Computer Technology and Application 6 (2015) 45-56
doi: 10.17265/1934-7332/2015.01.007

Information Technology in Domain of Electronic Intelligence and Cyberterrorism Combat

Robert Brumnik[1] and Sergii Kavun[2]

1. Metra Engineering Ltd., Ljubljana 1000, Slovenia

2. The Department of Information Technologies, Kharkiv Institute of Banking of the University of Banking of the National Bank of Ukraine, Kharkiv 61174, Ukraine

Abstract: Terms of intelligence in 20th and 21th century mean the methods of automatic extraction, analysis, interpretation and use of information. Thus, the intelligence services in the future created an electronic database in which to their being classified intelligence products, users could choose between the latter themselves relevant information. The EU (European Union) that activities are carried out from at least in year 1996, terrorist attacks in year 2001 is only accelerating. Proposals to increase surveillance and international cooperation in this field have been drawn up before September 11 2011. On the Web you can find a list of networks (Cryptome, 2011), which could be connected, or are under the control of the security service—NSA (National Security Agency). United States of America in year 1994 enacted a law for telephone communication—Digital Telephony Act, which would require manufacturers of telecommunications equipment, leaving some security holes for control. In addition, we monitor the Internet and large corporations. The example of the United States of America in this action reveals the organization for electronic freedoms against a telecom company that the NSA illegally gains access to data on information technology users and Internet telephony.

Key words: Intelligence and counterintelligence activities, electronic spy devices, detection methods, netwar, counterterrorism.

1. Introduction

1.1 Main Definitions in Research Field

First of all, anytime we use the prefix cyber, when we talking about something moving fast our motion always involved. Then, there is the whole problem of jurisdiction. Where exactly does cyberspace begin and end? The Internet, like space, does not have any borders.

Also known are Chinese dissidents, which were identified and arrested on the basis of data provided by the Chinese authorities to obtain from corporation Yahoo. Even Google has a history of bowing to pressure from China's censorship purpose of obtaining intelligence. Recently, however Facebook is the most frightening spy device that humanity has ever done. It consolidates information about people, their relationships, names, addresses, location, communication, relatives and all the available American intelligence [1].

It is understood that the success of preventive counter-terrorism, surveillance authorities want as much control. Recently, however, these skills can be used to gain competitive advantage of countries and the increase in economic espionage. Until these trends should take by a public policy, and a distance becomes too oversized "appetites" of the supervisor's limits. The problem is the surveillance technology can also turn against the state. A controlling existing technology, which was created for the purposes of legal supervision, can be abused from a side of the criminal or terrorist organizations. Typical examples had been listened as the affair in Greece and Italy. In Greece, the attacker, probably the Secret Service, but also could be a criminal group, managed to exploit security vulnerability in module PBX (Private, Branch, Exchange) designed to lawful interception.

Corresponding author: Robert Brumnik, Ph.D., assistant professor, research field: information and cyber security. E-mail: robert.brumnik@metra.com.

A great deal of "cracks" are committed for the purposes of anarchy, humor, or as often stated by the perpetrators, "to be annoying". However, is this the mindset of a cyber terrorist? Does he change a website to say a country's government is evil? Does he hack into a major corporation's voice mail system to make long distance calls? No, that is not domain of the cyber terrorist. That is domain of the amateur cracker demonstration. A cyber terrorist will disrupt the banks, the international financial transactions and the stock exchanges. The key: the people of a country will lose all confidence in the economic system. Would a cyber terrorist attempt to gain entry to the government building or equivalent? Likely, the arrest would be immediate. However, in the case of the cyber terrorism, when the perpetrator sitting on another continent while a national economic systems grind down, then destabilization will be achieved.

It is problematic defining a "cyber attack", such as "cyber crime" or "cyber terrorism", because of some difficulties for determining with certainty of identification, intent, or the attacker's political motivations. Often we equated simple use of malicious code with "cyber terrorism" which usually involves more factors like just a computer hack. However, a "cyber terrorism" event may also sometimes depend on the presence of other factors beyond just a "cyber-attack" [2].

There are many different definitions exist for the term "cyber terrorism" like as many definitions exist for the term "terrorism[1]". Security expert Denning (2007) defines cyber terrorism as "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" [3]. Some definitions of cyber terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives [4].

Other definitions indicate the physical attacks, which destroy computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard, also can be labeled as cyber terrorism [5]. Thus, it is possible that if a computer facility were deliberately attacked for political purposes, all the methods described above —physical attack, cyber attack etc. might contribute to, or be labeled as "cyber terrorism". Computer and information security, data protection, and privacy are all growing problems. No single technology or product will eliminate threats and risk. Securing our computers, information, and communications networks is securing our economy and our country.

To avoid such malicious possibility it is today's research and development task to produce the crime-resistant products of the future. Therefore, we must take every opportunity we can to use science and technology to reduce crime and improve the quality of our lives. In this module we focused on different aspects of "cyber terrorism", its basics and fundamentals methods of against fights.

1.2 Internet as a Forum of Terrorists Group

Groups with very different political goals but united in their readiness to employ terrorist tactics started using the network to distribute their propaganda, to communicate with their supporters, to foster public awareness of and sympathy for their causes, and even to execute operations. By its very nature, the Internet is in many ways an ideal arena for activity by terrorist organizations. Most notably, it offers as below:

- Easy access;
- Little or no regulation, censorship, or other forms of government control;

[1] Under 22 USC, Section 2656, "terrorism" is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The United States has employed this definition of terrorism for statistical and analytical purposes since 1983. U.S. Department of State, 2002, Patterns of Global Terrorism, 2003, http://www.state.gov/s/ct/rls/pgtrpt/ 2001/html/10220.htm

- Potentially huge audiences spread throughout the world;
- Anonymity of communication;
- Fast flow of information;
- Inexpensive development and maintenance of a Web presence;
- A multimedia environment (the ability to combine text, graphics, audio, and video and to allow users to download films, songs, books, posters, and so forth); and the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories.

Islamic militant organizations also use the Internet to disseminate their anti-Western, anti-Israel propaganda. Several Internet sites created by Hamas supporters, for example, carry the organization's charter and its political and military releases, some of which openly call for and extol the murder of Jews. Others, like Hizb ut-Tahrir, a radical Islamic organization based in Britain, uses its Web site to provide details to the public about its regular meetings around the United Kingdom. Still others use the Internet to raise funds; Hezbollah, for example, the pro-Iranian Shiite terrorist organization based in south Lebanon, sells books and publications through its Web site. Some terrorists from Hamas and Islamic Jihad use the Internet to provide specific instructions to fellow terrorists including maps, photographs, directions, codes and technical details of how to use explosives. Some of terrorists groups use encrypted E-mail to plan acts of terrorism; most groups appear to use the Internet to spread their propaganda [6].

1.3 Netwar Overview

Where is internet terrorism today? Where it is headed? Espionage? Botnets? Trojans? Spy ware? Denial of service attacks? Phishing scams? Zero-day exploits[2]? Or the new terrorist member recruitment? The reality is that no one can be immune from this malicious industry's reach not mention the individuals, businesses, even governments. Many sophisticated computer technologies are developing in new era [7]. In addition, there are growing dangers from crimes committed against information on computers, or against computers. In most countries around the world, however, existing laws are likely unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforcing as Internet terrorism increasingly breaches national borders. National governments should examine their current statutes to determine whether they are sufficient to combat the kinds of crimes discussed in this article. Where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes. Many reports describe about possible effects of a coordinated Net war against the most critical infrastructure. In addition, there are many discussions about open options to extremists, or terrorist groups for obtaining malicious technical services from cyber criminals to meet political or military objectives.

2. What Is New in Net War?

Undeterred by the prospect of arrest or prosecution, cyber terrorist around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nation's security. Headlines of Net war attacks command our attention with increasing frequency. Moreover, countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities the potential for copycat crimes and the loss of public confidence. Sophisticated tools for

[2] Zero-day exploits: computer code that exploits a vulnerability for which a patch is not yet available.

cyber-attack we can found for sale or freeware on the web [8]. Highly-organized underground cybercrime businesses host websites advertise a variety of disruptive software products and malicious technical services.

High-end cybercrime groups use standard software business development techniques to keep their products updated with the latest anti security features. In addition, they seek and recruit new and talented software engineering students into their organizations. As in next chapter, shows the laws of most countries do not clearly prohibit cybercrime.

3. Problems Combat Cyber Terrorism

3.1 Problem to Cybercrime Definition Harmonize

Cybercrime can be very broad in scope and may sometimes involve more factors than just a computer hack. Cyber terrorism is often equating with using of malicious code. However, a cyber-terrorism event may also sometimes depend on the presence of other factors beyond just a cyber-attack.

3.2 Problem of Transitional Nature of Cyber Crime

Effective law providing is complicate cause of transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cybercrime. However, the future of the networked world demands a more proactive approach, whereby governments, industry, and the public work together to devise effective laws that will effectively determine cyber criminals. “Fighting cybercrime is a 24/7 battle, a global battle, and it is far from over” [9].

It is easy to learn how to commit; they require few resources relative to the potential damage caused they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

3.3 Problem to International Law Harmonize

Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national. New technologies continue to outpace policy for law enforcement. Problems of coordination among agencies of different countries, along with conflicting national policies about crime in cyberspace, work to the advantage of cyber criminals who can choose to operate from geographic locations where penalties for some forms of cybercrime may not yet exist. That boundaries or designing attacks appear to be originating from foreign sources. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their “virtual” counterparts. Outdated laws may not cover web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks as protected forms of property.

4. Some Theory, Examples and Known Practices

4.1 Common Description of a Problem

The Internet is the ideal medium for terrorism today, anonymous and pervasive. Information technology and particularly the Internet has become a key tool of terrorist groups as well as a potential target. Terrorists use it to spread their ideology, to recruit, train and motivate their followers, to plan their attacks and communicate with each other across borders. However, al Qaeda’s move into cyberspace is far from total. In the mountains near Jalalabad in November 2001, as the Taliban collapsed and al Qaeda lost its Afghan sanctuary, Osama bin Laden biographer Hamid Mir watched every second al Qaeda member carrying a laptop computer along with a Kalashnikov as they prepared to scatter into hiding and exile. On the screens were photographs of Sept. 11 hijacker Mohamed Atta.

Physical sanctuaries or unmolested spaces in Sunni Muslim-dominated areas of Iraq, in ungoverned tribal territories of Pakistan, in the southern Philippines, Africa and Europe still play important roles. Most violent al Qaeda-related attacks even in the most recent period of heavy jihadist Web use appear to involve leaders or volunteers with some traditional training camp or radical mosque backgrounds.

Contributors to the Islamic forums also have worried publicly that some kind of Western cyber-attack targeted the Web sites. One prominent jihadi poster, quoted by SITE, suggested extremists should strike back by infiltrating other, more-moderate Islamic discussion forums and flood them with extremist rhetoric to turn them into Al Qaeda discussion groups.

Al Qaeda and its offshoots are building a massive and dynamic online library of training materials supported by experts who answer questions on message boards or in chat rooms covering such varied subjects as how to mix ricin poison, how to make a bomb from commercial chemicals, how to pose as a fisherman and sneak through Syria into Iraq, how to shoot at a U.S. soldier, and how to navigate by the stars while running through a night-shrouded desert. These materials are cascading across the Web in Arabic, Urdu, Pashto and other first languages of jihadist volunteers.

The Saudi Arabian branch of al Qaeda launched an online magazine in 2004 that exhorted potential recruits to use the Internet: Oh Mujahid brother, in order to join the great training camps you do not have to travel to other lands, declared the inaugural issue of Muaskar al-Battar, or Camp of the Sword. Alone, in your home or with a group of your brothers, you too can begin to execute the training program.

Al Qaeda's innovation on the Web erodes the ability of our security services to hit them when they are most vulnerable when they are moving, said Michael Scheuer, former chief of the CIA unit that tracked bin Laden. It used to be they had to go to Sudan, they had to go to Yemen, they had to go to Afghanistan to train, he added. Now, even when such travel is necessary, an al Qaeda operative "no longer has to carry anything that's incriminating. He does not need his schematics, he does not need his blueprints, and he does not need formulas". Everything is posted on the Web to send ahead by encrypted Internet, and it gets lost in the billions of messages that are out there [10].

The number of active jihadist-related Web sites has metastasized since Sept. 11, 2001. When Gabriel Weimann, a professor at the University of Haifa in Israel, began tracking terrorist-related Web sites eight years ago, he found 12; today, he tracks more than 4,500. Hundreds of them celebrate al Qaeda or its ideas, he said.

They are all linked indirectly through association of belief, belonging to some community. The Internet is the network that connects them all. You can see the virtual community come alive. Apart from its ideology and clandestine nature, the jihadist cyber world is little different in structure from digital communities of role-playing gamers, eBay coin collectors or disease sufferers. Through continuous online contact, such communities bind dispersed individuals with intense beliefs who might never have met one another in the past. Along with radical jihad, the Internet also has enabled the flow of powerful ideas and inspiration in many other directions, such as encouraging democratic movements and creating vast new commercial markets.

Western analysts have identified the webmaster and chief propagandist of the site as Yusuf Ayiri, a Saudi cleric and onetime al Qaeda instructor in Afghanistan. In the summer of 2002, U.S. authorities and volunteer campaigners who were trying to shut him down chased him across multiple computer servers. At one point, a pornographer gained control of the Alneda.com domain name, and the site shifted to servers in Malaysia, then Texas, then Michigan. Ayiri died in a gun battle with Saudi security forces in

May 2003. His site ultimately disappeared (see Fig. 1).

Abdullah Muhammad also contributes to Jihad Recollections, an English language online publication put out by Al-Fursan Media, an apparent collaboration of online terrorist sympathizers. In the inaugural issue, released in April 2009 and purporting to be the first English Jihad magazine, Abdullah Muhammad expresses support for Al Qaeda, writing that the September 11 terrorist attacks were, for the most part, positive and the results even better than expected. He also calls on like-minded Muslims to exploit these results and advance the jihad.

4.2 Al Qaeda Social Network

We know that terrorists make phone calls. After the 2001 attacks, the government determined that the 19 terrorists had made 206 international calls from the United States, according to press reports. Valdis Krebs, founder of social networking analysis company OrgNet.com, conducted his own analysis of the 9/11 terrorists by collecting information from press reports such as who called whom, the addresses shared by the terrorists and their known associates, and information that they used the same frequent flier number. Krebs found that more links led to the group's leader, Mohammad Atta, than to any other terrorist.

A logical step for data analysts would be to search through phone records to see if there are other networks of people whose calls followed similar patterns.

4.3 9/11 Terrorists Data Mining—Tracking Two Identified Terrorists

SNA (Social Network Analysis) is a mathematical method for connecting the dots. SNA allows us to map and measure complex, and sometimes covert, human groups and organizations [11].

Early in 2000, the CIA (Central Intelligence Agency) was informed of two terrorist suspects linked to Al Qaeda. Nawaf Alhazmi and Khalid Almihdhar were photographed attending a meeting of known terrorists in Malaysia (see Fig. 2). After the meeting, they returned to Los Angeles, where they had already set up residence in late 1999.

What do you do with these suspects? Arrest or deport them immediately? No, we need to use them to discover more of the Al Qaeda network. Once suspects have been discovered, we can use their daily activities to uncloak their network. Just like they used our technology against us, we can use their planning process against them. Watch them, and listen to their conversations to see:

- who they call/email;
- who visits with them locally and in other cities;
- where their money comes from.

The structure of their extended network begins to emerge as data is discovered via surveillance. A suspect being monitored may have many contacts both accidental and intentional. We must always be wary of guilt by association. Accidental contacts, like the mail delivery person, the grocery store clerk, and neighbor may not be viewed with investigative interest.

Intentional contacts are like the late afternoon visitor, whose car license plate is traced back to a rental company at the airport, where we discover he arrived from Toronto (got to notify the Canadians) and

First Issue of *Jihad Recollections*

Fig. 1 An example of site.

Fig. 2 Two known suspect in y. 2000.

his name matches a cell phone number (with a Buffalo, NY area code) that our suspect calls regularly. This intentional contact is added to our map and we start tracking his interactions where do they lead? As data comes in, a picture of the terrorist organization slowly comes into focus.

How do investigators know whether they are on to something big? Often they do not. Yet in this case, there was another strong clue that Alhazmi and Almihdhar were up to no good—the attack on the USS Cole in October of 2000. One of the chief suspects in the Cole bombing (Khallad) was also present (along with Alhazmi and Almihdhar) at the terrorist meeting in Malaysia in January 2000 [12].

Fig. 4 shows the two suspects and their immediate ties. All direct ties of these two hijackers are colored green, and link thickness indicates the strength of connection.

Once we have their direct links, the next step is to find their indirect ties—the connections of their connections. Discovering the nodes and links within two steps of the suspects usually starts to reveal much about their network. Key individuals in the local network begin to stand out. In viewing the network map in Figs. 3 and 4, most of us will focus on Mohammed Atta because we now know his history. The investigator uncloaking this network would not be aware of Atta's eventual importance. At this point, he is just another node to be investigated.

Fig. 4 shows the direct connections of the original suspects as green links, and their indirect connections as grey links. We now have enough data for two key conclusions:

- All 19 hijackers were within 2 steps of the two original suspects uncovered in 2000;
- Social network metrics reveal Mohammed Atta emerging as the local leader.

All data mining systems fail in two different ways: positives false and negatives false. A false positive exist, when the system identifies a terrorist plot which is not a really one. A negative false will appear when

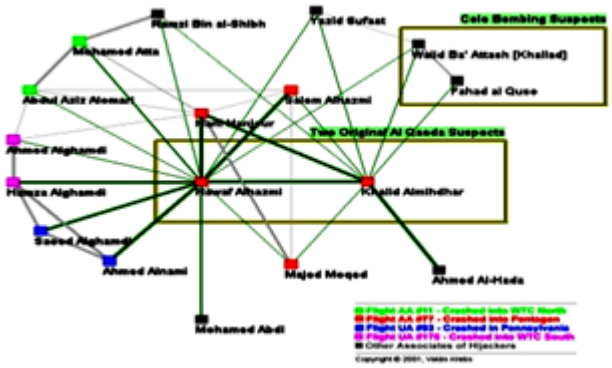

Fig. 3 All nodes within 1 steep (direct link) of original suspects.

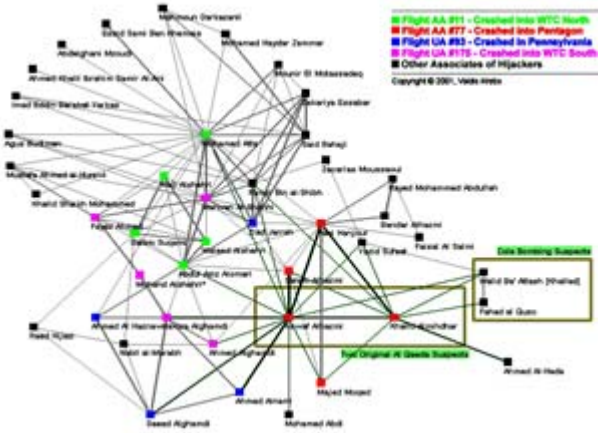

Fig. 4 All nodes within 2 steep (direct link) of original suspects.

the data mining system misses an actual terrorist plot. Depending on how you regulate your detection algorithms, you can fail on one side or the other: you can increase the number of positives false to ensure that you are less likely to miss an actual terrorist plot, or you can reduce the number of positives false at the expense of missing terrorist plots.

To reduce both those numbers, you need a well-defined profile. Moreover, that is a problem comes when we try to identify terrorism. In hindsight, it was really easy to connect the 9/11 dots and point to the warning signs, but it's much harder before the fact. Certainly, there are common warning signs that many terrorist plots share, but each is unique, as well. The better you can define what you are looking for, the better your results will be. Terrorist plots data mining is going to be sloppy, and it is going to be hard to find

anything useful.

With hindsight, we have now mapped enough of the 9/11 conspiracy to stop it. Again, the investigators are never sure they have uncovered enough information while they are in the process of uncloaking the covert organization. They also have to contend with superfluous data. This data was gathered after the event, so the investigators knew exactly what to look for. Before an event, it is not so easy.

5. Computer Networks Attack, Including the Internet

5.1 Tools for Password Cracking

Cain & Abel is one of the multi-purpose tools for decoding passwords of different coding algorithms in various operating systems in Fig. 5. Decoding passwords is not the only functionality. It is offer in use of other services, such as tapping network, search for wireless networks, and many others.

"John the Ripper" is a fast passwords cracking tool, which operates in the UNIX operating systems, Linux, Microsoft Windows, DOS (disk operating system), BeOS, and OpenVMS (virtual memory system) in Fig. 6. Its main purpose, as the authors argue, is in the detection of poorly selected UNIX passwords. In addition to breaking passwords it also supports cracking density value of the Kerberos AFS (Andrew file system) and Microsoft Windows NT/2000/XP/2003 LanManager. In addition to already implemented algorithms for breaking passwords, John the Ripper allows support for other coding algorithms, which are the form of a module included with the translation of source code.

5.2 The Attacks on the Password-Protected Systems

In roughly the attacks are separated into those where the attacker has local access to the target and those where attacker access to the target using a network—remote access. They are attacks where there is no direct contact between the attacker and the target. The attack is via the interface, which is in most cases what hacker own personal computer and/or telecommunication device. Access to the target is not given through the basic I/O interfaces (keyboard, mouse, screen), but through its interface for communication with other systems (modem, network interface, Bluetooth etc.). Access to the target is enabled through the selected communication path, wired or wireless. Today, most attacks occur on computer systems, which are coupled in the World Wide Web.

Brutus (see Fig. 7) is one of very interesting tools for the attack on the remote, password-protected systems, because of the greater protocols numbers, where authentication mechanisms can attack. Supported protocols are: HTTP (Hyper Text Transfer Protocol) (general authentication), HTTP (online), FTP (File Transfer Protocol), POP3 (Post Office Protocol Version 3), Telnet, NetBIOS (Network Basic

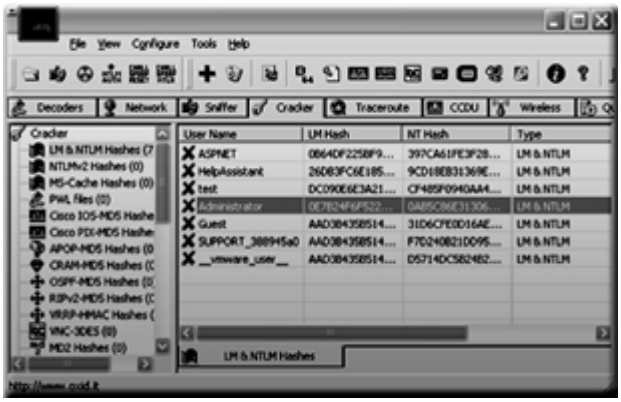

Fig. 5 Cain&Abel decoding password and algorithms tool.

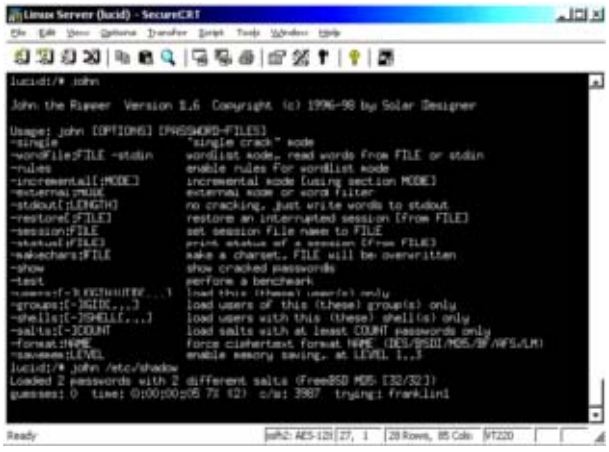

Fig. 6 John the Ripper password cracking tool.

Fig. 7 Brutus main interface.

Input/ Output System), and user-defined protocol. Brutus supports only attack with the use of verbal lists. It has the potential to establish a greater number (maximum 60) of simultaneous connections to the target, which dramatically increases the speed of the attack. On author's web site says that Brutus during the attack on the HTTP server operate at a speed of 501 attempts authentication to the second. This speed, of course, also depends on the speed of communication channels and the Web server.

5.3 Steganography: Hiding Data within Data

Steganography is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party. In this chapter, we will discuss what steganography is, what purposes it serves, and will provide an example using available software.

Imagine a scenario where persons A and B among themselves send e-mail, after they send hidden messages in digital photography. Even for the transfer of communication always used by the same image, this can become very suspicious. Someone who controls the transfer saw that the person B, has sent to person A the photo, which was received not long back straight from it. Why would you do? This is one of the samples, which suggest the suspicion and the need for a more detailed analysis of data transfers between persons A and B. Analysis would reveal that the size of files—digital photos, in any transfer actually changing. Steganography works to figure encode in the entire address space of media, not only for example. Thus, the binary comparison of two apparently identical files, in which we are in one encoded message cannot be easily, identified part of data, which are not part of the original file. Steganography is the most popular means of communication on the Internet between terrorists.

With computers and networks, there are many other ways of hiding information, such as:

- Covert channels (Loki[3] and some distributed denial-of-service tools use the Internet Control Message Protocol, or ICMP (Internet Control Message Protocol), as the communications channel between the "bad guy" and a compromised system);
- Hiding files in "plain sight" (what better place to "hide" a file than with an important sounding name in the c:\winnt\system32 directory?);
- Hidden text within Web pages;
- Null ciphers (using the first letter of each word to form a hidden message in an otherwise innocuous text).

The following formula provides a very generic description of the pieces of the steganography process: *cover_medium* + *hidden_data* + *stego_key* = *stego_medium*

The simplest approach to hiding data within an image file is called LSB (least significant bit) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB (*Red-Green-Blue*)

[3] Loki is a covert-channel client/server program. This program is a working proof-of-concept to demonstrate that data can be transmitted somewhat surreptitiously across a network by hiding it in traffic that normally does not contain payloads. url: http://www.phrack.com/issues.html?issue=51&id=6#article (04.27.2009).

encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed):

10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011

Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.

This description is meant only as a high-level overview. Similar methods can be applied to 8-bit color but the changes, as the reader might imagine, are more dramatic. Gray-scale images, too, are very useful for steganographic purposes.

Without going into any detail, it is worth mentioning steganalysis, the art of detecting and breaking steganography.

6. Conclusion

6.1 Netwar-war of the Future

There is only one thing we should add to conclusions: Islamic Al-Qaeda group displays peculiar interest to high tech weapon, including the Internet. Sheik Omar Bakri Mohammed's, founder of "Jama'at Al-Muhajiroun" group and Usama ben Laden's representative from international Islamic front "Jihad against Jew and crusaders". Technological means including the Internet are examined now in view of their application in large-scale war against West and Al Qaeda followers about planning new cyber-attacks.

In addition, cyber espionage involves the unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and copying of data files. However, should a terrorist group, nation, or other organization use computer hacking techniques for political or economic motives. Their deliberate intrusions may also qualify them, additionally as cyber terrorists. If there is disagreement about this, it is likely because technology has outpaced policy for labeling actions in cyberspace.

6.2 How to Avoid Unexpected Scenarios?

Satan[4]**:** SATAN (security administrator tool for analyzing networks) is an automated network vulnerability search and report tool that provides an excellent framework for expansion. The authors indicate that SATAN stands for "Security Analysis Tool for Auditing Networks".

Kerberos[5]: Kerberos is a network authentication system developed at MIT (Massachusetts Institute of Technology) to address the problem. It enables users communicating over networks to prove their identity to each other while optionally preventing eavesdropping or replay attacks. It provides data secrecy using encryption. Kerberos provides real-time authentication in an insecure distributed environment.

6.3 Law Harmonization and Standardization

To avoid many malicious possibilities it is today's research and development task to produce the crime-resistant products of the future. Therefore, we must take every opportunity we can to use science and technology to reduce crime and improve the quality of our lives.

In order for a wide implementation of this technology, standards must be developed that will allow for their consistent use. The International

[4] SATAN features an easy-to-use interface, an extensible framework, and a scalable approach to checking systems. First, the user interface consists of HTML pages that are used through a Web browser such as Mosaic or Netscape.

[5] KERBEROS model is based on a trusted third-party authentication protocol. The original design and implementation of Kerberos was the work of MIT Project Athena staff members. Kerberos is publicly available and has seen wide use.

Organization for Standards ISO is the governing body of international security standards, but this standardization is still in progress. Apply to the vast majority of people in the private sectors and government. The standard BS (British Standard) 7799 has also developed into a family of international standards ISO/IEC (International Organization for Standardization and the International Electrotechnical Commission) 27000 which is further supported by the standard 27006, and provided a global accreditation scheme, and the mutual recognition of certificates ISMS[6] worldwide.

ISO/IEC 27000 standard covers some parts of Information Security Management:

ISO/IEC 27001:2005 Information technology-Techniques to ensure the security-Information Security Management Systems-specification with guidance (Information technology-Security techniques-Information Security Management Systems-Requirements).

ISO/IEC 27002:2005 Information technology-Techniques for ensuring safety-Code for the management of Information Security (Information technology-Security techniques-Code of practice for Information Security Management).

ISO/IEC 27006:2007 Information Technology-techniques for ensuring safety-Requirements for certification bodies (Information technology-Security techniques-Requirements for bodies providing audit and certification of Information Security Management Systems).

About future challenges. Global security trend identified by security experts consulted is the emergence of an entire economy geared to outfit criminals with the tools for cyber terrorism. In fact, industrial cyber espionage may now be consider a necessary part of global economic competition, and secretly monitoring the computerized functions and capabilities of potential adversary countries may also be consider essential for national defense [13].

Reliance on terrestrial laws is an untested approach. Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cybercrimes. The majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court.

About weak penalties limit deterrence. The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects [14].

About self-protection which remains the first line of defense. The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.

About global patchwork of laws, this creates little certainty. Little consensus exists among countries regarding exactly which crimes need to be legislated against. All of countries need to take common steps to address cybercrimes, because in the networked world, no island is an island. Unless crimes are define in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber terrorism will be complicated.

About model approach which is needed. Most of countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for ecommerce [15]. However, few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cybercrime havens.

[6] ISMS—Information Security Management System. url: http://www.educause.edu/blog/StuartYeates/ISO27001InformationSecurityMan/166151 (04.27.2009)

References

[1] Assange. 2012. “Mark Zuckerberg Runs a Giant Spy

Machine in Palo Alto, California." Accessed July 17, 2015. http://www.businessinsider.com/deep-state-on-social-networking-privacy-2013-7#ixzz3g8Bpz4Nj.

[2] Wilson, C. 2008. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. CRS Report RL32114.

[3] Denning, E. D. 2015. "Is Cyber War Next?" Social Science Research Council. Accessed July 17, 2015. http://www.ssrc.org/sept11/essays/denning.htm.

[4] Verton, D. 2015. "A Definition of Cyber-Terrorism." Computerworld. Accessed July 17, 2015. http://www.computerworld.com/securitytopics/security/story/0,10801,83843,00.html.

[5] Reid, C. 2015. "Terrorists." Accessed July 17, 2015. http://all.net/CID/Threat/papers/Terrorists.html.

[6] Anti Defamation League. 2015. "Terror and Technology." Accessed July 17, 2015. http://www.adl.org/main_Terrorism/archive.htm#terror_and_technology.

[7] Europol. 2003. *Computer–Related Crime within the EU: Old Crimes New Tools; New Crimes New Tools*. Luxembourg: Office for Official Publications of the European Communities.

[8] Zanini, M., and Edwards, S. J. A. 2001. "The Networking of Terror in the Information Age." Arquilla, J., Ronfeldt, D. (eds.). Networks and Netwars: The Future of Terror, Crime and Militancy.

[9] DeWalt, D. 2009. "Cybercrime Versus Cyberlaw." McAfee Virtual Criminology Report. Accessed July 15, 2015. http://fserror.com/pdf/McAfeeReport.pdf

[10] National Institute of Standards and Technology. 1993. "Data Encryption Standard (DES)." *Federal Information Processing Standards Publication*: 46-2.

[11] Mitnick, D. K., Simon, W. L., and Wozniak, S. 2002. *The Art of Deception: Controlling the Human Element of Security*. Hoboken, New Jersey: John Willey & Sons Inc.

[12] Gunaratna, R. 2002. *Inside Al-Qa'ida: Global Network of Terror*. London: Hurst, 57.

[13] Pocar, F. 2004. "New Challenges for International Rules against Cyber-Crime." *European Journal on Criminal Policy and Research* 10 (1): 27-37.

[14] McConnel. 2000. "Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information." Accessed April 12, .2015. https://www.library.cornell.edu/colldev/mideast/cycrime.pdf

[15] Bhatambrekar, S. S. 2007. "Legal Issues and Challenges Involved in Cyber World Business." In *Proceedings of the Ninth European Conference on Information Warfare and Security*, 345.