Ishhanova G.T.

What is Cyber terrorism?

Cyber terrorism conjures up images of vicious terrorists unleashing catastrophic at-tacks against computer networks, wreaking havoc, and paralyzing nations. This is a frightening scenario, but how likely is it to occur? Could terrorists cripple critical military, financial, and service computer systems? Psychological, political, and economic forces have combined to promote the fear of cyber terrorism. From a psychological perspective, two of the greatest fears of modern time are combined in the term «cyber terrorism.» The fear of random, violent victimization segues well with the distrust and outright fear of computer technology. Many of these fears, the report contends, are exaggerated: not a single case of cyber terrorism has yet been recorded, hackers are regularly mistaken for terrorists, and cyber defenses are more robust than is commonly supposed. Even so, the potential threat is undeniable and seems likely to increase, making it all the more important to address the danger without inflating or manipulating it.

Key words: Cyber terrorism, computer, communication, information.

Ищанова Г.Т.

Кибертерроризм дегеніміз не?

Кибертерроризмнің пайда болуы компьютерлік желілерге қарсы шабуыл келтіруге пайдаланатын және нәтижесінде мемлекетке апат салдарын әкелетін ақпараттық және компьютерлік технологиялардың пайда болуымен байланысты. Біздің әрқайсымызды бұл үрейлендіретін көрініс ойландырары хақ. Шындығында террористер стратегиялық маңызды әскери, қаржылық және компьютерлік желілерге зиян келтіре алады ма? Халықаралық қауымдастық кибертерроризмді жою мақсатында психологиялық, саяси және экономикалық потенциалды біріктіру үшін қолдан келгеннің барлығын жасап күш салуда. Психологиялық көзқарас тұрғысынан, «кибертерроризм» терминінде қазіргі кезде екі үлкен қорқыныш біріктірілген. Кездейсоқ, күшті қылмыстылық қорқынышы компьютерлік технологиялар алдындағы тікелей қорқыныш және сенімсіздікке ұласуда. Бұл құбылыспен байланысты қорқыныш пен уайым көптеген жағдайларда бірнеше есе ұлғайтылып, кибертерроризм жағдайы тіркелмеген. Хакерлер террористермен үнемі қабылдануда. Киберқабілеттілік біз ойлағанымыздан да әлдеқайда тұрақты. Бірақ басым қауіптілік бар, сондықтан мұндай текті қылмыстардың алдын алу шаралары іске асырылуы қажет.

Түйін сөздер: кибертерроризм, компьютер, байланыс, ақпарат.

Ищанова Г.Т.

Что есть кибертерроризм?

Появление кибертерроризма связано с развитием информационных и компьютерных технологий, используемых террористами для нанесения атак против компьютерных сетей, а в результате – катастрофические последствия для той или иной страны. Каждый из нас призадумается над этим пугающим сценарием. Могут ли в реальности террористы нанести вред стратегически важным военным, финансовым и компьютерным служебным системам? Мировое сообщество делает все необходимое, чтобы объединить психологический, политический и экономический потенциал с целью предотвращения самого кибертерроризма и страха перед ним. С психологической точки зрения два самых больших страха настоящего времени объединены в одном термине «кибертерроризм». Страх перед случайной, сильной виктимизацией непосредственно переходит в недоверие и прямой страх перед компьютерной технологией. Переживания и страхи перед данным явлением в большинстве случаев сильно преувеличены, так как ни один случай кибертерроризма еще не был зарегистрирован, хакеры регулярно принимаются за террористов, и киберобороноспособность более устойчива, чем обычно мы предполагаем. Однако потенциальная угроза есть, поэтому необходимо предпринимать меры с целью профилактики данного рода преступлений.

Ключевые слова: кибертерроризм, компьютер, коммуникация, информация.

UDC 341.1/8

Ishhanova G.T.

Universitet Narhoz,
Kazakhstan, Almaty
E-mail: gulnar_tore@mail.ru

WHAT IS CYBER TERRORISM?

There have been several stumbling blocks to creating a clear and consistent definition of the term «cyber terrorism.» First, as just noted, much of the discussion of cyber terrorism has been conducted in the popular media, where journalists typically strive for drama and sensation rather than for good operational definitions of new terms. Second, it has been especially common when dealing with computers to coin new words simply by placing the words «cyber,» «computer,» or «information» before another word. Thus, an entire arsenal of words-cybercrime, cyber war, info war, net war, cyber terrorism, cyber harassment, virtual-warfare, digital terrorism, cyber tactics, computer warfare, information warfare, cyber-attack, cyber war, and cyber break-ins is used to describe what some military and political strategists describe as the «new terrorism» of these times [1].

Fortunately, some effort has been made to introduce greater semantic precision. Most notably, Dorothy Denning, a professor of computer science, has put forward an admirably unambiguous definition in numerous articles [2], and in her testimony on the subject before the congressional House Armed Services Committee:

Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

It is important to distinguish between cyber terrorism and «hacktivism,» a term coined by Denning to describe the marriage of hacking with political activism. («Hacking» is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software.). Hacktivists have four

main weapons at their disposal: virtual sit-ins and blockades; automated e-mail bombs; web hacks and computer break-ins; and computer viruses and worms. A virtual sit-in or blockade is the cyberspace rendition of a physical sit-in or blockade: political activists coordinate their visits to a website and attempt to generate so much traffic toward the site that other users cannot reach it, thereby disrupting normal operations while winning publicity – via media reports – for the protesters' cause. When large numbers of individuals simultaneously attack a designated site, the operation is sometimes referred to as «swarming.» Swarming can also amplify the effects of the hacktivists' second weapon: e-mail bombing campaigns (bombarding targets with thousands of messages at once, also known as «ping attacks»). In July 1997, for example, an e-mail bombing was conducted against the Institute for Global Communications (IGC), a San Francisco-based Internet Service Provider (ISP) that hosted the web pages of Euskal Herria (in English, the Basque Country Journal), a publication edited by supporters of the Basque separatist group Homeland and Liberty (ETA) [3]. The at-tackers wanted ETA's site pulled from the Internet. To accomplish this they bombarded IGC with thousands of spurious e-mails routed through hundreds of different mail re-lays, spammed IGC staff and customer accounts, clogged IGC's web page with bogus credit card orders, and threatened to employ the same tactics against other organizations using IGC services. IGC pulled the Euskal Herria site just a few days later.

Many cyber protesters use the third weapon in the hacktivists' arsenal: web hacking and computer break-ins, whereby they hack into computers to access stored information, communication facilities, financial information, and so on. For example, the Computer Emergency Response Team Coordination Center (CERT/CC), a federally funded research and development center operated by Carnegie Mellon University, reported 2,134 computer security incidents such as break-ins and hacks in 1997. This number rose to 21,756 in 2000, and to almost 35,000 during the first three quarters of 2001 alone. In 2003, CERT/CC received more than half a million e-mail messages and more than nine hundred hotline calls reporting incidents or requesting information. In the same year, no fewer than 137,529 computer security incidents were reported. Considering that many, perhaps most, incidents are never reported to CERT/CC or any other third party, these numbers become even more significant. Further, each incident that is reported corresponds to an attack that can involve thousands of victims. In April 2002, for instance, hackers broke into the payroll database for the state of California and gained access to the Social Security numbers, bank account information, and home addresses of 265,000 state employees. This rise in computer-based attacks can be attributed to several factors, including the growth of the Internet and a corresponding increase in the number of potential attackers and targets; a seemingly limitless supply of vulnerabilities that, once discovered, are quickly exploited; and increasingly sophisticated software hacking tools that allow even those with modest skills to launch devastating attacks.

The fourth category of hacktivist weaponry comprises viruses and worms, both of which are forms of malicious code that can infect computers and propagate over computer networks. Their impact can be enormous. The Code Red worm, for example, infected about a million servers in July 2001, and caused $2.6 billion in damage to computer hardware, software, and networks, and the I LOVE YOU virus unleashed in 2000 affected more than twenty million Internet users and caused billions of dollars in dam-age. Although neither the Code Red worm nor the I LOVE YOU virus was spread with any political goals in mind, some computer viruses and worms have been used to propagate political messages and, in some cases, cause serious damage.

Hacktivism, although politically motivated, does not amount to cyber terrorism. Hacktivists do want to protest and disrupt; they do not want to kill or maim or terrify. However, hacktivism does highlight the threat of cyber terrorism, the potential that individuals with no moral restraint may use methods similar to those developed by hackers to wreak havoc. Moreover, the line between cyber terrorism and hacktivism may sometimes blur, especially if terrorist groups are able to recruit or hire computer-savvy hacktivists or if hacktivists decide to escalate their actions by attacking the systems that operate critical elements of the national infrastructure, such as electric power networks and emergency services.

References

1 D. Ronfeldt and J. Arquilla. «Networks, Netwars, and the Fight for the Future.» First Monday 6(10) (2001); J. Arquilla and D. Ronfeldt. «The Advent of Netwar» (revisited) (2001). In Networks and Netwars, edited by J. Arquilla and D. Ronfeldt (Santa Monica: RAND Corporation), pp. 1–25).

2 Denning D. 1999. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy (Washington, DC: Nautilus, 1999), available at // http://www.nautilus.org/ infopolicy/workshop/papers/denning.html); D. Denning. 2000a. Testimony before the Special Oversight Panel on Terrorism, U.S. House of Representatives, Committee on Armed Services 23 May 2000a, pp. 11-47.

3 Nicol C. (not dated). «Internet Censorship Case Study: Euskal Herria Journal,» The APC European Internet Rights Project, available at // http://europe.rights.apc.org/cases/ehj.html