

Gina Fields
Dr. Pfaltzgraff
Contemporary Perspectives
Tues. & Thurs. 4:05 – 5:50 PM
April 18, 2006
The London Bombings: A Case Study
Part I

The London bombings impacted British society politically, economically, and socially, spreading awareness and fear of terrorism throughout Great Britain. “Thursday, July 7, 2005, will go down as one of the darkest days in British history since the Second World War. At least 52 people were killed in a series of bomb blasts in the heart of London, and several hundred were injured” (Gardiner). Terrorism is a global threat, leaving no one country immune to attacks.

Al Qaida, a terrorist organization, is at the forefront for these global attacks. “Whilst the U.K. has faced a variety of terrorists threats in the past, a unique combination of factors – namely global reach, capability, resilience, sophistication, ambition, and lack of restraint of Al Qaida and associated groups from around the world – place the current threat on a scale not previously encountered” (International Terrorism). In light of the July 7, London bombings, the British government is taking political action to fight the war on terrorism.

Politics

The British government experienced became alarmed when the terrorist attacked the London transit system, forcing them to realize they were susceptible, as well as, unprepared to handle terrorist attacks. Since the London bombings, the British government has been deliberating about anti-terrorism policies, and entertaining the idea

of holding a terrorist suspect up to 90 days without charge. The issues being discussed by British government to prepare for and fight against terrorism has been under scrutiny.

“All public discussion on how to defeat terrorism, in what Tony Blair terms the unique conditions of modern society, is now couched in a simple dichotomy: the tension between civil liberties and security” (Nabulsi). One of the more controversial debates in British government is the anti-terror legislation.

On March 22, 2006, the anti-terror legislation was passed and will shortly become law.

The House of Lords rejected by 172 votes to a 112 a Liberal Democrat amendment which would have removed any reference to prosecution for “glorification” of terrorism. Offenders could be jailed for up to seven years for encouraging or inducing terrorism under the clause, which has angered academics and artists who have warned it an unacceptable limit on freedom of speech. Other critics have condemned it too vague. (Woodward)

Those who support the bill feel those who glorify terrorism are unacceptable and may influence others to commit terrorist acts. “As a consequence of London’s “Black Thursday” – as it is described, and in defending his call for the endorsement of the glorification of terrorism bill, Tony Blair said: “There is no doubt that the rules of the game are changing. He added: “Anyone who has practiced terrorism or has anything to do with it, anywhere, will automatically be refused asylum in our country.” He also stated, “If people want to come here, they come here and play by our rules and our way of life. If they don’t, then they will have to go.” (*Saudi Paper...*) There were, however,

members of Parliament who opposed the bill. “That will give (the Lords) the opportunity to examine a range of issues that have given us deep discomfort in the course of the bill: the definition of terrorism, the use of the word glorification and so on” (Woodward). Due to the unclear definition of glorification, the government as well as security officials will ultimately have a difficult time distinguishing those who are terrorists and those who are not. The government must issue a definite definition of glorification before establishing a bill that would ultimately condemn a person for terrorist involvement; else a person’s rights may be infringed upon, especially expression of free speech.

The British Economy

The London bombings had not only impacted British policy, but also affected their economy. The British economy suffered from the London bombings, especially in sectors concerning retailers in London, tourism, and British government to establish pay compensation to UK victims of terrorist attacks. “Retailers across the region have unquestionably suffered the effects of a consumer crisis of confidence following the London terror attacks” (Yorkshire Post...). After the London bombings, the north of Great Britain appeared to be experiencing lower levels of consumer debt. “After exceeding 3% last year, national GDP growth has declined to around 1.8% in 2005, Commented Dr. Neil Blake, director of economics and forecasting at Experian. “This is one of the worst out-turns since the recession of the early 1990’s, with consumers largely responsible for the dip” (Gleeson). Consumers are still fearful of another terrorist attack, especially in London. Tourism, however, appears to be increasing, once again, especially with British tourists.

Right after the London bombings, tourism, of course, decreased within London. The publication, The Guardian Unlimited, is claiming British tourists are becoming less intimidated to travel. “Two-thirds of British adults said they would not give into terrorism and let it keep them from visiting places that have suffered attacks, a survey from market research company Mintel found” (*British Tourism...*). The article also acknowledged the terrorist attacks that have recently happened in the UK, and states, “the threat is no longer externalized or alien now.” (*British Tourism...*) Another economic issue in response to the London bombings involve a possible plan by government for pay compensation to UK victims of terrorist attacks, in particular those hurt in the London bombings. Recently, Labour’s David Winnick accused that payment to the victims of the London bombings was too slow and “totally inadequate.” (*In Parliament Today*) The government has a political and social responsibility to its people, whether it involves compensation for those victims of the London bombings, or providing aid and guidance to those businesses that may have suffered due to the terrorist attack.

Social Issues

After the London bombings, social issues began to arise, especially those concerning Muslim schools in Britain. “Since the London bombings on July 7th, fears have been growing that Britain is not only allowing, but actually facilitating, the creation of a radicalized Muslim community in its midst. Politicians, including some Labour ones, have attacked multicultural policies and demanded that Muslims integrate more fully. Among the targets of criticism are Muslim schools” (*Britain: Adobe...*). In Britain, there

are currently around 100 Muslim schools, of which 5 have joined the state sector. The remaining Muslim schools are independent and have more freedom to their teaching.

The terrorist attacks on July 7 brought focus from the British government towards the Muslim schools. 108 Muslim schools have shown interest in joining the state sector. “The government is keen to nudge things along because it feels that the way to keep Muslim schools moderate is to bring them into the heavily-regulated state sector. Even if they stay put, however, they will be watched more closely” (*Britain: Adobe...*). The social element being affected here is freedom of religion and interaction with fellow followers. The article points out, “The charge that Muslim schools entrench segregation in British cities is partly true. But the country’s roughly 7,000 Christian state schools can create equally strong barriers to integration.” (*British: Adobe...*)

Lessons and Future Challenges

The London bombings impacted British society, forcing them to acknowledge how unprepared and vulnerable they were to a terrorist attack. There are many lessons learned from the terrorist attacks that took place on July 7 2005, in the London transit systems. Probably one of the most important lessons learned was the government’s response before, during, and after the London bombings. In August The Observer revealed that Saudi intelligence had passed warnings to British and US intelligence in Riyadh in December 2004 about a terror plot aimed at London” (Barnett). There is speculation as to what, if anything had been done with this crucial information.

Another lesson learned is preparedness by local aid personnel, such as police, firefighters, ambulance, EMT, etc. Though the film was fiction, “Dirty War” showed the

lack of supplies, contingency plans, resources, and communication by first responders during a terrorist attack, as well as information by government officials. The British government, however, were not the only establishments that learned possible lessons from the London bombings, so too did businesses. “National surveys show 49 percent of all UK businesses lack plans to keep the wheels turning if the unthinkable happens... After the first wave of attacks on July 7, the heads of businesses found themselves doing staff roll calls, realizing they did not have correct contact details or effective cascade communications systems” (Valentine). Businesses have possibly learned to enforce a contingency plan, designated escape routes, and a designated safe zone away from harm.

A Fashion Apparel Management graduate would enter into the business world, faced with similar decisions and responsibilities for their employees, as well as a company's' business records and information. Today, outsourcing plays a major role in Fashion Management. When outsourcing overseas, it is imperative that one is familiar with the nation's government, culture, and current relationship with the United States. As an Executive Director of an apparel company, it is your duty to ensure the well-being and safety of your employees while in the workplace. Also, cyber terrorism is a global threat that could affect an apparel business. Cyber terrorism can disrupt a business through unauthorized access of computer systems and businesses, the theft of information, stealing data, launch of viruses and hacking into a systems infrastructure. Another duty in relation to Apparel Management and outsourcing is mode of transport for product.

With terrorism as a global threat, port control and inspection is imperative in eliminating possible transfer across borders of biological components and resources for terrorist groups. In light of recent controversy concerning the sale of six American ports

to Dubai Ports World, nations in the fight against terrorism are becoming less willing to do business with heavily Muslim populated nations. “In addition to their claims of terrorism, opponents argue that selling our ports to a foreign company is like outsourcing our security” (Maroshegyi). Challenges an Executive Director of an apparel company may face involve establishing relationships with other companies located in countries who hold unfavorable opinions toward the US, while ensuring the safety of your employees if relocated due to outsourcing. The employer must also have in place adequate communication with your employees and establish a contingency plan for your business in case of crisis.

Part II

As chief executive of a corporation in the apparel industry, our company is responsible for not only the safety of our employees but also the security of both our business and financial records. Our company specializes in the manufacturing and retail of women's apparel. We have production plants and have retail stores located both domestically in the United States, and off-shore, including London. It is imperative that, with the help of our government, as well as the government of the country we may be sourced, our company issues a contingency plan to ensure our business is not completely disrupted during a terrorist attack or a possible threat. A terrorist attack in the form of cyberterrorism could not only cripple our business, but also may lead to complete turmoil.

Cyberterrorism

Experts in the field of IT security have found it difficult to decide on a definition of cyberterrorism. "In fact, the term has been used to describe actions as varied as stealing data and hacking, planning terrorist attacks, causing violence, or attacking information systems" (Foltz). If you were to combine the definitions, however, one

would be presented with the definition that, “cyberterrorism is an attack or threat of an attack, politically motivated, intended to:

- *interfere with the political, social, or economic functioning of a group, organization, or country or
- *induce either physical violence or the unjust use of power, or
- *in conjunction with a more traditional terrorist action” (Foltz).

Researchers speculate that terrorist groups, especially Al Qaida are extremely computer literate and use the Internet as form of recruitment, terrorist planning, and a means to issue an attack.

The Scope and Implications of the Problem

Cyberterrorism is a global threat. “This is the kind of scenario that government and private computer experts will be studying as they look into the growing possibility of a “cyber-terrorist” attack on what is known as our “critical information infrastructure” – the electronic systems vital for government, armed forces, businesses, finance, telecommunications, utilities, or emergency services” (Ross). In relation to my company, a cyber attack could completely disrupt our business, as well as use our company’s ports as a means of transport for terrorist activity.

Manufacturing

Cyberterrorism could greatly affect our manufacturing process. If there was a cyber attack that effected utilities such as electricity, water, and telephone lines, our production would falter, causing our business to be completely incapacitated. The cost to our company would be great, causing us to delay production and delivery of our product to the client. Also, a cyber terrorist could alter information via Internet, during

production, causing a change of product. “Other scenarios posed by various authors include unauthorized access, modification, or theft of information. For example, a cyber terrorist could access a manufacturing facility and alter the formula used to produce a drug or other product, such as cereal so that the resulting products are lethal” (Foltz).

This situation can also relate to apparel; the terrorist possibly mixing a deadly solution that may be applied as a finish to a garment. Another concern our company has in relation to cyberterrorism is the use of our ports.

After September 11 and most recently, the London bombings, the transporting and inspection of cargo has become a priority for most government, including the United States and Britain. Our apparel company has our product shipped from port to port. The threat of terrorism has tightened security within the ports, as well as customs. Measures such as CSI (Container Security Initiative) have been implemented in many ports across the world to deter terrorist activities. “Currently, there are 42 operational CSI ports in Europe, Asia, Africa, the Middle East, and North, South, and now Central America. Approximately 75 percent of cargo containers headed to the US originate or are transshipped from CSI ports” (Key Honduran...). Though many countries are taking initiative to have a more reliable, thorough customs and search system to locate biological components, the CSI still only checks 75%, leaving an entire 25% of cargo completely unchecked and possible suspect cargo. Cyber terrorists could easily use this as an opportunity to corrupt files, using the Internet, allowing them access to this unchecked cargo.

Retail

In wake of the London bombings, retailers in the posh shopping section of London appeared to have suffered the worst in the business sectors. “Retailers across the region have unquestionably suffered the effects of a consumer crisis of confidence following the London terror attacks. It is essential for shops to plan ahead in the even of future emergencies” (Call to...). A cyber attack could have a retailer’s business come to an immediate halt. An attack could destroy a businesses electronic records and electrical and telecommunications could be wipes out. A retailer relies on computers to not only communicate to their home office, but also to the manufacturer. Information such as sales reports, SKU’s, financial records, merchandising records, and human resource information could fall victim to a cyber attack. The store itself would suffer from cyberterrorism, possibly loss of electricity could completely disrupt a business, being unable to service the consumer. Our company would immediately lose money due to a cyber attack and could quite possibly never be able to recover in the long run.

Responses to Cyberterrorism

Though apparel companies and cyberterrorism have not been directly influenced by the London Bombings, other than retail shops located within the shopping sector of London, terrorism in general has sparked awareness in many businesses. Preventing cyberterrorism is still a relatively new process. “With security procedures under review at companies across the country, officials are urging that business owners improve computer network security as part of that effort to prevent both industrial espionage and

cyber terrorism” (Carter). It is the company’s responsibility to secure its business information as well as provide ways of ensuring their operations are not disrupted.

Researchers suggest that many times a virus occurs or a business experiences some form of disruption, it is done internally. One initiative made by businesses is evaluating the background of an employee. Richard Oertle, an official with ExecuTrain, a computer training company, stated, “that a thorough check of a person’s background could be done easily and quickly through the Internet. If any aspect of a person’s resume is not accurate, officials should move on to the next applicant (Carter). The issue with this solution, however, is now days, a person’ especially a cyber terrorist, could easily forge information about themselves on the internet.

Another response to cyberterrorism is CIA models, found within the Handbook of Information Security Management. “The CIA models all offer some degree of protection against cyberterrorism; however as Bort (2002) notes, these goal oriented models are somewhat limited, even in terms of defending organizations against computer misuse, let alone cyber terrorism(Foltz). The CSM (computer security model), however, is intended to be a safeguard for information systems against an attack. The model serves as a detective as well as a preventative. This model, however, usually will only identify an internal enemy. (Foltz)

The third response our company made is directly influenced by the London bombings. Since our company does have retailers located within the London shopping district, we decided to respond to the attacks with establishing a contingency plan. After the London bombings, James Hart, commissioner of the City of London Police, called on all businesses to establish a contingency plan, and for larger businesses to provide

assistance to the smaller companies. (Business...) It is important to know your surroundings and your fellow companies in case of a terrorist crisis. "Police would recommend that all businesses become as familiar with their environment as possible: monitor vehicles being parked in the vicinity of the buildings. Undertake regular external patrols to ensure there are no suspicious bags or items left in the vicinity of the building" (Business...). A company should also be aware of who is in the building at all times, as well as have access controls in place. In regards to cyberterrorism, a contingency plan such as this can ensure the safety of employees, especially if there is loss of power. A continuity plan would also have adequate exits and safe zones. A business should also implement some kind of software that may prevent a direct cyber attack on the company's computer.

What Steps Remain to be Addressed

In regards to cyberterrorism, the London government, along with other countries has done little to fully prepare the country during a cyber attack. Because the definition of cyberterrorism is still unclear, this makes it difficult for the government to charge someone with the crime. The financial costs can be great if every company was to install a preventive software model against cyberterrorism. Even if the company was to install such devices, it does not ensure a cyber attack would still not occur. However, though the initial cost may be expensive to install such software, in the long run, it will benefit the business by keeping the company safe from cyberterrorism, and prevent disruption. In regards to cost as a whole to prevent cyberterrorism within my own business, the company should take responsibility.

The use of cyberterrorism could ultimately cripple an entire society. In this day and age, everyone relies on computers. Computers are used as communication, record and data storage, utility access, financial system, and so on, making technology an incredible force in our lives. Also, the Internet is a global phenomenon, creating an anonymous environment and easy access for terrorists to converse with one another. Though IT technologists are developing new software all the time to prevent a cyber attack, its still virtually unattainable to prevent all forms of an attack, whether it's a virus or computer hacking; as long as the Internet exists, it remains a playground for terrorist activity.

Works Cited

- Barnett, Antony. "UK was warned of July Suicide Attacks." 5 February 2006.
<http://politics.guardian.co.uk>. 23 March 2006.
- "Britain: Adobe of Islam; Religious Schools." The Economist. 13 August 2005.
Vol.376. Proquest. 20 March 2006.
- "British Tourists 'Not Put Off by Terrorism.'" Guardian Unlimited. 24 March 2006.
Lexis-Nexis. 26 March 2006.
- Business and the Terror." Financial Times.com. 17 August 2005.
- "Call to Shops over Emergencies." Yorkshire Post (England). 22 September 2005.
- Carter, Ray. "Terrorism Spurs Call for Network Security Upgrades." The Journal Record. 19 November 2001. ProQuest. 12 April 2006.
- "Dirty War." HBO. 2005.
- Foltz, C Bryan. "Cyber terrorism, Computer Crime, and Reality." Information Management & Computer Security. 2004. ProQuest. 12 April 2006.
- Gardiner, Nile and James Phillips. "The London Bombings: How the U.S. and the U.K. Should Respond." 21 July 2005. <http://www.heritage.org>. 21 March 2006.
- Gleeson, Bill. "North-South Gap Set to Close – for the Time Being; Terrorism Fears Hit London." Daily Post (Liverpool). 7 December 2005 Lexis-Nexis 26 March 2006.
- "In Parliament Today." Parliamentary News. 19 October 2005. Lexis-Nexis. 26 March 2006.
- "International Terrorism." <http://www.mi5.gov.uk>. 21 March 2006.
- "Key Honduran Apparel Port Selected for CSI." Florida Shipper. 6 February 2006.
Lexis Nexis. 23 March 2006.
- Maroshegyi, Chris. "Port Controversy Brings to Light Intolerance toward Arab World."

- The Heights. 17 March 2006. Lexis-Nexis. 23 March 2006.
- Nabulsi, Karma. "Don't Sign up to this Upside Down Hobbesian Contract." Guardian. 22 March 2006. <http://politics.guardian.co.uk>. 24 March 2006.
- Ross, Dickon. "Electronic Pearl Harbor." Guardian. 20 February 2003. <http://politics.guardian.co.uk>. 24 March 2006.
- "Saudi Paper Welcomes UK's Latest Antiterror Law." BBC Monitoring International Reports. 26 February 2006 Lexis Nexis. 22 March 2006.
- Valentine, Jo. "Companies must Plan for the Worst, and Hope for the Best." 25 July 2005. FT.com. 20 March 2006.
- Woodward, Will. "Terror Bill Ping-Pong Over as Tory Peers Back 'Glorification' Clause." Guardian. 23 March 2006. <http://politics.guardian.co.uk>. 24 March 2006.
- "Yorkshire Post: Call to Shops over Emergencies." Yorkshire Post (England). 22 September 2005. 23 March 2006.

