2006

Information Terrorism in the New Security Environment

Ken Webb
Edith Cowan University

DOI: 10.4225/75/57a821aeaa0d7
Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.

Information Terrorism in the New Security Environment

Ken Webb
Edith Cowan University, Perth, Western Australia
k.webb@ecu.edu.au

Abstract

Over the years there have been many interpretations of what constitutes Information Terrorism. This paper examines the correlation/relationship between Information Warfare and Terrorism, and describes what is considered to be Information Terrorism now. It achieves this by outlining the threat's impact, advantage and capability. It then examines the positives that can be derived from such and, based on the literature available on the subject, provides a deduced interpretation of what Information Terrorism is. The paper concludes with remarks supporting the assertion that Information Terrorism is a major dynamic and asymmetric threat contributing to a new national security environment.

Keywords

Information Terrorism, Information Warfare, Terrorism, National Security Environment

INTRODUCTORY REMARKS

This paper provides a review of literature to inform delegates of what constitutes Information Terrorism and the threat that pertains to it.

In essence, it is surmised that a consequence of the prompt evolution in Information Terrorism is the inability of nation states to respond quickly to such, which has been their approach up till now for countering terrorism. This puts nations in a defensive mode where they are impacting heavily on their own society. It also means it has become hard for nations to communicate worldwide and influence large geographical populaces in a globalised society. The traditional law enforcement model used is also not proving an effective strategy for addressing terrorist conduct of Information Warfare (IW) and the flexibility provided by means such as the Internet is making countermeasures difficult (Deeks, Berman, Brenner & Lewis 2005).

The summation above highlights a whole new capability/advantage for groups considering Information Terrorism, thereby burgeoning the new security environment.

THE THREAT

According to Schwartau (2001, p.4) "asymmetry is what gives terrorists their strength". Therefore, combine the asymmetric threats of terrorism and IW, and a hybrid form of asymmetric warfare is 'Information Terrorism'. Considering that, as contended by Wilson (2005), recent terrorist events have produced the effects of tighter physical and border security then terrorists have a reason to more heavily engage in Information Terrorism to achieve their aims and infiltrate nation states.

A review of literature reveals that many definitions of Information Terrorism exist. However, irrespective of an agreed definition, Libicki (1995) claims Information Terrorism has its advantages, as it allows effective terrorism by directing itself against very specific targets, even if carried out infrequently, from remote and often anonymous locations.

Another perspective given is that Information Terrorism can be called 'cyber terrorism'. This is because, as explained by Furnell (2001), 'cyber terrorists' are terrorists who employ hacker-type techniques to threaten or attack information systems, networks, and/or data". Clarifying this relationship, Furnell (2001, p.41) asserts that, "as with other forms of terrorism, cyber terrorist activities are conducted in the name of a particular political or social agenda to intimidate or coerce another party (e.g. a government)".

The relationship between IW and terrorism is broadened because the terrorists' sought after effect is achieved by conducting Information Terrorism even though information system abuse does not necessarily result in direct violence against humans (Devost, Houghton & Pollard, 2002). Although, as physical violence is a necessary component of terrorism then many acts of criminal computer abuse may not be considered terroristic if they do not result in direct physical violence. Further to this, Devost et al (2002) contend that as technology's implications broaden on society and politics then the outcome of terrorist action in this field will achieve greater effect.

This view is supported to some extent by Jones, Kovacich and Luzwick (2002) who argue that the action of terrorism is to cause 'terror' to the people and for this reason it is difficult, given the current state of information technological advancement, for Information Terrorism to be effective. They clarify this by noting this will change as cultural values change and society becomes more dependent on technology. Therefore, at the very least and in anticipation of this change, the social and political definitions of terrorism should likewise broaden to accommodate Information Terrorism, and the current semantic vacuum of a universally accepted comprehensive definition suggests that IW is a probable new facet of terrorist activity (Devost et al, 2002).

Underlying this conclusion is Hoffman (in Weimann, 2006) who outlines that one of the enduring axioms of terrorism is that it exists to attract attention and uses publicity to communicate its message. In the past, this has been relatively restricted because weapons to do this consisted mainly of guns and bombs. However, today terrorists no longer have this restriction because the modern terrorist's arsenal includes computers, CD burners, email accounts, the Internet and the World Wide Web.

THE THREAT IMPACT

Many countries heavily use information systems to manage and operate critical services. Electricity, gas, water, sewerage and other services are now highly automated and computerised. These systems, in addition to banking, defence, government, telecommunications and transportation systems, form part of a society's critical information infrastructure (Armstrong, 2001). Such systems have been major terrorist targets in the past, and now that they are automated and more critical to society than before makes them increasingly vulnerable and attractive.

Additionally, as attested by Wilson (2005), the computer networks that operate a nation's critical infrastructures now represent the nation's 'underbelly'. However, the software that operates them has proven vulnerable to attack through cyber crime, viruses, worms and other malicious code. Increasing the impact of an attack such as this is another observation made by Wilson. He claims that, because of the interdependencies among infrastructure sectors, a large scale cyber attack that affects one sector may also have disruptive, unpredictable and perhaps devastating effects on other sectors, and possibly long-lasting effects to the national economy. It is considered that this example would apply to most nations.

Hinde (2001) confirms the existence of the Information Terrorism threat in this regard by noting that shortly after the major physical terrorist attacks of 2001 in the US there were immediate concerns from data security experts that coordinated cyber-attacks might be launched against the telecommunications grid, which was already overloaded and slow because of the heavy demand caused by the physical attacks.

This assertion is supported by Bayliss, Wirtz, Cohen and Gray (2002) who claim policymakers now fear that non-state actors conducting terrorism (Terrorist Groups) will conduct electronic raids on vital national systems controlled by computers. They allege that fear is no longer based on the prospect of violence because information and the ability to control it has become a form of power, thereby amplifying the status of Information Terrorism. Another observation made by them is that terrorist cells can now share information and coordinate action without a hierarchical organisation that is vulnerable to penetration and subversion. Consequently, Information Terrorism appears to have become one of the unintended consequences of the 'Information revolution' and society's increased interconnectivity (Henych, Holmes & Mesloh, 2003).

The new situation is described by Dearth (2001, p.67) who states:

> *"Advanced societies are moving to a new place; call it the 'infosphere' or 'Cyberspace'. In the journey to this new place, humankind will bring with it old impulses and needs: the need to connect, to converse, to share intimacies, to conduct commerce…will also bring with it the impulse to violence, conflict and war."*

This observation conjures several scenarios of Information Terrorism. These include altering formulas for medication at pharmaceutical plants, 'crashing' telephone systems, misrouting passenger trains, and disrupting operations of air traffic control.

Jones et al (2002) give another dimension to the Information Terrorism threat, in the form of denial of service attacks. They explain that when a terrorist group cannot achieve its objective by physical means then it has the potential to gain the desired impact by using the Internet and the connectivity of other systems that the target audience relies upon. This is done by preventing legitimate users of a service from using that service, which can be done in a number of ways. This includes network flooding, disrupting connections and systems, and preventing direct access. Terrorists can also do this relatively anonymously and without much effort from themselves, which provides further advantages. Considering that many critical infrastructures now interact electronically with users this brings further frightening scenarios.

Information Terrorism can also, directly or subconsciously, be used in conjunction with or to supplement physical acts of terror, thereby magnifying the desired impact. This conclusion is implied by Emery (2005), who outlines that wherever human activity occurs physically such activity also takes place simultaneously in the information dimension. This means it is important to recognise that the residual effect from physical actions taken will shape the information environment. Additionally, Emery notes that because terrorists can not engage a superior force in the physical environment they conduct selected acts in the physical environment, such as bombings and small scale attacks, to shape the information environment. These acts can help achieve objectives in the information environment and, ultimately, in the physical environment. Therefore, terrorists who lack military parity achieve their ultimate objectives by being successful in the information environment, and this highlights the effectiveness and reasoning for Information Terrorism. Additionally, Wilson (2005) asserts that many security experts agree that a cyber attack would be most effective if it were used to amplify a conventional terrorist attack.

Evidence of the probable conduct of IW by terrorists was highlighted by Richard Clarke (Clarke 2003, p.1), the former US Presidential Adviser for Cyberspace Security, who noted that:

> *"…investigators have accumulated intelligence about Al Qaeda's interests and skills in using cyberspace to launch an attack. Many experts believe terrorists could likely combine such a cyber-based disruption with a real-world physical attack to amplify the impact. We're troubled by the fact that a number of people related to Al Qaeda -- including Khalid Sheikh Mohammed, who was recently arrested and was the chief operating officer... have [a] technical background. Recently, a student at the University of Idaho was arrested by the FBI for alleged terrorist connections, and he was studying in a PhD program on cyber security. So, I think, similarly to the fact that some of the*

> *Sept. 11 hijackers had training in flight training, some of the people that we're seeing now related to Al Qaeda had training in computer security."*

Clarke, only a year before and contrary to the above testimony, is cited via Conway (2003, p.39) saying he did not like to use the words' cyber terrorism because "most terrorists have not engaged in information warfare (read 'cyber terrorism'). Instead, he admits, terrorist groups at this stage have only used the internet for propaganda, communications and fundraising". This gives some idea of the threat's prompt evolution.

Based on the plethora of terrorist websites and their use of propaganda, many terrorist groups now have a profound understanding of the information environment and the ability to more effectively use such (Farrell, 2005). Terrorists have a whole new field of action because most aspects of living today are dependent on information networks. Exacerbating this is that even though the technology to operate and protect networks can be quite costly it is relatively cheap to attack them (Emery, Earl & Buettner, 2004). Shahar (2003).explains that, in the simplest case, only a computer, a modem and a willing hacker is needed, and with university education now globally accessible then terrorists have easy access to these means. Even if they do not, mercenary hackers are available to do the job for the right price.

Enhancing the future impact of Information Terrorism is that new technologies will pose new risks and demand new responses to those risks. This includes terrorist usage of information for attacking nations (Anderson, 1999). Clarifying this effect and possible change required for national security is an indirect example given by Schwartau (2001, p.2), who cites that:

> *"While Western Militaries struggle for a decade on average to acquire new weapons, a country with commercially available computer equipment and less rigorous democratic and accounting processes could field new systems within a few years. It is the stuff of military nightmares."*

Also of particular interest is that terrorism has been rooted consistently in Chinese society with no lapses in operation like much of the rest of the world (Thomas, 2004). Considering China is a prominent nation and now the world's largest supplier of information equipment, and the momentum and techniques of its information industry is increasing, further reasons to justify the increasing relationship between terrorism and IW are evident.

The Threat Capability

A primary enabler of Information Terrorism is the Internet, which is a reason for the current transition into a globalised society. While the Internet is a creation of the West, it is also attractive to terrorists for some of the same reasons it is attractive to society generally. It may be used anonymously so identity is masked; it is global, which allows access to huge audiences around the world; and it is inexpensive and subject to little regulation. Therefore, the Internet enables global terrorism (Deeks et al, 2005). Consequently, terrorist groups appear to be using it to their advantage.

Confirming this observation, Thomas (2005, pp.34-44) in discussing terrorist methodologies, identifies 16 measures for consideration, as the Internet:

- *can be used to put together profiles;*
- *access can be controlled or its use directed according to the server configuration, thus creating a true ideological weapon;*
- *can be used anonymously, or as a shell game to hide identities;*
- *produces an atmosphere of virtual fear or virtual life;*
- *can help a poorly funded group to raise money;*
- *is an outstanding command and control mechanism;*
- *is a recruiting tool;*
- *is used to gather information on potential targets;*

- *puts distance puts distance between those planning the attack and their targets;*
- *can be used to steal information or manipulate data;*
- *can be used to send hidden messages;*
- *allows groups with few resources to offset even some huge propaganda machines in advanced countries;*
- *can be used to disrupt business;*
- *can mobilise a group or Diaspora, or other hackers to action;*
- *takes advantage of legal norms; and*
- *can be used to divert attention from a real attack scenario.*

These measures highlight the value of the Internet to groups conducting terrorism. Weimann (2006), who monitored and archived terrorist Web sites for eight years, validates this by explaining that terrorists are now clearly using the Internet for fund-raising and recruitment, training and instruction, propaganda and psychological warfare, and for gathering open-source information to plan attacks.

The degree of Information Terrorism capability is given by Deeks et al (2005) who note that terrorist groups are now using the information means available to form an ideological platform that precondition its audience to respond to subsequent solicitations of financial support and entreaties to undertake violent operations. In addition to conditioning the minds of participants to accept acts of murder and destruction as politically expedient and morally acceptable, they explain that the electronic forms of communications used actively encourages participants to undertake such acts. They also note that terrorists are even taking advantage of charitable organisations to directly solicit support, and to collect funds and resources. They are also perpetrating online crimes such as identity and credit card theft. In regard to the latter, cyber crime has increased dramatically over the past few years with several recent terrorist events funded partially through online credit card fraud (Wilson, 2005).

As Alexander and Swetnam (2001) highlight, the capability of terrorist groups to conduct IW is occurring on all fronts. On the non-technical (soft) side transnational terrorist groups are becoming increasingly empowered by media outlets that present their position unaltered and unfiltered by governments or communication laws. They are using cellular phones, the Internet, and alternate news sources to do this. On the technical (hard) side, a growing danger is terrorists' slow but steady acquisition of digitally enhanced miniaturised technologies. Therefore, the 'information or cyber' age has enormously increased the capabilities of terrorists (Thomas, 2005).

The whole spectrum of IW is now a definitive capability for terrorist groups, as all the elements can be used and in combination with each other (Thomas, 2005). Additionally, as noted by Wilson (2005), terrorist group links with hackers and cyber criminals is adding to their skills, and finances obtained through drug trafficking may also provide terrorists with access to highly skilled computer programmers.

In effect, terrorist groups are becoming technically sophisticated and years of publicity about information security weaknesses have made them more aware of the vulnerabilities of nation states. Terrorists and their symphasisers are already embedded in societies with a large information technology workforce (Wilson, 2005) and the observations made above infer that the human aspects of IW must be considered when discussing Information Terrorism.

The human aspect includes the central part the Internet is playing in the battle for 'hearts and minds' (due to the global, easy and widespread accessibility of this form of information transmission). This is particularly apt, as terrorists attempt to influence their will upon people. Their threat to societies and states is more about the adverse psychological influence they cause rather than the physical damage they inflict (Radvanyi, 1990; Casciani, 2004).

The increasing capability and desire by terrorists to conduct IW is evident. A real example is given by Wilson (2005) in the form of a well distributed and publicised book by Iman Samundra, who was convicted and is now awaiting execution for his part in the 2002 terrorist bombings in Bali. In this book, Samundra advocates that Muslim youth actively develop hacking skills, and names several websites and chat rooms as sources for increasing these skills. He also urges Muslim youth to conduct credit card fraud to fund the cause. While it is acknowledged that Muslim youth generally will not follow this advice there are some who may be inclined to do so and this increases the capacity of this particular terrorist movement.

An outlook given by Post, Ruby and Shaw (2000) adds a further dimension to this capability. They outline that what is *avant garde* now will become mainstream in the next five to ten years as youth who have been socialised on computers join terrorist groups. Therefore, there is every reason to believe the reliance on information technology will become increasingly routinised and IW tactics will become incorporated in all terrorist operations. Post et al (2000) clarify this by explaining that the rapidity with which information technology is integrated will depend primarily on the group's socio-political context and the degree to which utilising it facilitates the group's cause. Additionally, Information Terrorism is likely to emerge among anti-establishment groups who perceive technological resources to be a source of vulnerability to their opponent or to be important to their opponent's efforts against them, and this creates a gambit of terrorist possibilities.

The Threat Advantage

Arquilla and Ronfeldt (2001) contest that not only has the information environment increased the types of targets and weapons for those wanting to conduct terrorism, but it has also provided more ways for these parties to better operate and structure themselves, thereby placing them at an advantage. They explain that not only has the world embraced an increased access to information, so it can operate more efficiently and with greater flexibility, but terrorists have harnessed this power to enable new operational doctrines and forms of organisations. Therefore, they are empowered to conduct IW.

This ability to conduct Information Terrorism is elevated by groups considering terrorism who are 'disaggregating' from hierarchical bureaucracies, and moving to flatter, more decentralised webs of groups united by a common purpose. This has brought a whole new dimension and set of capabilities (Ibid).

This advantage also introduces the relatively untouched dimension of 'netwars', which has practice ahead of theory. The 'information' revolution favours the rise of network forms of organisations and these appear to be the next major form of organisation after tribes, hierarchies and markets. This form is redefining societies, and in doing so, the nature of conflict and cooperation. Resultantly, network-based conflict and crime is a major future phenomenon (Ibid).

Furthermore, as Thomas (2005) outlines, symbolic leadership, which is instrumental to such organisations, is being magnified by using the Internet and other forms of information transmission. This appears to be placing terrorist groups at further advantage by conducting IW. He uses Osama bin Laden, the alleged leader of the al-Qaeda terrorist group, as an example. Thomas explains that bin Laden is an expert at buttressing Arab opinion with his TV and Internet messages that touch the souls and spirits of exasperated Arabs. He is a credible figure to many, as he extols al-Qaeda successes, gives directives and offers moral support. The media and international communication stations often pick up these broadcasts and replay parts of them to the public. Thomas emphasises that while bin Laden relays his message, as any leader should, the nation states are slow to respond because they are busy deciphering the message and trying to substantiate its authenticity. In the meantime, he moves onto his next planning phase.

THE THREAT POSITIVES

Also worth considering from a positive aspect of national security is that factors that can be used to counter Information Terrorism have evolved but are not yet generally publicised. An example is given by Weimann (2006), who argues that, despite the multiplicity and diversity of terrorist websites, there are nonetheless core and common characteristics that terrorist groups with a presence on the Internet share. As Weimann explains, most terrorist sites are particularly notable for their colourful, well-designed and visually arresting graphic content, selective presentation of information, and effective message. Other common elements include descriptions of the given terrorist group's history, its aims and objectives, and the depredations inflicted by an enemy state/s or people/s upon who/what the terrorists purport to represent. Much other information such as biographies of leaders, maps, photos and communiqués are also on the sites. Weimann concludes that, virtually without exception, all terrorist sites studiously avoid drawing attention to the violence or destruction that the group is responsible for. Instead, issues such as freedom of expression and human rights are used, and this indirectly suggests the psychological warfare purpose of Information Terrorism.

Regardless of the example above being confined solely to the Internet, this observation highlights that messages for improving the awareness of Information Terrorism and how to counter it exist when examining the positive indicators. Additionally, as Smith (2005) and Deeks et al (2005) imply, the approach taken can be changed by exploiting the increased information ability that has been created by nations, thereby placing nations at an advantage, and by winning the debate on aspects such as the Internet rather than by trying to suppress it. These are all worthwhile considerations for national security and enhance the importance of the intelligence function.

Another positive consideration for national security is given by Post et al (2000). They identify that, in contrast to the powerful group dynamics of traditional terrorist groups, those groups relying upon networked organisational structures and computer-mediated communications are subject to virtual group dynamics, which significantly affects their decision-making and risk-taking. This especially applies to those who may only be in contact electronically. It also implies that groups conducting Information Terrorism have serious security implications within themselves also.

Irrespective of these potential national advantages and vide Emery (2005), it is clear that terrorists compared to nation states have now adopted a much different strategy to achieve victory for their cause. They are now using a complex information operations strategy that, considering their circumstances, is more effective, efficient and efficacious than previous forms of operations. This has become an enabler for IW and, "as information systems increasingly form the underpinnings of modern society, terrorist attacks using tools of the information revolution and targeting information systems will become prevalent" (Post et al, p.119).

CONCLUDING REMARKS

As this paper highlights, the topic of Information Terrorism is diverse and relatively new in its nature. However, after reviewing the applicable literature, the conduct of **Information Terrorism** is interpreted as:

> ***A non-state actor's premeditated and asymmetrical warlike conduct of information activities to fulfil their ethos, foster mass acts of terror and/or affect and disrupt the security and/or well-being of a nation or series of nations. This is done to:***
>
> - ***appropriately effect and manage a change in a target audience's perception;***
> - ***market philosophical propaganda so a target public's governance, livelihood and will is influenced through fear;***
> - ***operate advantageously, efficiently, effectively and efficaciously; and***
> - ***preserve themselves from activities by allies, competitors and adversaries.***

This paper also implies that the threat of Information Terrorism is contributing to a new security environment, and a plethora of commentators reviewed in the literature, many of which are given in this paper, espouse a whole range of solutions to intervene and counter this threat. However, this observation intimates the complexity and nature of the overall problem of Information Terrorism, which is a major determinant for the new security environment. Despite this, it is noticeable that a large number of authors argue that, irrespective of what viewpoint they hold, solutions such as a humanitarian convention need to be considered. This infers a preference to just plain aggression and force, which many authors contend is the current approach. It also suggests that, due to the information capacity of the word today, IW itself be employed to counter Information terrorism, as it not only addresses the threat holistically but can be done immediately and expediently considering the capacity of nation states countering terrorism.

However, Buzan, Waever and de Wilde (1998) and Rogers (2000) explain that there are two main obstacles to this challenge and to countering terrorism generally. The first, and by far the most substantial in their eyes, is that the necessary response will involve considerable limits being placed on wealth and power of the elite global minority, thereby requiring radical economic and political changes that are substantially greater than anything previously experienced. The second is that most thinking and writing on international security is deeply ethnocentric and conservative.

Information Terrorism in the new security environment has provided a new dimension and complicates overcoming these obstacles whether IW is used by nation states or not to counter terrorism generally. This highlights a dilemma facing the world.

REFERENCES

Alexander, Y. & Swetnam, M.S. (2001). *Cyber Terrorism and Information Warfare: Threats and Responses*. New York: Transnational.

Anderson, K. (1999). *Intelligence Based Threat Assessments for Information Networks and Infrastructures.* Global Technology Research Inc. [On line] Available: http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml [23 March 2004].

Armstrong, H. L. (2001). Denial of Service and Protection of Critical Infrastructure. *Journal of Information Warfare* 1(2): 23-34.

Arquilla, J. & Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica: RAND.

Bayliss, J., Wirtz, J., Cohen, E. & Gray, C.S. (2002). *Strategy in the Contemporary World*. New York: Oxford University Press.

Buzan, B., Waever, O. & de Wilde, J. (1998). *Security: a new framework for analysis*. Boulder, Colorado:Lynne Rienner Publishers.

Casciani, D. (2004). An online war for hearts and minds. *BBC Magazine* 2(1): 4.

Clarke, R. (2003). *Interview: Vulnerability - what are Al Qaeda's capabilities?* CYBERWAR!. WGBH/Frontline. [On line] Available: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html [23 March 2004].

Conway, M. (2003). Cyberterrorism: The Story So Far. *Journal of Information Warfare* 2(2): 38-47.

Dearth, D. H. (2001). Critical Infrastructures and the Human Target in Information Operations. *Journal of Information Warfare* 1(2): 62-67.

Deeks, A.S., Berman, B., Brenner, S.W. & Lewis, J.A. (2005). Combating Terrorist Uses of the Internet. *American Society of International Law. Proceedings of the Annual General Meeting 2005*. pp.103-115.

Devost M.G., Houghton B.K. & Pollard N.A. (2002). Information Terrorism: Can You Trust Your Toaster? Sun Tzu Art of War *in Information Warfare Research Competition.* Washington DC: Institute for National Strategic Studies, National Defense University.

Emery, N.E. (2005).Fighting Terrorism and Insurgency: Shaping the Information Environment. *Military Review* 85(1): 32-39.

Emery, N.E., Earl, R.S. & Buettner, R. (2004). Terrorist Use of Information Operations. *Journal of Information Operations* 3(2): 34-45.

Farrell, L. (2005). The view from the other side: Terrorist websites and propaganda. *2005 Humanities – Security & Counter-Terrorism Research Forum.* Canberra, Australia: Australian National University.

Furnell, S. M. (2001). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare* 1(2): 35-44.

Henych, M., Holmes, S. & Mesloh, C. (2003). Cyber Terrorism: An Examination of the Critical Issues. *Journal of Information Warfare* 2(2): 1-14.

Hinde, S. (2001). Incalculable Potential for Damage by Cyber-Terrorism. *Computers & Security*, 20: 568-572.

Jones, A., Kovacich, G. L. & Luzwick, P. G. (2002). *Global Information Warfare: How Businesses, Government, and Others Achieve Objectives and Attain Competitive Advantages*. Florida: Auerbach Publications.

Libicki, M.C. (1995). *What is Information Warfare?* Washington DC: US Government Printing Office.

Post, J.M., Ruby, K.G. & Shaw, E.D. (2000). From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. *Terrorism and Political Violence*, 12(2): 97-122.

Radvanyi, J. (1990). *Psychological Operations and Political Warfare in Long Term Planning*. New York: Praeger Publishers.

Rogers, P. (2000). *Losing Control. Global Security in the 21st Century*. London: Pluto Press.

Schwartau, W. (2001). Asymmetrical Adversarialsm in National Defense Policy, The Marketplace and Personal Privacy. *Journal of Information Warfare* 1(2): 1-11.

Shahar, Y. (2003). *Information Warfare: The Perfect Terrorist Weapon.* Institute for the Advanced Study of Information Warfare (IASIW). [On line] Available: http://www.iwar.org.uk/cyberterror/resources/CIT.htm [17 March 2004].

Smith, R. (2005). *The Utility of Force: The Art of War in the Modern World*. London: Allen Lane.

Thomas, T.L. (2004). *Dragon Bytes. Chinese Information – War Theory and Practice*. Fort Leavenworth, Kansas: Foreign Military Studies Office (FMSO).

Thomas, T.L. (2005). *Cyber Silhouettes. Shadows over Information Operations*. Fort Leavenworth, Kansas: Foreign Military Studies Office (FMSO).

Weimann, G. (2006). *Terror on the Internet: The New Arena, the New Challenges*. Washington DC: United States Institute of Peace Press.

Wilson, C. (2005). Emerging Terrorist Capabilities for Cyber Conflict against the US Homeland. *US Congressional Research Service Report*, November 1. pp.1-18.

COPYRIGHT