# A framework for cyber war against international terrorism

Arash Barfar

Information Systems and Decision Sciences,
College of Business,
University of South Florida,
4202 East Fowler Avenue, CIS 1040,
Tampa, FL 33620-7800, USA
E-mail: abarfar@usf.edu

Kiyana Zolfaghar* and Shahriar Mohammadi

Faculty of Industrial Engineering,
KN Toosi University of Technology
P.O. Box 19395-1999, No. 17, Padis St.,
Molla-Sadra St., Vanak Sq., Tehran, Iran
E-mail: kzolfaghar@sina.kntu.ac.ir
E-mail: s.mohammadi@kntu.ac.ir
E-mail: smohammadi40@yahoo.com
*Corresponding author

**Abstract:** Nowadays, most of the countries have come to this conclusion that their plan for counter terrorism should be changed from 'passive' to 'active'. Consistently, this should be reflected on the internet as an important channel of communication and doing business in many countries. However, there are different barriers to achieve an effective online counter terrorism such as lack of 'cooperation' and 'universal legislation'. Accordingly, the first step of moving toward an effective online counter terrorism is to relieve these barriers. In this paper, a framework is proposed that aims at relieving these problems, using 'honeypots' and 'web mining' techniques by organising national efforts.

**Keywords:** online security; international terrorism; honeypots; web mining; universal legislation.

**Reference** to this paper should be made as follows: Barfar, A., Zolfaghar, K. and Mohammadi, S. (2011) 'A framework for cyber war against international terrorism', *Int. J. Internet Technology and Secured Transactions*, Vol. 3, No. 1, pp.29–39.

**Biographical notes:** Arash Barfar is currently a PhD student and Graduate Assistant in Information Systems and Decision Sciences at the University of South Florida. His current research interests include modelling online consumer behaviour and decision, trust, e-commerce success models, data mining, data warehousing, decision support systems and information security. His research work has been published in the proceedings of refereed conferences.

Kiyana Zolfaghar earned her Bachelor's degree in Information Technology Engineering from Amirkabir University of Technology, Tehran, Iran She is now working on her thesis in order to earn her Master's degree in Information Technology Engineering-Electronic Commerce from KN Toosi University of Technology (KNTU). Her research has focused on trust and reputation systems in social web applications. She is also interested in the fields of data mining, social network analysis, semantic web and user behaviour in electronic commerce.

S. Mohammadi is a former Senior Lecturer at the University of Derby, UK. He also used to be a Network Consultant in the UK for more than 15 years. He is currently a Lecturer in the University of Khajeh, Nasir, Iran. His main research interests and lectures are in the fields of networking, data security, network security, and e-commerce.

## 1 Introduction

Since September 11, counter terrorism programs have been changed in many countries. In other words, legal forces of different countries such as police and secret services do not wait until an act of terror committed by terrorists and then start to fight against them. On the other hand, legal forces of many countries have come to this conclusion that these methods are not efficient anymore and they must find a way that enables them to prevent these kinds of attacks. This is necessary, since the consequences of such attacks can be catastrophic. Accordingly, different channels that can be utilised for evil aims by terrorists are being actively controlled by legal forces.

The creation and increased use of the internet has changed our world in different manners. This new medium for information and communication changed how people live their daily lives, and has made unprecedented amounts of information available to a significant percentage of the global population.

But the internet has a very fragile framework which is at risk from attacks, historically it was sole hackers, but we are now seeing the development of cyber terrorist organisations. Considering that the internet is a very important channel not only for communication, but also for searching information and doing business, the pattern of counter terrorism should efficiently be reflected in that. In order to do so, different barriers that tie the experts' and legal forces' hands in online counter terrorism should be relieved.

In this paper, we aim at proposing a framework for achieving this. The remainder of this paper is organised as follows: in Section 2 we give some background information on terrorism concept, review the changes in counter terrorism methods in September 11 chronology and its reflection in online counter terrorism. Section 3 describes the major barriers to achieve effective online counter terrorism, and in Section 4, we present our proposed framework and describe its components. Finally, we conclude this paper in Section 5.

## 2 Terrorism

Many authors have defined terrorism from their perspectives. Consistently, there is a lack of consensus on a single definition for the word 'terrorism'. Nonetheless, a comprehensive definition which can encompass most of the rest is presented by Lutz (2002), in which he defined 'terrorism' as the use of force for political or religious motives.

Despite this lack of consensus among authors, most of them distinguish between the aims and the means being used when that they want to categorise 'terrorism' (Sorel, 2002).Consistent with this observation, Duez (2002) mentions that terrorism can be seen through three lenses: the aim, the methods and the expected consequences.

### *2.1 Counter terrorism*

Before September 11, terrorism was not considered as a major threat against the world. No one even believed that such incident happened in a city where The United Nations is located. Thus, after September 11 leaders of the world were woken up by an alarm warning about a new dreadful threat against the world: 'terrorism'. The first consequence of this was changing the pattern of counter terrorism from *passive* to *active*.

In *passive counter terrorism*, legal forces such as police waited until the acts of terrorism happened, and then they start the fight against that. However, September 11 and its consequences demonstrated that this method has lots of deficiencies. Renowned people such as the former President of the USA, Bill Clinton (2002), complained that September 11 could have been prevented. He, in November 6, 2002 lecture, mentioned that not long after the events of September 11, 2001, FBI agents examined great amounts of consumer data and found that five of the terrorist perpetrators were in the database. One of the terrorists possessed 30 credit cards with a combined balance totalling $250,000 and had been in the country for less than two years. The terrorist ring leader, Mohammed Atta, had 12 different addresses, two real homes, and ten safe houses. Clinton concluded that we should proactively search through this type of data and that "if somebody has been here a couple years or less and they have 12 homes, they're either really rich or up to no good. It shouldn't be that hard to figure out which". In a nutshell, what Clinton stated is that passive counter terrorism is useless and the acts of terror should be prevented through active counter terrorism.

Accordingly, September 11 has stimulated many countries to reconsider the effectiveness of their existing counter-terrorism policies and legislation. In Germany, as an illustration, the authorities renewed their policies and legislation that enables them to identify spies known as *sleepers* by seeking to identify persons who have always appeared to be behaving like good citizens and obeyed the law. Prior to September 11 this method was only used by the secret services, but it is now apparently applied by the German police forces.

Also, throughout the USA many states have modified their legislation against terrorism by introducing comprehensive anti-terrorist acts use of repressive actions. The ones who did not change their legislations asserted that their existing legislation and policies are sufficient to deal effectively with terrorism (IBA, 2003).

These modifications have resulted in some successes such as preventing the terrorists attack in Germany's airports. However, attacks such as the one happened in two hotels in India showed that these counter terrorism activities should be strengthened by the law and governments.

### *2.2 Cyber terrorism on the web*

Apparently, terrorists' attitudes reflect in their activities on the web. In this context, terrorists can come in many forms such as politically motivated, anti-government, anti-world trade, and pro-environmental extremists (Janczewski and Colarik, 2008). By taking full advantage of the unique benefits the internet provides, terrorist groups have been able to more effectively carry out their goals with less risk of apprehension. Weimann (2004) found that by 2000 practically all terrorist groups had established a presence on the internet and had developed their own websites. They might show interests in specific concepts on the web, such as the ones related to espionage, explosives and camouflage etc. They might also interact with each other by email or other facilities which offered by internet. Moreover, based on their aim, some of them may attempt to gain access to online forbidden systems, in order to gain information about various secret aspects of a subject. In summary, the use of internet by terrorists appears to diverge into two distinct modes neither of which is mutually exclusive. The first aligns to the view that terrorists will use the internet as a platform to launch cyber attacks against critical infrastructure nodes as well as key government and private sector networks and the second mode in which primary use of the internet by terrorists will be to recruit, train, communicate and gain information about potential targets by conducting virtual reconnaissance (O'Rourke, 2006). The unique design of the internet has made it especially conducive to the needs of these terrorist groups because The internet takes very little skill to use, has few regulations, provides a worldwide audience to whom information can be sent quickly at a low cost, and allows for anonymity of the user (Freiburger and Crane, 2008; Lachow and Richardson, 2007). So it is important to continually monitor the use of the internet by terrorists and the material they circulate examined in an effort to both understand their motivations and prevent further attacks.

#### *2.2.1 A simple scenario*

Let us imagine a simple scenario which is now possible to happen in any countries. It is true that a naïve chemical student may search for explosives on the web, a young soldier may search for different ways of camouflage, a witty man may send an email to his colleague about hijacking the plane taking them to Kish Island for vacation to scare their colleagues and make them laugh, and a white hat hacker may try to crack the Iran Air database to test its vulnerabilities.

Obviously, none of these individuals are going to really commit a terror. But what if these individuals were related? In this case, we should expect a disaster happens in an airplane/airport, in with many civilians as casualties. The focus of this research is on the ways that, this incident could be prevented only with the information we have gathered from the internet, as a real active counter terrorism.

With the use of proposed pattern of active counter-terrorism in the web, this research suggests that some of the acts of terrorism, at least ones that utilise the internet in different manners can be prevented.

## 3 Barriers to achieve effective online counter terrorism

Obviously, we should make our strong effort to make the internet an unsafe environment, in a way that they fear to use it for their evil aims. The question is: what are the barriers in this way?

One of the main barriers to achieve online counter terrorism which tie our hands is legislation. Current legislation, especially the ones related to privacy (FTC Report, 2000), does not let us to trace suspicious people on the web. The trace that can efficiently done by the use of intrusion detection systems (IDS) such as honeypots. This situation resembles the one before September 11 in which anti terrorism activities such as eavesdropping were forbidden by law. In fact, there is a constant gap between technological advances and the catching up of legal community with these changes. So usually computer system misuse cases are by far the first ones to be ruled in a number of jurisdictions.

Another barrier in this way is lack of cooperation between organisations and secret services of different countries. Every organisation faces the threat from cyber terrorism. These threats are sometimes high and sometime low, but always need to be taken seriously. Building individual defences will not always be enough to reduce threats. Quite often a wider cooperation is required. To illustrate, in the simple scenario discussed in Section 2.2.1, in order to become capable of revealing the terrorists aim, there should be a close cooperation between search engines and mail services being used by terrorists, Iran Air and Iranian police. Apparently, without this cooperation, it is not possible to prevent the act of terror.

Reputational damage is another point of concern. Organisations' reluctance to relieve the news that their information systems are hacked by anonymous people is a major barrier to achieve counter terrorism in cyber space. This reluctance may seem rational considering that they do not like their systems to be presented unsecured and unreliable. In other word, no system owner wants to lose its customer base just because it was attacked and it exposed it out by going to law enforcement and found the attacker. In our simple scenario, if the Iran Air does not mention that its database is hacked by an individual, one of the pieces of the puzzle is still hidden that does not let us find about the terrorists' plan.

## 4 Proposed framework

Obviously, the first step in achieving an effective online counter-terrorism is to prepare the corresponding infrastructure, by relieving the barriers mentioned in the previous section. In this part we aim at proposing a framework that tends to pave this way.

In order to achieve our proposed framework, we present some hypotheses that are necessary to solve the problem in Section 3.

H1 Summit meetings consisting judiciary systems and secret services of different countries, role player organisations on the web and organisations which are more vulnerable to the acts of terrors will be beneficial to revise the current legislation against terrorism in a way that pave the way for online counter terrorism.

Holding an international summit on countering cyber terrorism is the first international treaty on actions of terror committed via the internet. Notwithstanding the emphasis placed on the need for concerted international action to confront the problem of terrorism, positive international law is far from treating the issue of defining the criminal notion of terrorism coherently (Filippo, 2008). As it is mentioned in previous sections, current legislation may tie our hands for online counter terrorism activities. As an illustration, the current law of privacy forbids investigation of suspicious people activities on the web. Clearly more work is required at the international level to enact legislation that can successfully meet the challenges posed, by the exploitation of the internet by terrorist entities

However, periodical summits consisted of judiciary systems and secret services of different countries, role player organisations on the web such as famous search engines and mail service providers and organisations which are more vulnerable to the acts of terrors such as airlines will reveal the need to revise the current legislation and necessary improvements. Apparently, attendance of different governments' representatives will ease further revisions in current legislation.

H2 Summit of judiciary systems and secret services of different countries, role player organisations on the web and organisations which are more vulnerable to the acts of terrors will result in their further cooperation in the field of online counter terrorism.

As we mentioned in Section 3, one of the barriers to achieve effective online counter terrorism is lack of cooperation between different organisations and secret services of different countries. In such summit, these organisations can negotiate on their further cooperation in order to lead to effective counter terrorism.

These organisations should collaborate with each other producing results and solutions. They may also act on behalf of analysts and other law enforcement officials in combating terrorism.

H3 Revision of legislation will ease the usage of web mining for investigating terrorist's activities on the web.

As we will discuss later in this section, web mining plays an important role in tracing the suspicious people on the web. There has been much debate recently among counter-terrorism experts, civil liberties organisations, and human rights lawyers about the privacy of individuals. That is, gathering information about people, mining information about people, conducting surveillance activities, and examining personal communications such as e-mail and phone conversations are all threats to privacy and civil liberties. In other words, current law of privacy does not let experts apparently trace people on the web. However, revision in the current legislation will relieve this problem. So we need to involve law makers to determine privacy laws as well as to put together a plan for privacy-sensitive data mining.

H4 Revision of legislation will ease the usage of honeypots for discovering the terrorist attempts in hacking the information systems.

As we will see later in this part, honeypots are important tools in finding the attempt of terrorists for hacking the information systems. Currently, legislation does not support usage of these tools. The basic legal themes related to honeypots usage can be summarised to Entrapment including enticement, Privacy and liability (Spitzner, 2003).

In fact, honeypots are not a form of entrapment since they do not induce anyone. Attackers find and break into honeypots on their own initiative. They have already decided to commit an unauthorised activity and honeypots are merely providing a different target for the blackhat to attack. Therefore, in most cases involving honeypots, entrapment is not an issue.

Another major concern and the most complex legal issue related with usage of honeypots is privacy. To determine if a honeypot does violate an individual's privacy, there are two major factors: what the honeypot is being used for and how much information it is collecting. These two factors influence the privacy legal implications. But these factors are not only relevant to honeypots but to all IDS, firewall logging etc and There are various situations and debates related to this issue in literature.

The last major issue in deployment of honeypot is potential liability for the owner. In this regard liability can be defined as *"the requirement of the actor to confirm to certain standard of conduct, for the protection of others, against reasonable risks"* (Zimmerman et al., 2002). *In the case of honeypots*, if they are developed and deployed on an online network, it is the network owner duty to take 'due care' that they don't expose inadvertent loopholes by which other systems can be thrown at risk. Fortunately, there are possible solutions to this problem such as lessening as much outbound connections from honeypots as possible (Spitzner, 2002).

Thorough insight into these legal concepts related to honeypots revealed that these issues can be resolved by close cooperation between different online organisations. So the current legislation should be revised in a way that makes the usage of honeypot legal for counter terrorism purposes.

H5 Cooperation between secret services of different countries, role player organisations on the web and organisations which are more vulnerable to the acts of terrors will make web mining possible.

In order to trace the potential terrorist on the web through web mining, we should have access to log of the important sites he or she goes through. One major concern for us is data sharing for data mining. We need to have complete and accurate data for data mining. Otherwise, we may not be able to find useful patterns. This means that different organisations on the web should be willing to share data and mine it collaboratively. Consistent with this observation, close cooperation between the role players on the internet and secret services of different countries is inevitable.

H6 Cooperation between secret services of different countries, role player organisations on the web and organisations which are more vulnerable to the acts of terrors will ease the usage of honeypots.

Cooperation of different role players on the internet and secret services will lead to deciding different honeypots located on the web. In other words, different organisations on the web will be aware of the existence of their honeypots on the web.

Promoting widespread deployment of honeypots on the web should be an explicit universal policy. Isolating islands of honeypots lack the deterring power of a network infrastructure for deception (Schrage, 2004). Implementing such a policy invites fundamental rethinking of relationship and cooperation between different online organisations that must develop a plan to best use honeypot technologies to detect attacks, track down terrorists and initiate plans to better respond to them.

H7 Honeypots will be beneficial to trace the terrorists on the web.

As we mentioned in Section 3 the organisations may be reluctant in revealing that their information systems being hacked by individuals and this may result in the loss of one the effective counter terrorism puzzles. Honeypot is a solution for this barrier.

Honeypots are "*information system resources whose value lies in unauthorised or illicit use of that resource*" (Spitzner, 2002). They are primarily used for detection and are often used in conjunction with IDS (Provos, and Holz, 2007). In these cases they serve as *production honeypots*, extending the IDS and performing an advanced detection function. One of the most important benefits of honeypots is detecting attacks which are not caught by other security systems, such as IDS which needs a database with frequently updated signatures of known attacks: if an intruder finds a vulnerability which is not in that database, he will have the upper hand (Barfar, and Mohammadi, 2007). Honeypots can be categorised by the level of interaction between intruder and system: low-interaction, high-interaction and medium-interaction (Spitzner, 2002).

Consistent with this observation, utilising honeypots, organisations will not more fear about revealing that there was an attempt to crack their information systems and voluntarily announce about that attempt.

H8 Web mining will make tracing the terrorists on the web possible.

Web mining is a growing collection of computational techniques for automatic analysis of structured, semi-structured, and unstructured online data with the purpose of identifying important trends and previously unknown behavioural patterns (Han and Kamber, 2006). Due to the extent of internet usage by terrorist organisations, cyber space has become a valuable source of information on terrorists' current activities and intentions (Last and Kandel, 2005).So it would be beneficial to identify temporal trends in this terrorist-related data and track down the 'target audience' of their messages. The current number of known terrorist sites is so large that a continuous manual analysis of their multilingual content is definitely out of the question. This is why the automated Web mining approach is so important for the cyber war against international terror. Web mining techniques can be used for detecting and preventing terrorism. In this case we can match the activities of a potential attacker with patterns collected from honeypots to predict their future activities. The goal of web data mining then is to analyse data and make predictions and trends in real-time. For instance we can exploit web usage mining to analyse the usage of Web pages by terrorist groups. Web traffic analysis, click stream analysis, giving advice to Web users about browsing patterns, etc., are also part of web usage mining which can be used to find out the plans of adversaries (Thuraisingham, 2003). That is, we can mine the Web activities of terrorists to get information about their plans. We need to follow up on who they visit on the line, whom they are exchanging e-mail with, how many times they visit a Web page, and many other details to develop profiles of terrorists.

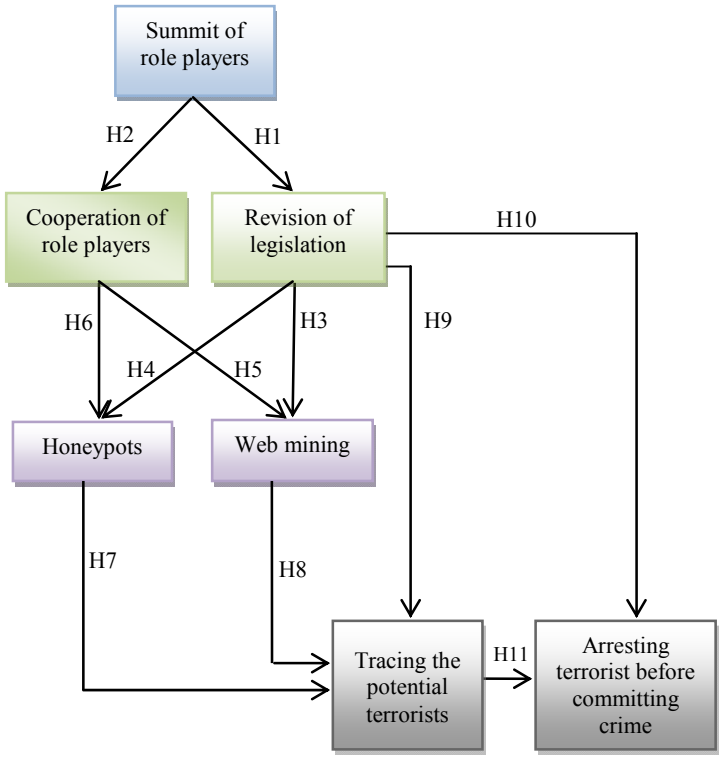
H9 Revising legislation will make tracing the terrorists on the web possible.

H10 Revising legislation will make arresting the terrorists before committing crime possible.

H11 Tracing the potential terrorists on the web can lead to arrest them before committing the crime.

Considering the hypothesis presented in this section, Figure 1 represents the framework that aims at relieving the barriers to achieve online counter terrorism.

**Figure 1** Proposed framework to relieve barriers and achieve online counter terrorism (see online version for colours)




## *4.1 Countering attack scenario based on proposed framework*

After the terrorist attacks of September 11, 2001, concerns about airline security increased dramatically. Shedding some light on our proposed framework mentioned above, we imagine a likely scenario in which a group of terrorists intend to hijack a plane from specific airline. In order to start a campaign of terror, they may use internet in different manners from interacting with members in terrorist group to collecting required information. In the first step, they may decide to hack the airline website and databases to capture or modify some of the information about the flights and their passengers. Combating the potential attackers, the airline designs some honeypots similar to its online systems in cooperation with role players on the web (H6) and makes use of them according to new laws (H4). These honeypots not only can alert the airline about imminent terrorist events but also help them know who are these potential terrorists and what kind of data they searching for without making them aware of being tracked. In this stage they can code the attackers who have any interaction with honeypot and trace them on the web to find which sites they visit and who they communicate and exchange messages to identify their cooperators in real world and collect more information about

their plans (H7). To achieve this, the airline can also use web mining techniques to extract more information about the attackers in order to trace them in real-time (H8) and develop profiles of the potential terrorists. We expect much of the data to be on the web. So different organisations and online role players like search engines will have to collaborate via the web to gather data required for web data mining (H5) and analyse this data based on new legislation that supports from investigation of suspicious people activities on the web (H3). Tracing the potential terrorist help the airline and intelligence services arrest these terrorist before committing the terror (H11) based on the revised legislation (H9) approved by summit of role players (H1) and evidences gathered over online investigation.

## 5 Conclusions

Considering that the consequences of the acts of terror can be catastrophic in every country, the pattern of counter terrorism has changed from passive to active. This should also reflect in online environment. In order to do so, the barriers to achieve an effective online counter terrorism should be relieved. The framework that is discussed in this paper aims at paving the way of online counter terrorism, which will be achieved by holding a summit of role player organisations on the web to follow two main objectives. First, they should strengthen the cooperation between role players on the internet and intelligence services to support the organisation which are more vulnerable to the acts of terrors such as airlines and the second step is the revision of current legislation in order to make the use of honeypots and web mining legal for counter terrorism purposes. These tools would help us to trace terrorists in real-time and arrest them before committing a crime.

## References

Barfar, A. and Mohammadi, S. (2007) 'Honeypots: intrusion deception', *ISSA Journal*.

Clinton, B. (2002) New York University speech', Salon.com, available at http://www.salon.com/politics/feature/2002/12/06/clinton/print.html (accessed on 6 December 2002).

Duez (2002) 'De la définition à la labellisation: le terrorisme comme construction sociale', in Bannelier et al. (Ed.): *Supra Note*, Vol. 1, p.105.

Filippo, M.D. (2008) 'Terrorist crimes and international co-operation: critical remarks on the definition and inclusion of terrorism in the category of international crimes', *European Journal of International Law*, Vol. 19, No. 3, pp.533–570.

Freiburger, T. and Crane, J.S. (2008) 'A systematic examination of terrorist use of the internet', *International Journal of Cyber Criminology*, pp.309–319.

FTC Report to Congress (2000) *Privacy Online: Fair Information Practices in the Electronic Marketplace*, available at http://www.ftc.gov/os/2000/05/index.htm (accessed on 22 May 2000).

Han, J. and Kamber, M. (2006) *Data Mining: Concepts and Techniques*, Morgan Kaufmann Publishers.

International Bar Association (IBA) (2003) *International Terrorism: Legal Challenges and Responses*, Transnational Publishers, Ardsley, p.186.

Janczewski, L.J. and Colarik, A. (2008) *Cyber Warfare and Cyber Terrorism*, (an imprint of IGI Global), Information Science Reference, USA.

Lachow, I. and Richardson, C. (2007) 'Terrorist use of the internet: the real story', *JFQ: Joint Force Quarterly*, pp.100–103.

Last, M. and Kandel, A. (2005) 'Fighting terror in cyberspace', *World Scientific*, Series in Machine Perception and Artificial Intelligence, Singapore, Vol. 65.

Lutz (2002) 'Was ist Terrorismus? Definitionen, Wandel, Perspektiven', in H-J. Koch (Ed.): *Terrorismus Rechtsfragen der Äußeren und Inneren Sicherheit*, pp.9–10.

O'Rourke, S. (2006) 'Global reach: terrorists and the internet', Paper Presented at the *Proceedings of the 7th Australian Information Warfare and Security Conference*, Perth, Western Australia.

Provos, N. and Holz, T. (2007) *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, Addison Wesley Professional, Reading.

Schrage, M. (2004) 'Digital dishonesty as best policy', *Breakthroughs Magazine*.

Sorel (2002) 'Existe-t-il une définition universelle du terrorisme?', *Le Droit International Face au Terrorisme*, p.38.

Spitzner, L. (2002) *Honeypots: Tracking Hackers*, Addison Wesley Professional.

Spitzner, L. (2003) *Honeypots: are They Illegal*, available at http://www.symantec.com/connect/articles/honeypots-are-they-illegal (accessed on 12 December 2009).

Thuraisingham, B. (2003) *Web Data Mining and Applications in Business Intelligence and Counter-Terrorism*, Auerbach Publications.

Weimann, G. (2004) How Modern Terrorism Uses the Internet, United States Institute of Peace, Washington DC, available at http://www.terror.net (accessed on 6 December 2002).

Zimmerman, S., Plesco, R. and Rosenberg, T. (2002) *Downstream Liability for Attack Relay and Amplification – Citation from RSA Conference 2002*, San Jose, California, available at http://www.cert.org/archive/pdf/Downstream_Liability.pdf.