies listed on the UK Stock Exchange to establish internal controls to manage significant risks to their businesses beyond those traditionally associated with finance and accounting. This is a mechanism whereby risks to information and related technology infrastructure can also be assessed. The US Securities and Exchange Commission (SEC) might also consider developing a similar reporting requirement for IT related risks.

<sup>18</sup> Stewart A. Baker, "Should Spies be Cops?", *Foreign Policy*, No. 97, Winter 1994-95, pp. 36-52. See also the classic by Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday, 1989).

<sup>19</sup> Olivia Bosch, *The Year 2000 Issue and Information Infrastructure Security*, IFS Info 2/2001 (Oslo: Institutt for Forsvarsstudier (IFS) (Norwegian Institute for Defence Studies), 2001); originally published in G. Ragsdell and J. Wilby (eds.), *Understanding Complexity* (Kluwer Academic and Plenum Press, 2001), pp. 191-200.

<sup>20</sup> Global Integrity (now a division within Predictive Systems) implemented early models of ISACs, an idea first suggested for critical infrastructure in the 1997 report of the US President's Committee on Critical Infrastructure Protection.