UDC 600

Robert Brumnik, Miran Vršec, Iztok Podbregar

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

CORE OF THE DIGITAL UNDERGROUND

Purpose – *With this research we will find out relation between worldwide countries which have been updated Convention on Cyber crime (Cyber Crime Laws and Terrorism Acts) up to y.2006, and Cyber attacks done up to y.2006. The primary research questions is; What is Cyber attacks impacts on Countries with Cyber Crime Laws and Terrorism Acts updated, comparative to Countries which not update Cyber Crime Laws and Terrorism Acts. Are Countries with updated Laws and Acts considerable less exposure to attacks, from Countries witch haven't Laws and Acts updated?*

Design/Methodology/Approach – *A mixed research method approach was used.*

Findings – *Research results shown on decreasing index (percent) of Cyber attacks in U.S. of America which have updating Cyber Crime Law and Terrorism Acts in years 2000.*

Research limitations/Implications – *In this comparison research we based on pre-research data's. Responders from second part of research (attack impact from y.2000 to y.2006) were from close base of U.S.-based members of the Computer Security Institute (CSI), information security professionals. Research conclusions in this paper are summarizing from one country U.S. of America.*

Practical Implications – *In article we examine how activists, hacktivists, and Cyber terrorists use the Information Technologies and what impacts they have been to exert on government and nongovernmental, Information Security Law. Article describes modern Cyber attacks, Netwar techniques, and offer worldwide overview methods of modern Warfare.*

Originality Value – *The techniques that have been developing to disrupt the "Cybercriminal" are now being implementing in the "War on Terrorism". This has greatly increased the burden on, and risks for, all in the government and commercial sector, together with their professional advisers.*

Paper type: *Survey Paper.*

Keywords: *Computer Systems Disrupting, Cybercrime, Botnets.*

1. Basic Methods for Disrupting Computer Systems

There are several effective methods for disrupting computer systems. This paper focuses on the methods known as cyberattack, or computer network attack, which uses malicious computer code to disrupt computer processing, or steal data. Brief descriptions of three different methods are shown here. Attacks against computers may disrupt hardware reliability and equipment, change processing logic, or steal and corrupt data (All methods of computer attack are within the current capabilities of several nations. See CRS Report RL31787, Information Operations and Cyberwar: Capabilities and Related Policy Issues, by Clay Wilson). However, as technology changes, future distinctions between these methods may begin to blur. This methods based on the technology asset against which each attack mode is directed, and produce effects of each method. The assets affected or effects produced can sometimes overlap for different attack methods such as:

Conventional kinetic weapons can be directed against transmission lines, a computer equipment, computer facility or to create a physical attack that disrupts equipment reliability.

The power of electromagnetic energy, most commonly in the form of an electromagnetic pulse which can be used to create an electronic attack (EA) directed against data transmissions or computer equipment. By overheating circuitry or jamming communications, EA disrupts the integrity of data and the reliability of equipment.

Malicious code is wery often used to create a cyberattack, or computer network attack, directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting a vulnerability in computer software, or a weakness in the computer security practices of an organization. This type of cyberattack can disrupt the reliability of equipment, the confidentiality of communications, and the integrity of data.

2. Botnets

Botnets are becoming a major tool for cybercrime, partly because they can be designed to very effectively disrupt targeted computer systems in different ways, and because a malicious user, without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal. "Bot Networks," or Botnets, are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-

controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code. Botnet code was originally distributed as infected e-mail attachments, but as users have grown more cautious, cybercriminals have turned to other methods. When users click to view a spam message, botnet code can be secretly installed on the users' PC. A website may be unknowingly infected with malicious code in the form of an ordinary-looking advertisement banner, or may include a link to an infected website. Clicking on may install botnet code. Also botnet code can be silently uploaded, even if the user takes no action while viewing the website, merely through some un-patched vulnerability that may exist in the browser. Antivirus software and firewalls do not inspect all data that is downloaded through browsers. Some of bot software may disable antivirus security before infecting the PC. Once a PC has been infected, the malicious software establishes a secret communications link to a remote "botmaster" in preparation to receive new commands to attack a specific target. Meanwhile, the malicious code may also automatically probe the infected PC for personal data, or may log keystrokes, and transmit the information to the botmaster. The Shadowserver Foundation is an organization that monitors the number of command and control servers on the Internet, which indicates the number of bot networks that are being controlled online at a given time. From November 2006 through May 2007, approximately 1,400 command and control servers were found to be active on the Internet. The number of individual infected drones that are controlled by these 1,400 servers reportedly grew from half a million to more than 3 million from March to May 2007. Symantec, another security organization, reported that it detected 6 million bot-infected computers in the second half of 2006 (Bort, 2007).

Some botnet owners reportedly rent their huge networks for US$200 to $300 an hour, and botnets are becoming the weapon of choice for fraud and extortion (MacLean, 2005). This, in turn, is expected to help increase the demand for malware services in future years (McAfee Virtual Criminology Report: Organized Crime and the Internet, December 2006, url:http://www.sigma.com.pl/pliki/albums/userpics/ 10007/Virtual_Criminology_Report_2006.pdf (05.04. 2009) url: http://www.sigma.com. pl/pliki/ albums/ userpics/10007/VirtualCriminology_Report_ 2006.pdf (05.04.2009)). One class of botnet architecture that is beginning to emerge uses peer-to-peer protocol (Gnutella emerged as the first fully decentralized peer-to-peer protocol in 2000, and was used on the Internet to share and swap music files in MP3 compression format. The music industry was often frustrated in their efforts to counter this peer-to-peer technology because it could not identify a main controlling source. Since then, several other peer-to-peer protocols have been developed), which, because of its decentralized control design, is expected to be more resistant to strategies for countering its disruptive effects (Symantec, Trojan.Peacomm: Building a Peer-to-Peer Botnet, 2007, http://www.symantec.com/ enterprise/security_response/weblog/2007/01/trojanpeacomm_building_a_peert.html Matthew Broersma, Peer-to-Peer Botnets a New and Growing Threat, CSO Online, April 17, 2007). For example, some experts reportedly argue that a well-designed peer-to-peer botnet may be nearly impossible to shut down as a whole because it may provide anonymity to the controller, who can appear as just another node in the bot network (Espiner, 2006).

3. Research for updating Cyber Law and Terrorism Act up to y. 2006

Over fifty national governments responded with recent pieces of legislation, copies of updated statutes, draft legislation, or statements that no concrete course of action has been planned to respond to a cyber attack on the public and private sector. Countries were provided the opportunity to review the presentation of the results in draft, and this report reflects their comments.

In this section (Figure 1) we research countries approach to Cyber Convention updated in y.2000. We can see that only 10 countries have fully updated Cyber Conventtion in y. 2000.

For furthure research (Chapter 3.1) we deside to fully researh U.S. of America from y.2000 to y.2006 cause of well-formed Information Technology. Our supposition is that U.S. of America have highly developed Information Technology from all of updated country in y.2000 so we can resume on competent research case.

3.a. About the Methodology, Respondents and Organizations.

(Respondents are drawn from a pool of U.S.-based members of the Computer Security Institute (CSI), 33-year-old professional organization for information security professionals. Details on survey methodology can be found in url: http://americas.utimaco. com/encryption/fbi_csi_2006_p6.html (15.05.2008)).

Information about organizations that responded (615 respondents) we can find in this chapter. There are, organizations covered by the survey include many areas from both the private and public sectors. The sectors with the largest number of responses came from finance (17 %), followed by consulting (14%), information technology (11 %) and manufacturing (9%). The portion coming from government agencies (combining federal,

state and local levels) was 14 %, and educational institutions accounted for 8 % of the responses. The diversity of organizations responding was also reflected in the 11 % designated as "other." The proportion of respondents coming from the various sectors remains roughly the same as in previous years. All shared information about occasions when their defenses were overrun and, in particular, to provide data regarding financial damages, the survey is conducted anonymously. A necessary result of this is that direct longitudinal analyses are not possible. For nearly all categories of attacks or misuse, (See figure 2) shows, the trend of such attacks detected appears to be decreasing over the years. However, there have been some small increases of reported attacks involving system penetration, financial fraud, sabotage, Web site defacement and misuse of public Web applications. Attacks involving unauthorized access to information and theft of proprietary information were reported at virtually the same levels as reported for y. 2005.

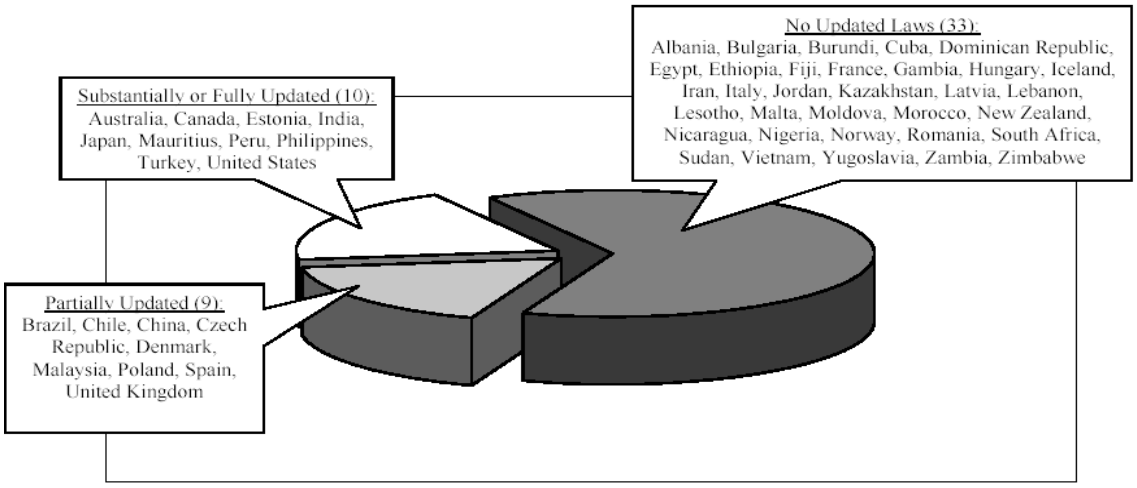

Figure 1. Progress on Updating Cyber Crime Laws in y.2000 (McConnell International website, www.mcconnellinternational.com , for each of the countries)

4. Research of most significant Cyber attacks on worldwide government's infrastructure in y.2007

(Some details of Researh are summarized from McAffe »Virtual Criminology Report« from y.2007 and from url:http://www.timesonline.co.uk/tol/ news/ world/asia/article2388375.ece (12.05.2008), url:http:// www.guardian.co.uk/china/story/0,,2162161,00.html (12.05.2008), url: http://news.zdnet.co.uk/ security/ 0,1000000189,39290289,00.htm (12.05.2008), url: http://www.washingtonpost.com/wp-dyn/content/ article/2007/05/18/AR2007051802122_2.html (12.05. 2008), url: http://www.csmonitor.com/2007/ 0914/ p01s01-woap.html (12.05.2008), url: http:// seattle times.nwsource.com/html/nationworld/2003886833_chi nahack16.html (12.05.2008)).

However, investigation into the incident continues, and officials from the United States view some aspects of the event as a possible model for future cyberwarfare or cyberterrorism directed against a nation state. In January 2008, a court in Estonia convicted and fined a local man for bringing down a government website, as part of the extended cyberattack in 2007. The 20- year-old, who is apparently an ethnic Russian Estonian, used his home PC to carry out the attack. The investigation continues, and so far, he is the only person convicted for participating in the cyberattack against Estonia (Sachoff, 2008).

5. Case: Estonia, 2007

In the Spring of 2007, government in Estonia experienced a sustained cyberattack that has been labeled by various observers as cyberwarfare, cyberterror or cybercrime. On April 27, in Estonia officials moved a Soviet-era war memorial commemorating an unknown Russian who died fighting the Nazis. The move stirred emotions, and led to rioting by ethnic Russians, and the blockading of the Estonian Embassy in Moscow. The event also marked the beginning of a series of large and sustained Distributed Denial-Of-Service (DDOS) attacks launched against several Estonian national websites, including government ministries and the prime minister's Reform Party (Vamosi, 2007). In the early days of the cyberattack, government websites that normally receive around 1,000 visits a day reportedly were receiving 2,000 visits every second. This caused the repeated shut down of some websites for several hours at a time or longer, according to Estonian officials (Rhoads, 2007). Security experts say that the cyberattacks against Estonia were unusual because the rate of the packet attack was very high, and the series of attacks lasted weeks, rather than hour or days, which is more commonly seen for a denial of service attack (Marsan, 2007). Eventually, NATO and the United States sent computer security experts to Estonia to help recover from the attacks, and to analyze the methods used and

attempt to determine the source of the attacks. This event can serve to illustrate how computer network technology has blurred the boundaries between crime, warfare, and terrorism. A persistent problem during and after any cyberattack is accurate identification of the attacker, by finding out whether it was sponsored by a nation, or was the independent work of a few unconnected individuals, or was initiated by a group to instill frustration and fear by damaging the computerized infrastructure and economy. Initially, the Russian government was blamed by Estonian officials for the cyberattacks, and there were charges of cyberwarfare. Other observers argued that the cyberattack involved collusion between the Russian government and transnational cybercriminals who made their large botnets available for short-term rent, either to individuals or to larger groups. However, not all security experts agree, and it remains unclear at this time whether the cyberattacks were sanctioned or initiated by the Russian government, or if a criminal botnet was actually involved. After some investigation, network analysts later concluded that the cyberattacks targeting Estonia were not a concerted attack, but instead were the product of spontaneous anger from a loose federation of separate attackers.

These analysts state that although access to various Estonian government agencies was blocked by the malicious code, there was no apparent attempt to target national critical infrastructure other than internet resources, and no extortion demands were made.

Their analysis thus far concluded that there was no Russian government connection to the attacks against.

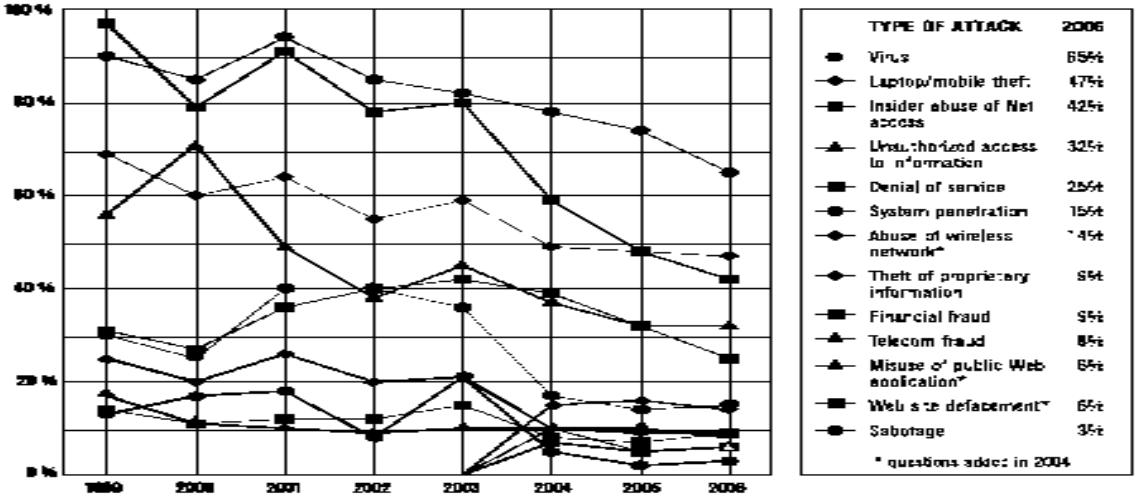

Figure 2: Types of attack or misuse detected up to y.2006 by percentage respondents (Figure 3 is summarized from CSI/FBI Computer Crime and Security Survey 2006. Source: Computer Security Institute url: http://americas.utimaco.com/encryption/fbi_csi_2006_p3.html (14.05.2008)

Estonia (Heise Security, Estonian DDoS - a final analysis, url: http:// www.heise-security.co.uk/news/print/90461 (01.04.2009)).

However, investigation into the incident continues, and officials from the United States view some aspects of the event as a possible model for future cyberwarfare or cyberterrorism directed against a nation state. In January 2008, a court in Estonia convicted and fined a local man for bringing down a government website, as part of the extended cyberattack in 2007. The 20- year-old, who is apparently an ethnic Russian Estonian, used his home PC to carry out the attack. The investigation continues, and so far, he is the only person convicted for participating in the cyberattack against Estonia (Sachoff, 2008).

6. Trends in Cybercrime Methods

Cybercrime is usually conducted through a connection to the Internet, but can also involve unauthorized removal of data on small, portable flash drive storage devices. Cybercrime, usually in the form of network hacking, has involved persons with strong technical skills, often motivated by the desire to gain popularity among their technology peers.

However, the growing trend is now to profit from these network cyberattacks by targeting specific systems, often through collaboration among criminals and technical experts. The motives that drive these cybercriminal groups now may differ from those of their paying customers, who may possess little or no technical skills. New technologies continue to outpace policy for law enforcement. Sophisticated tools for cyberattack can now be found for sale or for rent on the Internet, where highly-organized underground cybercrime businesses host websites that 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 antisecurity features, and seek to recruit new and talented software engineering students into their organizations.

UNITED STATES In June 2007, a Pentagon computer network was hacked into by China-based perpetrators in "one of the most successful cyber attacks" on the US Department of Defense. While it is questionable how much sensitive information was stolen, the incident succeeded in raising concerns to a new level as it highlighted how systems could be disrupted at critical times. Many were quick to point the finger at the Chinese military, but a Chinese Foreign Ministry spoke-sperson dismissed the allegations as groundless."

GERMANY Germany's respected weekly, Der Spiegel, reported that China was thought to have hacked into the computer systems of Germany's chancellery as well as systems at three ministries, infecting the networks with spy programs. The alleged attacks occurred just before Chancellor Angela Merkel visited Beijing. Computers in the chancellery and the foreign, economics and research ministries were targeted. The German Federal Office for the Protection of the Constitution (BfV) conducted a comprehensive search ofgovernment IT installations and prevented a further 160 gigabytes of information from being transferred to China. They described it as "the biggest digital defense ever mounted by the German state." The information was being siphoned off almost daily by hackers in Lanzhou (northern China) in Canton Province and in Beijing. The scale and nature of the stolen data suggested that the operation could have been steered by the state.

ESTONIA In April 2007, Estonia experienced distributed denial-of-service (DDoS) attacks on government, and bank servers for several weeks. The incidents followed the removal of a Soviet statue from a central Tallinn Square to the outskirts of the city. At the height of these attacks, 20,000 networks of compromised computers were linked, and analysis of the malicious traffic showed that computers from the United States, Canada, Brazil, Vietnam and others were involved. "It was a political campaign induced by the Russians; a political campaign designed to destroy our security and destroy our society. The attacks had hierarchy and co-ordination," said Mikhel Tammet, director of the Estonian communication and information technology department. It was a probing attack from which attackers and defenders both learned a great deal. Russian officials deny that claim. Kremlin representative Dmitri Peskov called it "out of the question" that the Russian government was involved in the attacks.

INDIA The National Informatics Centre (NIC) was reportedly attacked from dial-up Internet connections in China. Key intelligence officials claimed that hackers broke into the e-mail accounts of 200 ministers, bureaucrats and defense officials and continue to raid Indian servers at the rate of three to four a day.vi China has denied all claims that it is behind the attacks.

NEW ZEALAND & AUSTRALIA Asia Pacific News reported that Chinese hackers had allegedly tried to hack into highly classified government computer networks in Australia and New Zealand as part of a broader international operation to glean military secrets from Western nations. According to news.com.au, Canberra refused to either confi rm or deny that its agencies, including the Defense Department, had been subject to cyber attack. New Zealand Prime Minister Helen Clark confirmed that foreign intelligence agencies had tried to hack into government computer networks but had not compromised top-secret data banks. The Chinese government has denied any involvement.

Where illicit profits are potentially very large, some high-end criminal groups have reportedly adopted standard IT business practices to systematically develop more efficient and effective computer code for cybercrime. Studies also show that organized crime groups now actively recruit college engineering graduates and technical expert members of computer societies, and sponsor them to attend more information technology (IT) courses to further their technical expertise.

Literature and sources

1. Bort J. Network World / J. Bort // Attack of the Killer Bots. – 2007. – P. 29.

2. Crabb G. U.S. Postal Service Global Investigations, and Yuval Ben-Itzhak, CTO Finjan // Presentation at the Gartner IT Security Summit 2007. – Washington: DC, 2007. – 234 p.

3. Europol: Computer-related crime within the EU / Old crimes new tools; new crimes new tools. Luxembourg // Office for Official Publications of the European Communities,

2003. – 176 p.

4. Espiner T. Security Expert / T. Espiner // Storm Botnet services Could Be Sold, 2007. – CnetNews.com: http: //www.news.com/Security-expert-Storm-botnet-services-could-besold/2100-7349_3-6213781.html.

5. Lemos R. Bot software looks to improve peerage / R. Lemos // The Register, 4 May 2006. – http://www.there gister.co.uk/2006/05/04/nugache_p2p_botnet/(03.05.2009)

6. MacLean S. Report warns of Organized Cyber Crime / S. MacLean // ItWorldCanada, 2005. – url: http:// www.itworldcanada.com/a/IT-Focus/39c78aa4-df47-4231-a083-ddd1ab8985 fb.html (05.04.2009)

7. Marsan C. Examining the Reality of Cyberwar in Wake of Estonian Attacks / C. Marsan // Network World. – Vol. 24, 2007. – № 33. – p. 24.

8. Mitnick D.K. The Art of Deception: Controlling the Human Element of Security / D.K. Mitnick. – Indianapolis: John Wiley & Sons Inc, 2002. – 246 p.

9. Pocar F. New Challenges for International Rules against Cyber-Crime / F. Pocar // European Journal on Criminal Policy and Research. – Vol. 10, 2004. – № 1. – P. 27-37.

10. Rhoads C. Cyber Attack Vexes Estoni / C. Rhoads Poses Debate; The Wall Street Journal, 2007. – P. A6.

11. Sachoff M. Man Convicted In Estonia Cyber Attack / M. Sachoff // WebProNews, January 24, 2008. – url: http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack (25.02.2009)

12. Vamosi R. Cyberattack in Estonia What It Really Means / R. Vamosi. – CnetNews.com, 2007. – url: http:// news.com.com/Cyberattack+in+Estonia-what+it+really+ means/2008-7349_3-6186751.html (02.04.2009).

13. Wilson C. CRS Report for Congress / C. Wilson // Cybercrime and Cyberterrorism:Vulnerabilities and Policy Issues for Congress. – Washington, 2008. – 166 p.

Надійшла до редколегії 18.02.2009

Рецензент: канд. техн. наук, доцент С.В. Кавун, Харківський національний економічний університет, Харків.

ОСНОВА ЦИФРОВОГО АНДЕГРАУНДУ

Роберт Брумник, Міран Вржек, Іжток Подгрегар

На основі представленого дослідження можливе одержання співвідношень стану справ у розвинених країнах миру, які прийняли Угоду про кіберзлочини (Закон про кіберзлочини й терористичні акти) і здійснених кібератаках до 2006 року. Розглянуті первинні дослідницькі питання: що являє собою кібератака для країн із прийнятими змінами в законах і актах про тероризм і кіберзлочини у порівнянні із країнами, де ці зміни не були прийняті. Проведено дослідження країн із внесеними змінами в закони й акти й країн, де ці зміни не були прийняті.

Ключові слова: *комп'ютерні системи, що руйнуються, кіберзлочинність, ботнети.*

ОСНОВА ЦИФРОВОГО АНДЕГРАУНДА

Роберт Брумник, Миран Вржек, Ижток Подгрегар

На основе представленного исследования возможно получение соотношений состояния дел в развитых странах мира, которые приняли Соглашение о киберпреступности (Закон о киберпреступности и террористических актах) и осуществленных кибератаках до 2006 года. Рассматриваемые первичные исследовательские вопросы: что представляет собой кибератака для стран с принятыми изменениями в законах и актах о терроризме и киберпреступлениях по сравнению со странами, где эти изменения не были приняты. Проведено исследование стран с внесенными изменениями в законы и акты и стран, где эти изменения не были приняты.

Ключевые слова: *разрушаемые компьютерные системы, киберпреступность, ботнеты.*