

*An analysis of international security issues compiled by security professionals for business leaders and those who advise them*

As our societies become increasingly digitised we introduce vulnerabilities that we barely understand. Malicious individuals and organisations, from the amateur hacker to the sophisticated criminal or terrorist, are already seeking to exploit these weaknesses, before we have even really become aware of them.

In this issue of *Janusian Thinking*, guest contributor **Dr Kevin O'Brien, Senior Policy Analyst, RAND Europe**, offers an insight into a future where terrorists and criminals target critical infrastructures to cause harm, whilst using the information society to their own advantage.

PLEASE NOTE: The views expressed here are those of the author alone, and do not necessarily reflect those of RAND Europe, Janusian Security Risk Management Ltd or The Risk Advisory Group Ltd.

## ***"Asymmetric" Threats To Society***

Today, much is made of the emergence of 'new' threats. In reality, many of these are evolutions of threats, brought about by modernisation and technological advances. Contemporary parlance refers to these 'new' as "asymmetric" – so called because they attempt to find and exploit 'Achilles Heels' in Western societies/strengths where none were believed to exist previously. The links between two 'asymmetric' threats – cyber-attacks and terrorism – have increased awareness that the threat is no longer just to the state and its institutions, but (perhaps more importantly) to everyday society, itself supported by the Critical National Infrastructures of the state.

Globalisation, new liberalisations in formerly autocratic states, increasing privatisation of state-functions, and, most importantly, the revolutions in computing, telecommunications, and data-transference capacities have affected strongly both today's international security agenda and the nature of the threat. This, in turn, has led to concerns about the ways in which today's terrorists can use cyber-space<sup>1</sup> to both plan and conduct their attacks. These forms of asymmetric (cyber-)attacks target the major elements of the national economy: the public telecommunications network, the financial and banking system, the electric power-grid, the oil and gas networks and the national transportation system (including the air transportation system). While their success rate is low, this will likely change in the near future, as the more the world digitises, the more vulnerable it becomes – and the abilities of cyber-terrorists to copy and share each other's capabilities are only facilitated by the Internet. The spectrum of cyber-threats ranges from recreational hackers at the bottom end to national intelligence services and armed forces at the top end. In between, in terms of capability, entities such as semi-organised crackers, hacktivists, organised criminals and terrorists all float. These cyber-threats can be defined as "all forms of electronic attack as well as physical

<sup>1</sup> The term "cyber-space" is used here to refer to any and all aspects of the Internet and World-Wide Web (including communications and informational means), as well as any networked system or systems which are connected to other systems outside of themselves.

attacks and threats to system integrity". The most worrying of these threats are those that may cause observable disruption (e.g. direct action, terrorism) and those that may be clandestine (e.g. espionage and crime). Such threats jeopardise both the functioning of infrastructures and the data they carry (i.e. the confidentiality, integrity and availability of information and information systems).<sup>2</sup>

These "information age terrorists" present a potentially greater threat – in terms of the potential to render mass destruction/disruption to today's information-age societies – than many others in the past.

Terrorism is about creating fear in society, through the threat or use of violence, in support of a political or religious agenda; what has changed about the 'new' (versus traditional) terrorism is that today's terrorist is virtually unlimited in their targeting and their demands, often using terror as an ends itself. These terrorists, as exemplified by al-Qaeda and its supporters, are constantly searching for new 'asymmetric' means to attack all aspects of society – the attacks of September 2001 were exemplary of such asymmetric means.

Ironically, the technologically-advanced nature of Western society is making the terrorist's job much easier through its reliance, increasing daily, on large volumes of information provided through a largely unregulated Internet that is unimpeded by 'national' boundaries. In most instances, the populations and governments of Western countries rely almost entirely on the critical information infrastructures of government and corporate computer-servers, telecommunications facilities and Internet Service Providers. This is all the more concerning when the West's reliance on information and information systems as a vital component of decision-making is made clear; the exploitation of these nodes by terrorists can be used to infiltrate or disrupt Information Technology systems, including those used for command, control, communications and logistics, to modify or manipulate data, or to attack the national strategic infrastructure (e.g. by disrupting critical systems such as international air traffic control systems).

Future terrorists will have a number of tools at their disposal, including the use of cyber-warfare and the acquisition of selected high-technology sensors, communications, and weapon systems. The exploitation of civilian resources such as the Internet and commercial satellite imagery, as well as the proliferation of advanced weapons, allow the terrorist better operational planning, more accurate targeting and, thus, greater damage potential. This strategy would see cyber-weapons and -tools being used to disrupt information-technology (IT)-dependent military and civilian systems, as well as launching attacks on critical infrastructures in order to disrupt and destroy the economies and infrastructures of Western states.

All of these present ready 'asymmetric' targets; this is especially the case for 'cyber-terrorism', where attacks that undermine trust and confidence would seem to be directly useful, even (or especially) if they leave the functioning of the infrastructure and the transmission of signals intact. Responding to a potentially devastating cyber-attack – or mitigating the threat of one – has become one of the key priorities of most advanced governments today.

### **Information Terrorism**

In the Information Age, terrorism has found increasingly prominent uses for instruments such as the Internet to facilitate its efforts. This "information terrorism" exploits the Internet, providing the nexus between the criminal abuse of information systems and the physical violence of most terrorism (all in the interests of supporting or facilitating a terrorist campaign or action). The Internet has facilitated the metamorphosis of many terrorist networks from

---

<sup>2</sup> As defined by the Information Assurance Advisory Council (IAAC) Threat Assessment Working Group – see: [www.iaac.org.uk](http://www.iaac.org.uk)

those of strong central control to ones with no clear centre-of-control due to its networked nature. In this same sense, the Internet can be used for clandestine communications through Virtual Private Networks, posting messages on e-mail and electronic bulletin boards, as well as steganography (hiding messages within pictures and objects) and encryption. Terrorists, organised crime and other sub-state malicious actors can use the data, information and knowledge resources available in the Information Society to plan and organise, finance and communicate, and ensure command-and-control over real-world operations – indeed, terrorists gain secrecy, increased ease of locating or interacting with those who share their interests, and a certain 'virtuality' that lowers the human barriers to terrorist activity through their exploitation of cyber-space; this was clearly demonstrated over the past eight years by al-Qaeda and other pan-Islamist terrorist organizations, and is not a post-September 2001 realisation.

It is also likely that these asymmetric threats will come from diverse, differing and simultaneous vectors. For example, the possibility that terrorism will be accompanied or compounded by cyber-/infrastructure-attacks damaging vital commercial, military, and government information and communications systems is of great concern. In this sense, a major Western country could suffer greatly at the hands of an educated, equipped, and committed group of fewer than fifty people; such an attack could cause an effect vastly disproportionate to the resources expended to undertake it. The attacks of September 2001 were – in themselves – attacks on the advanced 'Information Society' as they aimed to destroy trust and confidence in both the financial and politico-military pillars of Western society.

In the future, groups like al-Qaeda may use cyber-tools and knowledge at their disposal to cause additional destruction and chaos alongside real-world attacks. Attacking an information system would be a good way to either distract the target or otherwise enable the terrorist to perform a physical attack: for example, had Aum Shinrikyo been able to crack the Tokyo power system and stop the subways, trapping passengers on the trains, the number of casualties caused by their 1995 Sarin gas attack might have been significantly larger. Another example could be taking down a city's emergency telephone system through a cyber-attack while setting off terrorist bombs and interfering with the media – producing an asymmetric synergy, increasing the exploitation levels and making the individual attacks much more effective than they would have been alone.

### ***Information Terrorism and Cyber-crime***

While amateur hackers receive most publicity, a greater threat is posed by professionals or "cyber-mercenaries", some highly-skilled and -trained veterans of government agencies or corporate intelligence branches working on the open market, increasingly in support of terrorist and/or criminal groups. The Colombian drug cartels, for example, hired cyber-mercenaries to install and run a sophisticated secure communications system, while Amsterdam-based gangs (including people-smugglers) used professional hackers to monitor and disrupt the communications and information systems of police surveillance teams. Numerous trained hackers, some the product of Russian and Eastern bloc governments, have located themselves in countries such as Bulgaria (notorious as a virus factory) and the Baltic States, where portable Directed Energy Weapons (which will devastate unshielded electronic circuitry) can be purchased openly. In addition, compared to amateur hackers, these professionals can be very mobile – making links with crime groups of great interest.

There is a strong concern that such threats – compounded by cyber-crime activities – will undermine citizen trust in the new economy, threatening the development of the Information Society. In March 2001, Robin Cook warned that "a computer-based attack on the national infrastructure could cripple the nation more quickly than a military strike." The European Commission similarly pointed out that "the information infrastructure has become a critical part of the backbone of our economies. Users should be able to rely on the availability of information services and have the confidence that their communications and data are safe

from unauthorised access or modification. The take up of electronic commerce and the full realisation of Information Society depend on this.”

The commercial world is paying increasing attention to this problem: it is not only in the military but also in the civilian and commercial sectors that such threats have grown, as was aptly demonstrated by both the Distributed Denial of Service attacks launched against the Internet-based companies Yahoo, Amazon and E-bay during 1999-2000. Similarly, the ILOVEYOU e-mail virus – estimated to have cost Western businesses US\$7 billion (£4.7 billion) in damage – was launched seemingly as a practical joke from the Philippines by college students in 2000. Worldwide computer network intrusions were estimated to have cost companies some \$15bn in 2000, with European companies alone losing some \$4.3bn from information security breaches. This rising tide of crime is undermining consumer confidence and slowing the growth of e-Business. In the US, the Federal Trade Commission estimates that 61% of Internet users do not buy online because of security fears; in Britain, the National Consumer Council found that over 45% of Internet users would spend more if they could be reassured about the security of e-Commerce sites. This could have a potentially damaging effect on e-Business and e-Commerce for all. In this sense, an opponent could also conduct a slow-motion strategic economic warfare campaign against private economic interests in the West, through attacks on a wide range of e-payments or electronic currency systems that facilitate the global transition to e-commerce by a high-performance criminal organisation.

### ***"Information Age Terrorism" and Netwar***

One of the ways in which officials world-wide are developing new methods for critical infrastructure protection (CIP) is through developing an understanding of how the terrorists carried out the September 2001 attacks. Many observers have stated that Bin Laden demonstrated a sophisticated knowledge of ICT in the months between the August 1998 attacks in Africa and the September 2001 attacks in the US. A report released the day after the US attacks stated that Bin Laden may have deliberately used the West's intelligence capabilities against it by 'spoofing' these intelligence services – and particularly their SIGINT assets – into believing that an attack was going to take place in Africa and not the US. Since May, there had been numerous warnings that bin Laden or another terrorist leader was preparing a major campaign against Americans, but all the intelligence suggested that any attacks would come overseas. Until as recently as 2000, Bin Laden used high-technology means (such as satellite telephones) to communicate with his followers. Government officials have reported that this stopped abruptly as Bin Laden realised the potential threat this presented him, and subsequently used the communications he knew the United States was monitoring to throw America's spies off his trail, while deploying "human couriers" to carry his real messages and money. However, although Bin Laden may only use the lowest technology means – such as in-person communication with his subordinates – these subordinates are believed to use high-tech means (such as encrypted Internet messages) to correspond with each other; this was clear from the capture of Khalid Sheik Mohammed in Pakistan, who had masses of IT-supported data with him at the time of his capture.

Today, terrorists and crime groups are using cyber-space for their own means:

- a number of transnational terrorist groups, such as the Peruvian Sendero Luminoso, are becoming more involved in cyber-crime to fund their activities
- the Russian mafiya and other groups are moving away from drugs into the more profitable business of cyber-crime
- the most noticeable real attacks by a terrorist group have been those conducted by the Tamil Tigers (LTTE) who swamped Sri Lankan embassies with 800 e-mail messages a day for 2 weeks, an attack characterised as the first known attack by terrorists against a country's computer systems
- the Provisional IRA is believed to have hired hackers to penetrate British government computers in order to get the home addresses of law enforcement and intelligence

officers for a plan to kill them in a "night of the long knives" if the British government didn't meet the cease-fire terms.

- in the aftermath of September 2001, a new group calling themselves the "al-Qaeda Online Alliance" began to undertake cyber-attacks in support of Osama bin Laden
- perhaps most interesting of all is the massively-increased interest shown by Japanese terrorist cult Aum Shinryko in computer firms and software, whose shadow-companies include more than 80 firms and 10 government agencies (including police) amongst their clients.

## Future Outlook

One of the restraints on an all-out terrorist assault on critical infrastructures is that the barrier to entry for anything beyond hacking is quite high: generally, terrorists lack the wherewithal and human capital needed to mount a meaningful operation. Many terrorists have not yet integrated ICT into their strategy and tactics; in addition, the generally non-lethal nature of cyber-attacks thus far may make them less attractive to terrorists wishing to cause casualties, although the attraction of undermining society should not be ignored. Ultimately, in the opposite sense, the ICT revolution may also lessen the need for violence by making it easier for sub-state groups to get their message out – although looking at al-Qaeda as an extremely ICT-proficient organisation does not support this thesis: unless casualties occur, there is less drama and emotional appeal. In this sense, a full-scale "cyber-terrorist" capability remains something very much of the future.

This may change rapidly, however: the next generation of terrorists are growing-up in a digital world, with ever-more-powerful and easy-to-use hacking tools at their disposal. They might see greater potential for "cyber-terrorism" than do the terrorists of today, and their levels of knowledge and skills relating to hacking will be greater. For the moment, hijacked vehicles, truck bombs, and biological weapons seem to pose a greater threat than "cyber-terrorism"; however, just as the events of September 11 caught us by surprise, so could a major cyber-assault.

**Further information:** Janusian Security Risk Management is the specialist political risk and security subsidiary of The Risk Advisory Group Ltd. For further information please visit [www.janusian.com](http://www.janusian.com).

### **CORPORATE SECURITY PROFESSIONALS**

If you have not already done so, please take the time to complete our terrorism risk survey at [www.janusian.com/survey.htm](http://www.janusian.com/survey.htm). The survey is a joint venture with **RAND Europe** to help us better understand corporate attitudes to critical risk issues. We will be presenting our findings at a free conference in London on 1<sup>st</sup> April 2003. Details of the conference are available from our website ([www.janusian.com](http://www.janusian.com)) under the News section.

David Claridge  
**Managing Director**