UDC 623.6

Robert Brumnik

Faculty of Criminal Justice and Security, University of Maribor, Ljubljana, Slovenia

TERRORISTS CYBER ATTACKS AND ICTD INDEX

Terrorism and the Internet are related in two main ways. First, the Internet has become a forum for terrorist groups and individual terrorists both to spread their messages of hate and violence and to communicate with one another and their sympathizers. Secondly, individuals and groups have tried to attack computer networks, including those on the Internet, what has become known as cyber terrorism or cyber warfare. Digital development index is indicator which measures the level of Information Communication Technology (ICT) adoption of countries. Purpose of this article is to find correlation functions of Denial-of-Service (DoS) attacks (most known cyber terrorist method) and index of digital development of countries and provide information of their relations.

Keywords: *Psychological Warfare, Cyber Terrorism, Cyber War.*

Design/methodology/approach. The paper gives a comparative literature review of cyber terrorism methods and activity and will be a summary of the selected sources to combines both summary and synthesis. A literature search of articles published from January 1997 to December 2010 dealing with research studies comparing results of DoS attacks with the U.S. Company Symantec and Digital Development of worldwide countries with International Telecommunication Union is carried out. Literature reviews of two relevant research papers (research of the digital development index and research of internet Denial-of-Service attacks) will provide a background for our overview analysis which gives us a new interpretation of these correlation researches.

Findings: Computer security vulnerabilities may expose critical infrastructure and government computer systems to possible cyber attacks by terrorists, possibly affecting the economy or other areas of national security. A correlation research of the index of digital development ICTD (Information Communication Development Index) of a country shows that ICTD has no significant effects on the DoS index. There is no significant difference in the DoS index between countries with high and low ICTD index, which confirms that cyber terrorists do not choose between the digitally developed and undeveloped countries. These conclusions cannot confirm the proposed hypothesis that digitally higher developed countries are more exposed to internet terrorism (digital war) than countries with lower ICTD index.

Research limitations/implications: The limitation of this paper is to put forward a comparison scale to rank several EMEA (Europe, Middle East, and Africa) and APJ (Asia, Pacific and Japan) countries according to their ICTD and DoS index. In this paper we will discuss ten EMEA and APJ countries with the highest DoS index.

Practical implications: First, the paper explains practical cases of technologies underlying computer viruses, worms, and spyware, how these malicious programs enable cyber crime and cyber espionage, and which tactics are currently used by computer terrorists-

hackers for the planning of internet terrorism. Secondly, the paper offers a critique of the interpretation of internet terrorism, which has gained considerable popularity in the media.

Originality/value: Potential issues presented in this paper deal with the following questions: Is there an appropriate guidance for known practices of warfare response to cyber attacks or the need for detecting possible Al Qaida psychological warfare and Muslim hackers club's terrorist activity with cyber data mining? Do roles and responsibilities for protecting against a possible cyber terrorist attack need more clarity for government, industry, and home users and, should the sharing of information on cyber threats and vulnerabilities between private industry and the federal government be further increased?

Introduction

Terrorists are increasingly using the internet as means of communication with each other and the rest of the world. Terrorists use the internet in different ways to raise funds, collect resources, plan attacks, spread propaganda and recruit adherents. Nowadays, the internet is also being used to train terrorists given the closure of larger training camps in Afghanistan. Terrorist affiliated entities and individuals have also established internet-related front businesses as means of facilitating communication among terrorist cells and raising money. A terrorist group may also gain control of a legitimate charity and use it to accept electronic value held in bearer smart cards as donations which in reality could be the proceeds of drug trafficking (Kaplan, 2009). The earliest academic literature on Internet terrorism was produced by experts on online security, Hayward (1997), Cohen (2002), Denning (2005), Furnell and Warren (1999). Although the literature did not deal with the topic in an academic context, it still offers a good description of today's situation. By now, nearly everyone has seen at least some images from propaganda videos published on terrorist sites and rebroadcasted on the world's news networks. Western governments have intensified surveillance of such sites, but their prosecution of site operators is hampered by concerns over civil liberties, the internet's inherent anonymity, and other factors.

Digital wars can be defined as a specific type of information warfare (Giacomello, 2003). The term Information Warfare (IW) has been applied to a rather dissimilar (and often incongruent) collection of situations. Its origins can be traced back to the Gulf War, when the UN coalition simply annihilated Iraq's information systems (Campen, 1992). The official US Department of Defense's (DoD) definition of IW is: »Actions taken to affect adversary information and information systems while defending one's own information and information systems« (DoD, 1998). The current use of the term, however, has come to include precision-bombing of enemy's information infrastructure, cyber terrorism and cybercrime, script kiddies practicing Denial-of-Service (DoS) attacks on commercial Web sites, Web defacement, etc. Libicki (1995) identified seven forms of IW, of which cyber war is only one. In an effort to clarify the matter, Arquilla and Ronsfeld (2001) have recently distinguished between cyber war and net war. However, the NATO nowadays tends to distinguish between Computer Networks Attacks (CNA) and Computer Networks Defense (CND), also called the Information Assurance. The present plethora of various »e-something« (e-jihad, e-intifada, electronic Pearl Harbor, electronic Waterloo etc.) are both confusing and meaningless, and is of immediate use only for the media, who tend to consider all these terms rather modern, which often causes confusion of terms (Giacomello, 2003).

Problem. A global strategy and policy for combating this type of terrorism are needed. It is also necessary to know that methods of terror, producing destruction, and fear can be much more destructive online than other conventional methods in the real world.

Problem case has happened during the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings (Acharya, 2008).

Next case for example is Estonia, heavily dependent on modern technology, who recently implored NATO to take a position against cyber terrorism after accusing Russia of cyber terrorism against their country. Estonia is experienced attacks on their government, banking, and media websites in year 2007. These attacks used a Distributed Denial of Service (DDoS) attack which flooded Estonian websites with false information shutting down a number of governments (including military) and banking sites rendering the country extremely vulnerable. The Estonian government has been able to trace the initial IP addresses to Russian government offices and the Telegraph UK notes that this includes a link to president Putin's office (Blomfield, 2007). Further in article (chapter 3 and 4) we showed a number of practical cases for the individual variation of computer attack.

In the second half of 2010, no single topic dominated cyber security news more than WikiLeaks. A denial-of-service attack was also launched against the WikiLeaks site.

The paper discusses possible cyber capabilities of terrorists and sponsoring nations, describes how computer security vulnerabilities might be exploited through a cyber terror attack, and raises some potential issues. In the paper, we deal with DoS attacks, which are one of the major threats to Internet-dependent organizations. We can therefore assume that they are also the most commonly used internet tool of cyber terrorists.

Hypothesis. The most ambitious goal of this paper is to confirm the hypothesis that digitally higher developed countries are more exposed to internet terrorism (digital war) than countries with lower ICTD index.

Cyber terrorism

Cyber terrorism is typically defined as using the internet as a tool for launching an attack. Terrorists could conceivably hack into electrical grids and security systems or perhaps distribute a powerful computer virus (Janczewski & Colarik, 2007). Al-Qaeda operative terrorists are known to have training in hacking techniques, such as remote cyber attacks etc. Western governments have accused state and nonstate the actors of enabling the infiltration into state security networks, including an alleged breach of a Pentagon system, by Chinese hackers in 2007.

The established definition of cyber terrorism needs to be broadened (Kohlmann, 2006). He argues that any application of terrorism on the Internet should be considered as cyber terrorism. There's no distinction between the »online« terrorist community and the »real« terrorist community. As evidence, recounts one extreme instance in which the Iraqi insurgent group Army of the Victorious Sect held a contest to help design the group's new website. According to Kohlmann (2006), the prize for the winning designer was the opportunity to, with the click of a mouse, remotely fire three rockets at a U.S. military base in Iraq.

Terrorist websites

Defining a terrorist website is as contentious as defining terrorism. Pentagon analysts testifying before Congress have said that they monitor some five thousand jihads websites, though they closely watch a small number of those - less than one hundred – that are deemed the most hostile.

Terrorist sites include the official sites of designated terrorist organizations, as well as the sites of supporters, sympathizers, and fans (Weimann, 2006). But when websites with no formal terrorist affiliation contain sympathetic sentiments to the political aims of a terrorist group, the definition becomes murky. Hoax sites can also prove a troublesome red herring for monitors of terrorist sites. For instance, in recent years a number of sites sympathetic to the Taliban have proliferated on the web. Frequent site outages, however, make it difficult to track their content and sentiment.

Terrorist organizations use of the internet. Weimann (2006) argues that the number of terrorist sites has increased exponentially over the last decade - from less than 100 to more than 4,800 from year 2005 to year 2006. The numbers can be somewhat misleading, however. In the case of Al-Qaeda, hundreds of sister web sites have been promulgated but only a few of them are considered active. Nonetheless, analysts forecast a trend of proliferation of web sites for terrorist activity.

Chat rooms, propaganda and recruitment. The Internet is a powerful tool for terrorists, who use online message boards and chat rooms to share information, coordinate attacks, spread propaganda, raise funds, and recruit new followers, all of which are non-technical approaches of using the Internet for terrorist activity (Thomas, 2003). Terrorist sites also host messages and propaganda videos which help to raise morale and further the expansion of recruitment and fundraising networks. Today Al-Qaeda's media arm and foundation for Islamic media publication (As-Sahab) are among the most visible. However, an entire network of jihadist media outfits has sprung up in recent years, according to a study of Radio Free Europe/Radio Liberty, conducted by Kimmage (2008). The highest leadership and members of Al-Qaeda, led by Osama bin Laden, count for a mere fraction of jihadist media production. A widespread network of media-related institutions that deliberately operate in support of extremist terrorist groups was established.

Tutorials. Terrorist websites can serve as virtual training grounds, offering tutorials on building bombs, firing surface-to-air missiles, shooting at U.S. soldiers, and sneaking into Iraq from abroad. For several years, terrorist groups including al-Qaeda have used cyberspace for communication, recruiting and propaganda but today there are also other procedures and techniques of using the internet, such as credit card theft or money laundering for terrorist activity, hacking, steganography, data mining, etc (Kushner, 2003).

Methods of internet terrorism

The greatest advantage of internet terrorism is undercover activity. There are many ways of internet terrorism, while cyber fraud, ranging from credit card theft to money laundering, belongs to one of the latest and most modern ways of terrorist operations on the Internet. The next chapter describes some practical technical methods of internet terrorism and supports them with well-known events.

Hacking. "Hacking, Why Not?" were the instructions of Muslim radicals when they hacked into Indonesian Web sites and chat rooms for online credit card fraud and money laundering. Samudra, responsible for the bombing in Bali in October 2002 (Indonesia), in which 202 people were killed, writes about the funding of terrorism through cyber fraud. Evidence collected from Samudra's laptop showed he tried to finance the bombing through cyber fraud. Terrorist organizations have graduated to the Internet to steal, because it reaches more potential victims and is harder to trace (Kohlmann, 2006).

Internet use by cyber terrorists mirrors that of criminals. While some security experts fear a cyber strike could disrupt power supplies to millions of

homes, disrupt air traffic control systems and shut down water supplies, most agree that terror groups are more likely to exploit the Internet for financial gain and to spread propaganda.

Previously, militants used more conventional ways for funding. The Roubaix gang in France robbed armored cars to help fund terrorist activities in 1990, while the group behind the abortive millennium attack on the Los Angeles airport robbed supermarkets in Canada and engaged in traditional credit card fraud. According to Weimann (2006) it is a paradox that those movements, which criticize Western technology and modernity, are using the most advanced communication Internet technology to spread their message and terrorism activity. However, the U.S. government should not dismiss the possibility of a large-scale electronic attack by terrorists against the nation's computer systems (Clarke & Knake, 2010).

Denial-of-Service Attacks. The increasingly known scenario is this: potential attackers with the Internet looking for vulnerable Web sites. Just as businesses sectors, public sectors are also not DoS immune, in fact, they may be the most vulnerable to a attack. These sites are often the least prepared to defend themselves against such an attack, lacking the resources to devote to sophisticated security measures (Computer Crime Research Center, 2004).

Attacker normally use User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Internet Message Protocol (ICMP), (synchronize) SYN, etc. protocols scanning. UDP and TCP protocol to passing through every door in computer, ICMP echo protocol sending only part of the TCP SYN packets are very suitable for Server DoS. DoS attack works by overwhelming a target with SYN requests and not completing the initial request, which thus prevents other valid requests from being processed. In many cases, SYN requests with forged IP (Internet Protocol) addresses are sent to a target, allowing a single attacking computer to initiate multiple connections, resulting in unsolicited traffic, known as backscatter, being sent to other computers on the Internet. This backscatter is used to derive the number of DoS attacks observed throughout the reporting period. Although the values Symantec derives from this metric will not identify all DoS attacks carried out, it will highlight DoS attack trends. However, in this case, attackers who were considered were those carrying out a set of DoS attacks that were detected by IDS and IPS software.

A possible DoS attack can be carried out as follows: When the attacker finds vulnerability, he/she will provide a mini attack just to send a message to the target (company or government) to let them know that he/she is serious and has what it takes to overwhelm the server. After this procedure, the attacker will send an email taking responsibility for the attack and asking for cash payments to stop a larger, full-scale DoS attack being launched from a distributed network of thousands of unwitting computers. The results of an attack include a downed Web site, the inability to take and process orders from customers (potentially fatal for e-commerce sites), damaged customer relationships, injured brand reputation or damaged critical infrastructure if the target is a country. Hoping to avoid such consequences, many individuals, companies or state departments will submit to the extortion and pay their attackers. The Russian Interior Ministry, which fights cybercrime, broke up the extortion ring after two of the victimized companies agreed to pay the gangs U.S. $40,000 each (The Australian, 2004)

DoS attacks have become a dark fact of life. But while this may seem a daunting trend, companies and hosts are not powerless against it, as many security related products are available today, including firewalls, automated systems patching, vulnerability notification services, Internet threat assessment and notification systems, intrusion prevention and anti-spyware software. There are some basic procedures for every company or government to limit the possibility of attack and diminish the effectiveness of an attack, if exist.

Hidden Network/IP address. Terrorists use the internet as a pervasive, inexpensive and anonymous means of communication through which they can plan and orchestrate other fund raising activities. Terrorists also use online banking and other financial services and internet based alternatives to the banking system such as internet payment services and e-cash (Bedi, 2005).

The anonymity of the internet (TOR, JAP etc.) is enhanced by the fact that many servers do not use »log files« to trace the origin of the computer through which the transaction is made. TOR is a network of virtual tunnels that works on the real world internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable compromise between privacy (anonymity and security), usability, and efficiency (Dingledine, Mathewson in Syverson, 2004). Java Anonymous Proxy known as JAP is also a proxy system designed to allow browsing the web anonymously. Thus, the IP (internet protocol) number of the server and the date and time of connection are not kept in an electronic file. The roots of the transmissions are effectively kept private and virtually untraceable.

Terrorist web-sites can be made anonymous by using anonymizers which replace the IP address for the user’s home computer with another IP address that cannot be traced back to the user because anonymizers generally do not maintain logs. An anonymizer can also provide the ability to simply browse the web or send emails without the website host or the email ISP knowing the source of a web page request or email message.

A common method to communicate safely for the

terrorist is to save a draft of a message on a free e-mail account (Hotmail, Gmail, Yahoo etc.) which is read by terrorist in other parts of the world. Because the draft was never sent by e-mail, the ISP (Internet Service Provider) does not retain a copy of it and there is no record of its traversing the internet. We write a message, but instead of sending it, we put it in the »draft file« and then log off. Someone else can then log in to the same account using the same username and password, read the draft and then delete it.

Another common method involves providing basic electronic mail services in conjunction with a terrorist-sympathizer web site. Imagine a secure web site that supports basic e-mail services. An e-mail can be sent from one of its e-mail accounts to another without ever leaving its servers. To further add to the burden of law enforcement, by the use of something called Unicode, messages can be written in Cyrillic, Hindi, Japanese, Chinese, Korean, Arabic, Hebrew or in just about any other alphabet (Bedi, 2005).

Terrorists may also use encryption and steganography to hide the content of electronic communications regarding raising and moving funds. A website can also be used for interaction in encoded content or hidden messages. Because the actual server that houses a website can be located anywhere, the ability of law enforcement to track illegal activity is very complicated.

Encryption tools. Terrorists have developed sophisticated encryption tools and creative techniques that make the Internet an efficient and relatively secure means of correspondence (Lyon, 2008). These include steganography, a technique used to hide messages in graphic files, and »dead dropping«: transmitting information through saved email drafts in an online email account accessible to anyone with the password. The files cannot be distinguished without a decoding tool. The Internet also provides a global pool of potential recruits and donors. Online terrorist fundraising has become so commonplace that some organizations are able to accept donations via the popular online payment service PayPal.

Yet some terrorism experts argue that while the Internet has proven effective at spreading ideology, it is used as an optimized planning terrorism activity operational tool with high efficiency. Internet will be important for future terrorism activity.

Credit card numbers stolen over the Internet. Internet is the very efficient tool for terrorists to finance operations. Online scams are harder to trace because they are relayed through a sophisticated network of individuals and Web sites worldwide. And many schemes originate from abroad, where cyber laws don't exist or law enforcement is lax.

In dozens of incidents over the past few months, groups linked to terrorism have stolen credit card numbers over the Internet, laundered money and hijacked Web sites (Swartz, 2005).

The recent surge in activity has given counterterrorism specialists, already concerned with threats to physical structures, another worry. Like other security organizations; FBI, Secret Service, the Treasury Department and others must use Internet technology to fight the terrorists and are now branched into many areas.

Credit card numbers are often swiped through hacking attacks and phishing, fraudulent e-mails that trick consumers into surrendering personal information. In 2005, a suspected Palestinian supporter of Middle Eastern terrorist groups posted several credit card numbers online and instructions for stealing databases of other active credit card numbers from the Web sites of U.S. businesses (Swartz, 2005).

Wi-Fi Hack. Wi-fi hacking has featured prominently in some big cyber crimes, including the attack on TJ Maxx that exposed at least 45 million customer credit card numbers and other data. In that case, Gonzalez »Segvec« and associates allegedly cracked the weak WEP key and used it to gain entry to the corporate network, where he planted packet sniffers to scoop up the data. But this proves that the FBI is using the same tactics. By using one of the better encryption options (WPA2), one would presumably be immune to this kind of cyber terrorism (Poulsen, 2009).

Online terrorism propaganda. Perhaps the most effective way in which terrorists use the Internet is the spreading of propaganda. Abu Musab al-Zarqawi's al-Qaeda cell in Iraq has proven particularly adept in its use of the web, garnering attention by posting footage of roadside bombings, the decapitation of American hostage, and kidnapped Egyptian and Algerian diplomats prior to their execution.

In Iraq, experts say terrorist propaganda videos are viewed by a large portion of society, not just those who sympathize with terrorists and insurgents. In addition to being posted online, the videos are said to be sold in Baghdad's video shops, hidden behind the counter along with pornography. Terrorists use of the Internet, points out that propaganda films are not exclusively made in the Middle East. Groups from Bosnia, Afghanistan, and Chechnya also produce propaganda videos. However, videos are not the only form of propaganda. Some jihads websites have even offered video games in which users as young as seven can pretend to be holy warriors killing U.S. soldiers.

How to respond to Internet terrorist activities?

There is some debate within the counterterrorism community about how to combat terrorist sites. Inappropriate reaction is if you see a terrorist site and you decide to shut it down, says Kohlmann (2006). This reaction can cause that investigators might miss out on a

wealth of valuable information. For instance, German officials monitoring online terrorism issued early warnings prior to the Madrid train bombings in March 2004.

Shutting down a terrorist website is just a temporary disruption. To truly stop a terrorist site, experts say, the webmaster must be stopped. The ability of the U.S. National Security Agency to monitor such individuals inside the United States has been subject of a heated political and legal debate. The United States have tried to prosecute webmasters who run terrorist websites in the West, but ran into opposition from advocates of free speech. Sites that tell the terrorist side of the story go right up to the brink of civil liberties. Al-Hussayen, a Saudi Arabian graduate student at the University of Idaho, was charged by U.S. officials for supporting terrorism because he served as a webmaster for several Islamic groups whose sites linked to organizations praising terrorist attacks in Chechnya and Israel. Al-Hussayen was acquitted of all terrorism charges by a federal court in June 2004 under the First Amendment.

Another approach officials have taken is to create phony terrorist websites. These can spread disinformation, such as instructions for building a bomb that will explode prematurely and kill its maker or false intelligence about the location of U.S. forces in Iraq, intended to lead terrorist fighters into a trap. This tactic must be used sparingly, or else officials risk »poisoning a golden pot of information« about how terrorists operate (Kaplan, 2009).

There are indications terrorists may next steal trade secrets from U.S. federal states as their computer skills improve and they begin to work with organized crime in Europe. The stolen documents could then be sold to rogue foreign businesses or held for ransom.

After September 11, the emphasis has clearly been on physical infrastructure rather than cyber security what is understandable. But we have to understand that cyberspace is also a tool for providing terrorist activity.

Realizing that fixed Internet sites had become too vulnerable, al-Qaeda and its affiliates turned to rapidly proliferating jihadist bulletin boards and Internet sites that offered free upload services where files could be stored. The outside attacks on sites like Alneda.com forced the evolution of how jihadists are using the Internet to a more anonymous, more protected, more nomadic presence. The groups gave up on set sites and posted messages on discussion boards. One of the best-known forums that emerged after September 11 was Qalah or Fortress. Registered to an address in Abu Dhabi, the United Arab Emirates, the site has been hosted in the U.S. by a Houston Internet provider, Everyone's Internet, which has also hosted a number of sites preaching radical Islam. Researchers who follow the site believe it may be connected to Saad Faqih, a leading Saudi dissident living in exile in Britain.

Comparative analysis of literature rewiev results

The comparative literature review analysis is produced to examine and explain regional computer security dynamics, depends of digital development of countries fall into three broad categories: first, accounts of regional DoS attacks second is research of worldwide digital development index and third largely empirical surveys of how regional digital development arrangements influented with DoS computer attack issues.

In first part with summary we will recap the most important information of the our source (Symantec Corporation & International Telecommunication Union). With a synthesis in second part we re-organization, that information of DoS attacks related to digital development of countries to confirm or reject our hypotesis that digitally higher developed countries are more exposed to internet terrorism (digital war) than countries with lower ICTD index. The focus of this our literature review is to summarize and synthesize the arguments and ideas of selected research to adding new scientific contributions in cyber terrorism field.

With 2 comparative studies we fulfilled inclusion criteria, with a total of 10 countries in the world of EMEA regions and 10 countries in the world of APJ regions related of the highest DoS attacks index. The third comparative study gives us digital development index of this selected countries of both regions.

Attack trends in this report are based on the analysis of data retrieved from the Symantec Global Intelligence Network (SGIN). This global network database includes the Symantec DeepSight Threat Management System, Symantec Managed Security Services, and the Symantec Honeypot Network. We combine data retrieved from these sources for analysis.

Results of DoS and ICTD index. Information about for these countries was retrieved from research on the digital development of countries and the research on current global percentage DoS attacks on countries in year 2007. Table 1 shows calculated Information Communication Development Index (ICTD) index (ITU, 2010) and (common) DoS index of top ten of Asia, Pacific, Japan (APJ) regions (Symantec Corporation, 2009a) and Europe, Middle East, Africa (AMEA) regions (Symantec Corporation, 2009b).

Top countries of attack origin Symantec was identifies with the national sources of attacks by automatically IP addresses cross-referencing source of every IP attacking with several third-party, subscription-based databases that link the geographic location of systems to source IP addresses. While these databases are generally reliable, there is a small possibility of error margin. Sectors targeted by DoS attacks were identified using the same methodology as targeted countries.

Table 1 shows the DoS index and the ICTD index trend and their correlation. Hierarchical diagrams sum-

marizing the relationships between both indexes. It is clearly seen that (if we approximate results with exponential distribution) the DoS index is decreasing while the ICTD index is also decreasing. With other words this could mean that digitally higher developed countries are more exposed to internet terrorism. A more detailed explanation is shown on a different picture, where it is clear that even countries with low ICTD index show a relatively high DoS index. These conclusions contradict the hypothesis that digitally higher developed countries are more exposed to internet terrorism (digital war) than countries with lower ICTD index.

Table 1

Top ten countries
of current global percentage
DoS attacks (EMEA, APJ) and ICTD index

Global rank	Country	DOS (%)	ICTD
1	China	11	6,78
2	United Kingdom	6	6,70
3	South Korea	6	7,23
4	Germany	2	6,60
5	France	2	6,09
6	Australia	2	6,51
7	Netherlands	1	7,06
8	Italy	1	5,91
9	Russia	1	4,13
10	Spain	1	5,84
11	Sweden	1	7,27
12	Thailand	1	3,03
13	Japan	1	6,89
14	India	1	1,62
15	Ireland	<1	6,14
16	Belgium	<1	6,10
17	Singapore	<1	6,47
18	Malaysia	<1	3,66
18	Indonesia	<1	2,15

Source: Symantec Corporation (2009a, b) & ITU (2010)

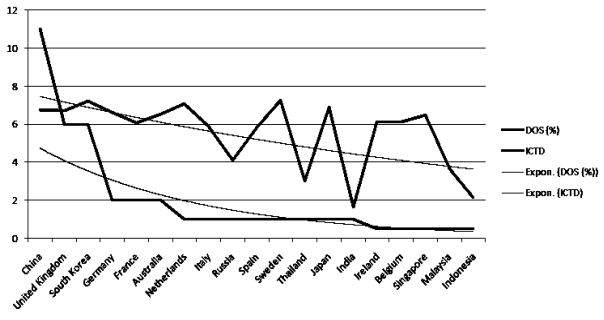

Fig. 1. Correlation graph of DOS and ICTD index

The position of Slovenia through the prism of global Internet terrorism. Slovenia was ranked fourth (Table 2) among the countries of attack origin targeting EMEA regional, with four percent of the total in end of year 2007 (Symantec Corporation, 2008). This is interesting for Slovenia because it was not ranked among the top 10 countries previously. This is much higher than Slovenia's one percent share of attacks globally (Symantec Corporation, 2008), and indicates that attacks are originating from Slovenia and are targeting the EMEA region specifically. These findings also confirm conclusions from chapter 7.1 that countries with a relatively low ICTD index are not any safer from internet terrorism than countries with higher ICTD index.

The model of combined DoS and ICTD index is useful when considering the varied ways that impacts accumulate. The table 2 above demonstrates some of the different sources and pathways of cumulative effects where Slovenia shift to fourth place related DoS attacks.

Table 2

Top ten countries of attack origin

Current Rank	Previous Rank	Country	Current Regional Percentage
1	1	United States	52 %
2	2	United Kingdom	11 %
3	3	China	5 %
4	36	Slovenia	4 %
5	5	Germany	4 %
6	8	Canada	3 %
7	6	Italy	3 %
8	4	Norway	2 %
9	7	France	2 %
10	9	Spain	1 %

Source: Symantec Corporation (2008)

Conclusion

We have to understand that some terrorist organizations, like criminals, could exploit the Internet to further their goals. With the growing economic dependency on information communication technology, civilian infrastructures are increasingly the primary targets of cyber-attacks. It is possible to compare the fight against terrorist funding to the war against money-laundering and drug trafficking. As Internet technologies become more advanced, so do those who use them for illicit and illegal activities. Security must remain a continuous process which is a never-ending dynamic cycle. Company-wide security procedures must be developed. A list of rules that includes shutting down computers every night, specific back-up procedures, a schedule of regular updates and patches, periodic password changes, rules about opening email attachments, guidelines on how to protect data while working in public places, and tips on how to ensure the physical security of laptop computers and actual office buildings must be created.

This article demonstrates the rapid entry of information conflicts into developed and less developed regions by highlighting DoS trends. Develop and maintain an organizational cyber security strategy that can help organizations safeguard their critical information. Flowing from this article's thesis, two primary strategies are

recommended to mitigate the cyber-warfare threat: an architectural strategy and a managerial strategy.

First, an architectural strategy should promote layers of security to increase the time and resources necessary for attackers to penetrate multiple barriers. This defence-in-depth approach is similar to an architectural fortress of high walls and armed guards behind a protective moat. Although each barrier alone does not ensure sufficient protection, taken together, a layering of firewalls, with antivirus software, combined with intrusion detection and prevention systems can greatly help to repel many of the types of attacks mentioned in this article.

Critical overview. This literature reviews provide us state information's of DoS attacks about world vide regions and give an particular topic overview or act as a stepping stone for further detail research. For professionals, these reviews are useful reports that keep them up to date with what is current in the cyber terrorism field. Comprehensive knowledge of the literature with these statistical informations of the field is essential for most cyber terrorism researchers.

Although there are numerous methods for carrying out DoS attacks, in this comparative study we derived metric by measuring DoS attacks that are carried out by flooding a target with SYN (synchronize) requests which are often referred to as SYN flood attacks.

There are different approaches to cyber war threat level assessment or defining an index which can successfully assess real circumstances in countries. One of these approaches is the CNO (Computer Network Operations) – the formula for calculating the CNO Index is = (X1+X2+X3+X4+X5+X6+X7+X8+X9+X10 +X11)/ 11 (UNDP, 2001).

War Index which is calculated from 11 single indexes. Each single index is previously calculated as following: index = (actual value - observed min value)/(obs. max value - obs. min value). The method is akin to the one presented in UNDP (2001). For a detailed study, it would be useful to use this comparative method.

Further work. The most important criterion which has to be implemented in each business or government for successfully fighting internet terrorism is the critical infrastructure assessment of information communication technology:

- measuring cyber security and vulnerability detection,
- training employees,
- relevant information assurance and risk management,
- active security testing and
- providing cyber insurance.

The first part of the managerial strategy is to hire certified security professionals as the commissioned officers of the cyber war. In second part of strategy employee training has been a recognized task for effective computer security since the proliferation of the computer. The third part of the managerial strategy is to mandate periodic risk assessments to identify the most serious cyber-threats. For an assessment to be successful and have a positive impact on the security posture of a system (and ultimately the entire organization), elements beyond the execution of testing and examination must support the technical process (NIST, 2008). After identifying threats, managers can allocate resources necessary to mitigate the most serious risks (Vacca, 2009). Considering societal reliance on IT, the growing cyber threat is highlighting the need for risk mitigation strategies such as cyber-insurance. Cyber-insurance policies often have higher premiums and deductibles because of the uncertainties in assessing cyber-risk (Kolodzinski, 2002).

Historically, information security concerns have not had a high priority with most managers. Many seemed willing to risk major losses by permitting their information systems to be either lightly protected or wholly unprotected (Straub, 1990). Yet, the growing reliance on IT has increased exposure to diverse sources of cyber war threats. Corporate leaders must be aware of the diversity of attacks, including high-tech espionage, organized crime, perception battles, and attacks from ordinary hackers, cyber terrorists or business competitors.

References

1. *Acharya, S. (2008). Cyber Terrorism-The Dark Side of the Web World. Retrieved February 3, 2011, from: http://www.articlesbase.com/law-articles/cyber-terrorism-the-dark-side-of-the-web-world-331261.html*
2. *Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica: Rand Corporation.*
3. *Bedi, R. (2005). Telecom-The Terrorism Risk. International Centre for Political Violence and Terrorism Research. Singapore: IDSS.*
4. *Blomfield, A. (2007). Russia accused over Estonian »Cyber-Terrorism«. Telegraph UK. Retrieved February 3, 2011, from: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/17/westonia117.xml*
5. *Campen, A. D. (1992). The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax: AFCEA International Press.*
6. *Clarke, R. A., & Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do about It. New York: Ecco, an imprint of HarperCollins Publishers.*
7. *Cohen, F. (2002). Terrorism and Cyberspace. Network Security, 5, 17-19.*
8. *Computer Crime Research Center (2004). Cyber Terrorism: The new kind of Terrorism. Retrieved October 21, 2010, from: http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/.*
9. *Denning, D. (2005). Information Operations and Terrorism. Innovative Terrorism in the Information Age: Understanding the Threat of Cyber-Warfare. Monterey: Naval Postgraduate School, Center of Terrorism and Irregular.*
10. *Department of Defense (1998). Joint Doctrine for*

Information Operations. Retrieved October 22, 2010, from: http://www.c4i.org/jp3_13.pdf.

11. Dingledine, R., Mathewson, N. in Syverson, P. (2004). Tor: The Second-Generation Onion Router. Retrieved February 3, 2011, from: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

12. Furnell, S., & Warren, M. (1999). Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium? Computers and Security, 18(1), 28-34.

13. Giacomello, G. (2003). Measuring »Digital Wars«: Learning from the experience of peace research and arms control. Retrieved February 3, 2011, from: http://www.iwar.org.uk/infocon/measuring-io.pdf.

14. Hayward, D. (1997). Net-Based Terrorism a Myth. TechWeb, November 19.

15. ITU International Telecomunication Union (2010). Measuring the Information Society 2010. Retrieved October 18, 2010, from: http://www.itu.int/ITU-D/ict/publications/idi/2010/index.html

16. Janczewski, L. J., & Colarik, A. M. (2007). Cyber Warfare and Cyber Terrorism. Hershey, New York: Information Science Reference.

17. Kaplan, E. (2009). Terrorists and the Internet. Retrieved October 18, 2010, from http://www.cfr.org/publication/10005/terrorists_and_the_internet.html

18. Kimmage, D. (2008). The Al-Qaeda media nexus. Retrieved October 20, 2010, from http://docs.rferl.org/en-US/AQ_Media_Nexus.pdf

19. Kohlmann, E.F. (2006). The Real Online Terrorist Threat. Foreign Affairs, 85(5), 115-124.

20. Kolodzinski, O. (2002). Cyber-Insurance Issues: Managing Risk by Tying Network Security to Business Goals. CPA Journal, 72(11), 10-11.

21. Kushner, H. W. (2003). Encyclopedia of terrorism. London: Sage Publications.

22. Libicki, M. (1995). What Is Information Warfare. ACIS Paper 3. Washington, DC: National Defense University.

23. Lyon, G. (2008). Nmap Network Scanning. Sunnyvale: Insecure.com, LLC, USA.

24. NIST National Institute of Standards and Technology (2009). Technical Guide to Information Security Testing and Assessment. Retrieved February 6, 2011, from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

25. Poulsen, K. (2009). More FBI Hacking: Feds Crack Wi-Fi to Gather Evidence. Retrieved February 6, 2011, from http://www.wired.com/threatlevel/2009/04/more-fbi-hackin/

26. Swartz, J. (2005). Terrorists' use of Internet spreads. USA Today. Retrieved October 20, 2010, from http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm.

27. Symantec Corporation (2008). AMEA Internet Security Threat Report. Retrieved October 21, 2010, from http://www.symantec.com/business/theme.jsp?themeid=threatreport

28. Symantec Corporation (2009a). APJ Internet Security Threat Report. Retrieved October 21, 2010, from http://www.symantec.com/business/theme.jsp?themeid=threatreport

29. Symantec Corporation (2009b). AMEA Internet Security Threat Report. Retrieved October 21, 2010, from http://www.symantec.com/business/theme.jsp?themeid=threatreport

30. Straub, D.W. (1990). Effective IS security: An Empirical Study. Information Systems Research, 1(3), 255-276.

Thomas, T. (2003). Al Qaeda and the Internet: The Danger of Cyberplanning. Parameters, 112-123.

31. UNDP United Nations Development Program (2001). Human Development Report: Making New Technologies Work for Human Development. Oxford and New York: Oxford University Press.

32. Vacca, R. J. (2009). Computer and Information Security Handbook. USA, Morgan Kaufmann Publishers (Elsevier Science).

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

Поступила в редколлегию 26.03.2011

Рецензент: канд. техн. наук, доц. С.В. Кавун, Харьковский национальный экономический университет, Харьков.

ТЕРРОРИСТИЧЕСКИЕ КИБЕРАТАКИ И ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЙ ИНДЕКС РАЗВИТИЯ

Роберт Брамник

Терроризм и интернет связаны в двух основных направлениях. Во-первых, Интернет стал форумом для террористических групп и отдельных террористов для распространения своих сообщений ненависти и насилия, а также для общения с другими их сторонниками. Во-вторых, отдельные лица и группы пытаются атаковать компьютерные сети, в том числе в Интернете, что стало называться кибер-терроризмом и кибер-войнами. Цифровой индекс развития является показателем, который измеряет уровень информационно-коммуникационных технологий (ИКТ), принятый в стране. Цель этой статьи заключается в нахождении корреляционных функций атаки типа отказ в обслуживании (DoS), который является самым известным кибертеррористическим методом, и индекса цифрового развития страны и предоставление информации об их взаимоотношениях.

Ключевые слова: *психологическая война, кибертерроризм, кибервойна.*

ТЕРОРИСТИЧНІ КІБЕРАТАКИ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИЙ ІНДЕКС РОЗВИТКУ

Роберт Брамник

Тероризм та інтернет пов'язані в двох основних напрямках. По-перше, Інтернет став форумом для терористичних груп та окремих терористів для поширення своїх повідомлень ненависті і насильства, а також для спілкування з іншими їхніми прихильниками. По-друге, окремі особи і групи намагаються атакувати комп'ютерні мережі, в тому числі в Інтернеті, що стало називатися кібер-тероризмом і кібер-війнами. Цифровий індекс розвитку є показником, який вимірює рівень інформаційно-комунікаційних технологій (ІКТ), прийнятий у країні. Мета цієї статті полягає в знаходженні кореляційних функцій атаки типу відмова в обслуговуванні (DoS), який є найвідомішим кібер-терористичним методом, та індексу цифрового розвитку країни та надання інформації про їх взаєминах.

Ключові слова: *психологічна війна, кібертероризм, кібервійна.*