日本財団
The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

“The IT Revolution and Security Challenges”

Tokyo

December 10-11, 2002

“Dealing with Security Challenges of the Impact of IT”

by
Olivia Bosch
Visiting Fellow (Information Technology)
International Institute for Strategic Studies
UK

IIPS Conference on

“The IT Revolution and Security Challenges”

10-11 December 2002, Tokyo, Japan

Session 2: The Transformation of National Security and Cyber Terrorism

“Dealing with Security Challenges of the Impact of IT

by Olivia Bosch

In examining the impact of a revolution, or evolution, a significant factor is the degree to which the resulting transformations become absorbed and institutionalised, whether in government, industry or other sectors of society. The focus here is to explore where such processes are taking place to deal with security challenges arising from the seemingly rapid developments that have occurred in information technology (IT) particularly in the last decade. An IT revolution was expected in the mid 1970s when there were calls for a “new world information and communication order”, but that appeared not to have resulted as expected. During the 1990s there have been renewed claims for another “IT revolution” yet it, too, remains unclear in its progress given recognition of a global “digital divide”. Technology is not always implemented as quickly as expectations or market projections suggest.

Nevertheless, new IT has been implemented in economic and defence sectors as well as more widely throughout societies. These have occurred variably in different countries pending factors such as GNP, literacy and skills for learning about IT, and the industrial or economic infrastructure to facilitate new economies. Despite the attention that the Internet receives, most of the world’s population still does not have access to it, while television and mobile communications are much more prevalent.

With the new IT benefits, however, there also arise new challenges to national security and law enforcement concerns. Policies regarding security therefore are also likely to be relative – with budgets to be devised according to the nature of the threats, the value of the information and infrastructure to be protected, and resources available to do so. That costs associated with information security are becoming line-items in budgets is an indication that IT security is becoming institutionalised – in the way that corporate or defence budgets allocate funding for the security of physical assets or territory and people. As these processes become more institutionalised and accountable, it is suggested therefore that the element of surprise that might be associated with “information operations or attacks” broadly defined, diminishes and security and stability of information assets might increase.

Threats and vulnerabilities to information and related infrastructure will be outlined, followed by examination of some of the processes that are beginning to be institutionalised to deal with related security challenges. Some of these processes include:

1. networks to monitor computer "incidents", particularly derived for the Year 2000 experience;
2. risk assessment and business continuity planning;
3. some new trends in technology, for example, open source software, and quantum communications, aimed to improve information security.

Vulnerabilities and Threats to Information and Infrastructure

The 1990s brought new developments in information technology (IT). Companies, governments and individuals around the world understandably were keen to introduce these communications and computing technologies into their 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.

During the 1990s, owners of critical infrastructure assets primarily associated with energy and communications, also acquired or adopted new IT components to facilitate increased connectivity with other major industrial or commercial sectors such as banking and transportation. These IT networks, including both computers and telecommunications, therefore comprise critical *information* infrastructure, which being relatively new, is subject to new forms of electronic attack. Three types of IT asset requiring protection are:

- data and information whether stored in databases or transmitted in real time;
- communications and computing hardware – coaxial and fibre cables, microwave stations, satellite ground stations, SCADA networks; and
- services that are delivered along these means – for example, electricity and electronic fund transfers.

Some of the specific threats and vulnerabilities that give rise to computer "incidents" – a term neutral as to cause, can be outlined as follows. At least half of all computer incidents are the result of non-malicious events such as accidents or the unintentional results of such vulnerabilities as 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 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 both good business continuity planning and IT security.

The remaining half of incidents primarily result from the malicious, criminal or political intent of individuals, the majority of which are disgruntled employees – also known as "insiders".[1] 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. This may be easier than admitting bad management giving rise to dissatisfied employees, but it can be misleading in the context of what is needed to improve information security. A small proportion of 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, an even smaller proportion of incidents arise from activity by "hactivists" (who conduct civil protest on-line) and hackers (who obtain unauthorised network access simply for the intellectual challenge). Most of the latter seek media or other forms of attention. Unlike cyber terrorists however, they are not likely to intend to cause deaths or large-scale destruction or disruption in the pursuit of their activist or civil protest goals.[2]

In contrast, "cyber terrorism" can be defined 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. Given the low frequency of cyberterrorism, 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 more generally.[3] 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 recognise, as intelligence successes are reported less frequently than intelligence failures. A claim is not being made here that cyber terrorism will not occur or has not yet been attempted, but seeks to place into better perspective what its results might be compared to the great majority of computer and network "incidents" that already occur from other causes.

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 or particular commercial sectors, 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 and government departments do not yet properly implement even the most basic security policies implies that IT networks are susceptible to an "attack" from almost anyone, including a potential cyber terrorist.

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.

One comment is made here with respect to issues concerning "cyberwarfare". It is suggested that this term be used less promiscuously and instead focus more specifically on the use of "information operations" in times of armed conflict. One recent report presented case studies of cyber attacks on critical information infrastructure during the Kashmir, Israeli-Palestinian, and Kosovo conflicts. 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.[4] 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 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.

International Monitoring of "Incidents"

While the above indicates the many types of threat or vulnerability that might arise, when a computer incident does occur it is often difficult to pin-point, or attribute, its cause or origin. This becomes even more difficult if an incident affects public safety and security, as BCP and emergency services to rescue casualties and restore local order, may sometimes disturb or inadvertently destroy evidence that might be useful to assessing the cause or doing so in a timely manner.

The Year 2000 (Y2K) experience gave rise to new ways in which governments and critical infrastructure sectors worldwide shared information to monitor incidents as they arose.[5] As many of the industrial and commercial sectors involved in critical infrastructure are increasingly reliant upon the (tele)communications sector to deliver information and services, protection of communications to monitor all types of incidents is also important. International mechanisms for sharing information about electronic incidents in various sectors 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) [6] 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 those that address financial services 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. 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, relying extensively on 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, or as was known for Y2K, many businesses, especially small- and medium-sized ones, are less willing to spend money on security from potential and unknown cyber terrorist activity. Furthermore, many companies write off losses until they exceed the cost of making security improvements. Since the events of 11 September 2002, however, there has been a renewed surge in monitoring flows of information and "incidents". The distributed denial of service (DDoS) "attacks" on 21 October 2002, on the thirteen root servers of the Internet has highlighted the recent focus on mechanisms to monitor computer incidents against it. These monitoring systems are gradually becoming institutionalised in the first instance to provide early warning that something is not working as it should – not necessarily however the diagnosis.

Risk Assessment and Business Continuity

Given that correct attribution of an incident's cause may be delayed or difficult to ascertain, business continuity plans (BCP) are often implemented in advance of that knowledge to restore essential corporate or government services. Mechanisms for early warning and intrusion detection, information sharing of such incidents can be part of BCP, and also feedback into threat or risk assessments. Many computer emergency response teams (CERTs) already exist to try to trace the origins of incidents or propagation of computer viruses that could spread worldwide – not dissimilar too to the requirements for epidemiological surveillance systems that are being established or further developed to keep a watch on disease outbreaks.

Having in place an early warning mechanism to assess the origins, type, and development of a computer incident arising from less newsworthy but more common incidents means that local authorities and central government can be in a better position to deal with a potential terrorist act. Governments, however, are also likely to need to pay additional attention to the possibility that there will be public panic, created intentionally by a terrorist group, which may result in additional injuries and accidents. Risks and threats however have different implications or effects in different parts of a country, or different regions in the world, in part due to differences in GNP, geographical location, and degree of dependency or reliance on IT.

Implementing early warning and information sharing mechanisms also facing short-term difficulties. These include large computer projects not being implemented correctly that burdens a monitoring system with too much “noise”; and shortages of IT engineers and properly trained staff that puts pressure to outsource abroad which may add additional security risks.

At the corporate board or senior government policy level, it becomes important to link both security management and business continuity planning. Companies and governments need to assess not only threats but also vulnerabilities arising from both dependencies and interdependencies of IT networks – one of the most important interdependencies is that between the communications and the utilities sectors, recognised during the Year 2000 experience. The degree of interconnectedness, however, can be viewed as an asset. For example, the national utilities 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 meant that countries 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 who make BCP decisions involving choice of alternative supply. Varying incompatibilities among communications standards, such as among mobile communications (CDMA-GSM-Imode), might reflect concerns about market share and be inconvenient to business users, but it is suggested that such differences have the effect of making a large-scale or global communications outage less likely to be conducted.

Understandably, everyone was delighted about the prospects of implementing new IT, but senior management must rethink how data and cyber protection is to be re-integrated with physical asset protection – as well as with processes of vetting personnel handling sensitive employee or proprietary data. Prior to the 1990s, information security tended to be synonymous with physical asset protection; this is less the case since the 1990s when information is in electronic form. While one can also put a computer in a safe or disconnect it from the Internet, data becomes more difficult to protect when it is online or in databases interconnected with customers to provide 24-hour services or sustain new business models. Thus a holistic approach for both business continuity planning and security management is required for protecting information and services as well as the infrastructure upon which they are transmitted. These issues can no longer able be dealt with solely by a technical person in a back office and have become corporate board room issues. In the United Kingdom, *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. There is a requirement to report such risks, a prerequisite of which would be an internal assessment of IT projects. There has been considerable press coverage on the high number of capital intensive large-scale IT projects that have not been implemented properly, which implies that management of information security is not effective either. The US Securities and Exchange Commission (SEC) might also consider developing a similar reporting requirement for IT related risks.

New Technologies

While companies and governments are struggling to deal with the risks associated with existing IT, and consortium and IT associations and networks are organised to try to improve or upgrade existing protocols, software and security measures,[7] there are other developments that are coming onstream. Among them is the growing use of Open Source Software (eg, Linux) that over the past six to twelve months is gaining wider acceptance for future use in government information networks. From a national security perspective, some governments are concerned that the sensitive or classified government electronic data they use is on foreign-made computer systems about which they have little knowledge or control over. Some of these concerns might be addressed as proprietary software providers can provide that on a case-by-case basis. Additionally, many developing countries believe the use of open source software provides cheaper and wider educational and training opportunities for their population to learn more about IT than that provided by the fewer jobs available in proprietary software companies. The degree to which OSS becomes even more adopted may have implications for the future of the structure of the IT industry that remains to be seen.

Another development is that quantum computing and "quantum communications", in particular the latter which is a cryptographic key management system. While quantum communications are expected to provide for the secure distribution of keys without the need for traditional couriers, its value is also in the ability to detect interception. The US NIST and UK Financial Services Foresight committee have advocated the need for companies to be aware of these developments which also has implications for government funding of science in these areas or of new fibre and infrastructure requirements to operate these new systems. Government funding reflects new policy priorities.

Developments in technology impact on states' security in different ways. 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.[8] 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.

[1] 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.riptech.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 but may be more significant given "insider" knowledge of networks.

[2] 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 means to win conflicts; see his *Strategic Warfare in Cyberspace* (London: MIT Press, 2001), p. 141.

[3] 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.

[4] *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; 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.

[5] Bosch…

[6] GI

[7] Andrew Updegrove, "Forming, Funding, and Operating Standard-Setting Consortia," *IEEE Micro*, Vol. 13, No. 6 (December 1993), pp. 52-61.

[8] Olivia Bosch et al., "Telecommunications Security and Reliability in the 21st Century", proceedings of CGSR-Office of Engineering Technology (FCC) conference October 2000.