CYBER TERRORISM- GLOBAL SECURITY THREAT

Mitko BOGDANOSKI,
Drage PETRESKI1

Abstract: It is more than obvious that the way of conducting terrorism with the time
is becoming more sophisticated. The cyber terrorism is real threat to fast technology
development. Potential targets are systems which control the nation's defenses and
critical infrastructure. The terrorist of the future will win the wars without Þring a shot
- just by destroying infrastructure that signiÞcantly relies on information technology.
The fast growth of the Internet users and Internet dependance dramaticly increased
the security risks, unless there are appropriate security measures to help prevention.
To understand cyber terrorism it is important to look at its background, to see how the
terrorist organisations or individuals are using the advantage of new technology and
what kind of measures governments and international organizations are taking to help
the Þght against cyber terrorism.

Key words: syber, attack, security, terrorism, DoS

Introduction

        Although there are a number of deÞnitions which describe the term terrorism, one of the
deÞnitions that are frequently encountered is that terrorism is "the unlawful use or threatening use
of force or violence by a person or an organized group against people or property with the intention
of intimidating or forcing societies or governments, often for ideological or political reasons." 2

        Interactions between human motives and information technology for terrorist activities in
cyberspace or in the virtual world can be addressed as cyber terrorism. Yet this is

the deÞnition of
cyber terrorism that Sarah Gordon and Richard Ford from Symantec have used in their efforts to
deÞne "pure Cyberterrorism." 3

The cyber terrorism as a concept has various deÞnitions, mostly because every expert in
security has its own deÞnition. This term can be deÞned as the use of information technology by
terrorist groups or individuals to achieve their goals. This may include the use of information technol-
ogy to organize and execute attacks against networks, computer systems and telecommunications
infrastructure, and to exchange information and perform electronic threat. This kind of security

1 The authors are professors at the Military Academy of RM
2 S. Best, DeÞning Terrorism: http://www.drstevebest.org/Essays/DeÞning%20Terrorism.htm
3 www.symantec.com/avcenter/reference/cyberterrorism.pdf

CONTEMPORARY MACEDONIAN DEFENCE
59
♠   INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

threat can manifest itself in many ways, such as hacking computer systems, programming viruses
and worms, Web pages attack, conducting denial of service (DoS) attacks, or conducting terrorist
attacks through electronic communications. More common are claims that cyber terrorism does not
exist and that actually it is a hacking and malicious attacks. Those who support these claims do not
agree with the term "terrorism" because if we take into account the current technologies for preven-
tion and care, the likelihood of creating fear, signiÞcant physical damage or death among population
using electronic means would be very small.

Considering the fact that the terrorists have limited funds, cyber attacks are increas-
ingly attractive, because, their implementation requires a smaller number of people and
certainly smaller funds. Another advantage of cyber attacks is that they allow terrorists to
remain unknown, because they can be very far from the place where the act of terrorism is
committed. Unlike the terrorists that place their camps in countries with weak

governance,
    cyber terrorists can store anywhere and remain anonymous.4 It is believed that
the most effec-
    tive use of cyber terrorism is when it is used in combination with physical
terrorism. For example,
    disabling the operation of emergency services in situations where the need for
deployment of such
    services is caused by the use of physical terrorism is really an effective way
of pooling of mentioned
    types of terrorism. There are huge possibilities of conducting cyber terrorism
through Internet using
    advanced technology.As possible targets of cyber terrorism can be considered
government computer
    networks, Þnancial networks, power plants, etc., and the reason for this is
that the terrorists identi-
    Þes all the above as most suitable targets to be damaged or put out of
operation in order to cause
    chaos. Systems manipulation through "secret entrance" software, stealing
classiÞed information,
    data deletion, Web sites damaging, viruses inserting, etc. are just a few
examples of how terrorists
    can enter into the secured system. The terrorist attacks enabled by computer
technology can be also
    conducted through the air trafÞc control system or rby emote damage of the
power supply networks.

            The new information technologies (IT) and the Internet are more often
used by terrorist
    organizations in conducting of of their plans to raise the Þnancial funds,
distribute their propaganda
    and secure communications. Director of the Central Intelligence Agency (CIA),
George Tenet, in
    his statement in 2000 for global security threats, explained that the terrorist
groups including Hez-
    bollah's, Hamas and al-Qaeda, for support of their operations, use computerized
Þles, e-mails and
    protection (encryption). The convicted terrorist Ramzi Yousef, the main planner
of the attack on the
    World Trade Centre in New York in encrypted Þles in his laptop computer stored
detailed plans for
    aircraft destruction in the United States.5

            The terrorist organizations also use the Internet to "reach out" their
audience, without need
    to use other media such as radio, television or holding various press
conferences. Web pages are
    used as a way to highlight injustice and to seek support for as the call
"political prisoners" wich

are "illegaly captured". Typical Web pages will not display any information related to the violent
activities and will usually claim to be left with no other choice but to resort to violence. They claim
to be persecuted, that their leaders have been targets of assassination and their supporters were
massacred. They use this tactic to give impression that they are weak and to present themselves as
outsiders. This public performance is a very easy way to recruit supporters and members. Besides
propaganda, on the terrorist organizations Web sites can often be found content and instructions on

4 M. Cereijo, Cuba the threat II: Cyberterrorism and Cyberwar, 16 Maj 2006: http://www.lanuevacuba.
com/archivo/manuel-cereijo-110.htm

5 R. L. Dick, Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation,
Before the House Energy and Commerce Committee, Oversight and Investigation Subcomittee Washington,
DC, 05April 2001,
http://www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks

how to make explosives and chemical weapons. This allows them to identify the most common users
that can have sympathy for their cause and because of that this is an effective method for recruiting.

This also helps individuals acting as terrorists to engage in terrorist activities. In 1999, a ter-
rorist named David Copeland killed 3 people and injured 139 in London. He did this with the help
of bombs placed in three different locations. At his trial it was discovered that he used Terrorists
Manual (Terrorist Handbook - Forest, 2005) and How to Make a Bomb (How to Make Bombs -
Bombs, 2004), which had downloaded from the Internet.6

Cyber terrorism

The terrorists use cyberspace to cause uncertainty. They, for their own reasons, are
struggling against state authorities and governments and use all available means to

achieve
their own aim. Cyber attacks occur in two forms, one used to attack data, and others focused
on control systems. 7 Data theft and destruction leads to service sabotage and this is the
most common form of Internet and computer attacks. The attacks focused on the control
systems are used to disable or manipulate the physical infrastructure. For example, you can
perform remote power supply networks, railway and water supplies in order to achieve a
negative opinion on larger geographic areas. This is accomplished by sending data over the
Internet or by penetrating security systems. These weak spots in the system were used in the
incident in Australia that occurred in March 2000, where disgruntled employee (who failed
to provide full-time employment) used the Internet to slip one million liters of unprocessed
sewage into the river and coastal waters in Queensland.8 In fact, after 44 unsuccessful
tries, the 45th was successful. The Þrst 44 trials were not detected at all.

        After the September 11 attacks, the auditors of public safety are worried because
the most critical infrastructures are owned by private companies, which are not always
interested in possible security threats.

        In 1988, a terrorist guerrilla organization, within two weeks, ßood embassies
of Sri Lanka with 800 email-s a day. The message which was appearing was "We are
the Internet Black Tigers and we are doing this to disrupt your communications." De-
partment of Intelligence characterizes the attack as the Þrst known terrorist attack on
government computer systems.

        Internet saboteurs in 1998 attacked Web site of the Indian Bhabha Atomic Re-
search Centre and stole e-mails from the same center. The three anonymous saboteurs
through online interview claimed that they protest against recent nuclear explosions
in India. 9 In July 1997, the leader of the Chinese hacker group claimed that temporarily
disallowed Chinese satellite and announced that hackers set up a new global organization
to protest and prevent investment by Western countries in China.

        In September 1998, on the eve of parliamentary elections in Sweden, saboteurs attack
the Web site of the right-wing political party in Sweden and created a link to a Web

site on

        6 www.terror.net: How Modern Terrorism Uses the Internet, 21 February 2007:
http://www.asiantribune.
com/index.php?q=node/4627

        7 R. Lemos, Cyberterrorism: The real risk, 2002:
http://www.crime-research.org/library/Robert1.htm
        8 Ibid
        9 D.Briere, P.Hurley, Wireless network hacks and mods for dummies, 2005,
Wiley.

CONTEMPORARY MACEDONIAN DEFENCE
                                61
♠INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

the left and to the pornographic sites. The same month, saboteurs attacked the
website of
the Mexican government in protest against government corruption and
censorship.Analysts
point out these crime examples as low level information warfare.

        Romanian hackers on one occasion managed to intrude into the computer systems
controlling the life support systems at an Antartic research station, endangering
the 58
scientists involved. Fortunately, their activity is stopped before any accident
occurred.

        During the Kosovo conßict, Belgrade hackers conducted a denial of service
attack
(DoS) on the NATO servers. They "ßooded" NATO servers with ICMP Ping messages,
typically used for diagnostic or control purposes or generated in response to errors
in IP op-
erations.

        During the Palestinian-Israeli cyber war in 2000 similar attack has been
used. Pro-
Palestinian hackers used DoS tools to attack Israel's ISP (Internet Service
Provider), Netvi-
sion. Although the attack was initially successful, Netvision managed to resist
subsequent
attacks by increasing its safety.

        Also inApril 2007, numerous journalistic organizations associated with the
"Associ-
ated Press" reported that cyber attacks on critical information infrastructure on
Estonia is
conducted by computer servers located in Russia, although it was later determined

that it is
a Distributed DoS attacks carried out by different locations around the world (U.S., Canada,
Brazil, Vietnam and other locations). Of course, the locations of the computers involvedin
the attack do not always shows the location of the direct participants in the attack. It is
actually the location of the so-called "zombie" machines that act as intermediaries during
the attack, without their knowledge or without any knowledge of the direct attackers. The
attack completely put out the function of the Web sites of many governmental, media and
Þnancial institutions and leads to diplomatic talks which was a reason to examine the pos-
sibility of creating a NATO-supported research center capable of identifying the source of
cyber attacks. InAugust 2008, a similar attack was conducted against Georgia. It is assumed
that the attack was perpetrated by Russian hackers.

        In October 2007, hackers attacked the Web site of Ukrainian President Viktor Jush-
enko. The responsibility for this attack took over the radical Russian nationalist youth group,
the Eurasian Youth Movement.10

        An analyst from the U.S. Central Intelligence Agency (CIA) publicly revealed
that in January 2008, hackers successfully stopped power supply networks in several
U.S. cities. In November 2008, the Pentagon had a problem with cyber attacks carried
out by computer virus, prompting the Department of Defense (DoD) to take unprec-
edented step of banning the use of external hardware devices, such as ßash memory
devices and DVDs. 11 OfÞcially, U.S. never felt cyber terrorist attack.

        One of the examples that have caused global panic occurred in late 2008, when
a
group of hackers called "Greek Security Team", "intrude" into CERN computer systems
(European Center for Nuclear Research) so deep, that they were very close to take control

                10 Radio Free Europe, 2007 CONTEMPORARY MACEDONIAN DEFENCE
                11 FOX News, 2008

62
♠   INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

of one of the detectors at LHC (Large Hadron Collider), the largest particle accelerator.

Hackers broke into the system on the Þrst day of the experiment and placed a fake page on
the site of CERN, whose aim was to defame the experts responsible for computer system,
calling them "a group of students." CERN ofÞcials said that it was not caused any damage,
but knowing that the detectors and all valuable equipment is vulnerable to digital threats
is really uncomfortable.

Methods and techniques of the cyber terrorism

As we already explained, except for offencive operations the terrorist can effectively
use the cyberspace for secure communications. 12

Information security is of great importance to many organizations, including the
terrorists. The reason for this primarily lies in their malicious activities, so it is obvious that
they will be faced with a well-equipped government security forces and coalition forces,
that can easily reveal their intentions through the interception of communication using
sophisticated monitoring equipment.

This problem is well known for the terrorist organizations, which is the reason for
them to pay great attention to security aspects during the transmission of subtle information.

"Al Qaeda Training Manual" is just one of the many evidence of the commitment
of terrorist organizations for safe communication. Notably, among the most important and
most extensive lessons described in this guide are two lessons that provide guidance on
the proper usage of communications and data protection. Special emphasis on this issue
is placed in the thirteenth lesson "Secret Writing and Ciphers and Codes" which aim is to
train potential members of this terrorist organization for secure data transmission.

Data hiding by the members of terrorist organizations is revealed on many occasions,
but for sure it can be said that the number of cases where the data transmission covered
using steganographic methods is not registered by security services is much larger.

Evidence for the use of steganography by al-Qaeda terrorist organization is the ar-
rest in Berlin in 2012 of a 22 year old Austrian who had just arrived from Pakistan. Later
it was conÞrmed that he is a member of this terrorist organization. The digital storage and
memory cards he tried to hide were password protected and the information were invisible.
After the initial analysis it was found that inside memory cards was buried a pornographic
video "Kick Ass" and a Þle named "Sexy Tanja". A few weeks later, after great efforts to
combat a password and the software to make the Þle almost invisible, German researchers
encoded in the video of a treasure trove of intelligence - over 100 documents including
al-Qaeda Þrsthand about some of the plots of the terrorist group and a bolder road map for
future operations for which there were not speciÞed neither the date nor the location. Also
various terrorist training manuals used by this organization were found. All these data were
hidden using steganographic tools.

12 M. Bogdanoski,A. Risteski, & S. Pejoski, (2012, November). Steganalysis--A way forward against
cyber terrorism. In Telecommunications Forum (TELFOR), 2012 20th (pp. 681-684). IEEE.

CONTEMPORARY MACEDONIAN DEFENCE
                        63
♠   INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

The National Coordination OfÞce (NCO) for Networking and Information Technol-
    ogy Research and Development (NITRD), in a report released in 2006's gave the following
    statement: 13

"......immediate concerns also include the use of cyberspace for covert communica-
    tions, particularly by terrorists but also by foreign intelligence services; espionage against
    sensitive but poorly defended data in government and industry systems; subversion by
    insiders, including vendors and contractors; criminal activity, primarily involving fraud
    and theft of Þnancial or identity information, by hackers and organized crime

groups... "

"International interest in R&D for Steganography technologies and their commer-
cialization and application has exploded in recent years. These technologies pose a potential
threat to national security. Because Steganography secretly embeds additional, and nearly
undetectable, information content in digital products, the potential for covert dissemination
of malicious software, mobile code, or information is great."

"The threat posed by Steganography has been documented in numerous intelligence
reports."

Rumors about the usage of Steganography by terrorists Þrst appeared in the daily
newspaper "USA Today", on 5 February 2001, in two articles titled as "Terrorist instruc-
tions hidden online" and "Terror groups hide behind Web encryption". In October 2001, the
information looked even more precise: "militant wired Web links to jihad". In October 2001,
"The New York Times" published an article claiming that al-Qaeda had used steganogra-
phy techniques to encrypt and insert messages into images and then transported via e-mail
and possibly via USENET to prepare and execute the September 11, 2001terrorist attacks.

With reference to research on Jamestown Foundation, captured terrorist training
manual "Technical Mujahid, a Training Manual for Jihadists", contains a section titled
"Covert Communications and Hiding Secrets inside Images".

Centre for Steganographic Research and Analysis, during the latest research, identi-
Þed more than 725 applications for digital steganography.14

National responses to the cyber terrorism threat

The European Commission adopted a provision that requires all members of the
European Union all activities deÞned as "attack through interference with information
systems" to be punishable as terrorist act, if their goal is "serious alteration

or destruction
    of political, economic or social structures". France expanded police power to search private
    property without warrants. 15

        13 A. Jahangiri, Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confu-
      sion:
http://www.alijahangiri.org/publication/Cyberspace-Cyberterrorism-and-Information-Warfare-A-Perfect-
      Recipe-for-Confusion.htm

        14 E. S. Othman, Hide and Seek: Embedding Audio into RGB 24-bit Color Image Sporadically Using
      Linked List Concepts: IOSR Journal of Computer Engineering (IOSRJCE), Volume 4, Issue 1 (Sep-Oct. 2012),
      PP 37-44, http://iosrjournals.org/iosr-jce/papers/Vol4-issue1/G0413744.pdf

        15 E. Waak, The Global Reach of Privacy Invasion, Humanist, November/December: http://www.
      thehumanist.org/humanist/articles/waakND02.htm

        Spain, similar to the UK legislation, restricts the activities of any organization that
is directly or indirectly related to the ETA (Euskadi Ta Askatasuna) - an armed separatist
group for Basque Homeland and Freedom. The European Council took steps to establish the
wanted level across Europe and to deÞne the term "terrorist crime." Germany's government
cuts the limits about monitoring telephone calls and monitoring e-mails and bank accounts
and restores previously limited communication between the Secret Service and the police.
In June 2002, the United Kingdom, under the pretext of counter-terrorism, tried to bring
regulations that would mandate almost all local and national government agencies to gain
access to data communications trafÞc without the need of a warrant. 16

        Australia introduced a law on terrorists in order to intercept electronic mail (giving
power to the main Australian Security Intelligence Organisation), and to create an attack
directed against the preparation and planning of terrorist acts. This law allows the

terrorist
property to be "frozen" or taken away. New Zealand has introduced similar legislation in
order to comply with the bilateral agreement on legal harmonization between these two
countries.

India also brought its own decree to protect against terrorism, enabling authorities to
apprehend suspect without trial, to conduct surveillance and to seize money and property
of suspected terrorists, and in some cases to implement the death penalty.17

Some states, such as is the case with the U.S. and Australia, recommended setting
of network operation center in cyberspace, which will include Internet service providers,
and developers (programmers) of computer hardware and software.

Their task is to develop safe technology, as intelligent analysis software, that will be
able to analyze existing data, both public and private, in order to detect suspicious activities.18

Multilateral responses to threats of cyber terrorism

Response of cyber terrorism by the North Atlantic Treaty Organization (NATO)

As sophisticated political-military alliance, NATO has long been familiar with the
use and defense of electronic and information warfare. For years, NATO is involved in
efforts to transform the military organization and conduct of operations by "networking
oriented warfare" and "network enabled capabilities". At the Prague Summit in November
2002, NATO leaders decided to strengthen its capabilities to defend against cyber attacks.
Decision in Prague resulted in many initiatives.19

A new NATO Cyber Terrorism Program is initiated, involving various NATO bod-
ies: NATO Communication and Information Systems ServicesAgency (NCSA), described
as the "Þrst line of defense against cyber terrorism," NATO INFOSEC Techinical Center

16 K. Curran&Others, Civil Liberties and Computer Monitoring, 2004:
http://www.jiti.com/v05/jiti.
v5n1.029-038.pdf

17 Ibid
18 B. Simons, & E. H. Spafford, Inside Risks 153 , Communications of the
ACM, 46(3), March 2003
19 NATO Prague Summit Declaration Article 4(f), 21 November 2002:
http://www.nato.int/docu/
pr/2002/p02-127e.htm.

CONTEMPORARY MACEDONIAN DEFENCE

(NITC), responsible for communication and computer security; NATO Information As-
surface Operations Centre (NIAOC), responsible for management and coordination of
cryptographic equipment in response to a cyber attack against NATO; NATO Computer
Incident Response Capability (NCIRC), whose task is to protect the NATO encrypted
communications systems.20

After the cyber attack against Estonia in April and May 2007, NATO ministers
agreed on the outline of the NATO's cyber defense concept, which was brought in
Nordwijk, in October 2008.21 This concept at the beginning of 2008 was developed
into a NATO Policy on Cyber Defense.22 The NATO members were informed in more
details about this policy on the NATO Summit held in Bucharest at the beginning of
April 2008. 23

Following the Summit, NATO established Cyber Defence Management Authority
(CDMA), in order to bring together all key players in the NATO activities related to cyber
defense, and better management of the cyber defense support to any member of the alliance
in defense against cyber attack, upon request.24 At the same time, NATO leaders agreed
with the formal establishment of the NATO Cooperative Cyber Defence Center of
Excellence (CCD-CoE), which has been in development since 2004. The signiÞcance
of the CCD-CoE, based in Tallinn, was conÞrmed during the attack of Estonia in 2007,
so in October 2008 the NATO Council grants the Centre full NATO accreditation and
theorganisation obtains the status of International Military Organization.25

"The mission and vision" of the CCD-CoE are described as follows:

"enhance the
    capability, cooperation and information sharing among NATO, NATO nations and part-
    ners in cyber defence by virtue of education, research and development, lessons learned
    and consultation" and to be "the main source of expertise in the Þeld of cooperative cyber
    defence by accumulating, creating, and disseminating knowledge in related matters within
    NATO, NATO nations and partners". 26 The organization current has elevan "nations-
    sponsors": Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland,
    Slovakia, Spain and the USA. Invitation for membership is open to all NATO members,
    but cooperation projects are also conducted jointly with NATO partner countries, academia
    and the private sector.

            20 NATO Communication and Information Systems ServicesAgency: http://www.ncsa.nato.int/topics/
        combating_cyber_terrorism.htm

            21 European Security and Defence Assembly, `Cyber warfare' (Assembly of the Western European
        Union, Defence Committee Report C/2022. 5 November 2008), p.19.

            22 NATO, `Defence against cyber attacks', 26 June 2008: http://www.nato.int/issues/cyber_defence/
        index.html.

            23 NATO, Bucharest Summit Declaration, Art. 47, 3 April 2008: http://www.nato.int/docu/pr/2008/
        p08-049e.html.

            24 NATO, `Defending against cyber attacks: what does this mean in practice?', 31 March 2008: http://
        www.nato.int/issues/cyber_defence/practice.html.

            25 CCD-CoE, `History and way ahead': http://www.ccdcoe.org/12.html
            26 CCD-CoE, `Mission and Vision': http://www.ccdcoe.org/11.html

66 CONTEMPORARY MACEDONIAN DEFENCE
♠INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

        United Nations (UN)

        Cyber security is one of the main themes on the traditional debates on

security policy
in the UN system. Normally this refers to those debates related to the threat of terrorism and
in the form of Resolutions of the UN Security Council. 27 The topic is covered in the work
of the Counter Terrorism Committee established by Security Council,28 and it is mentioned
in the UN Global Counter-Terrorism Strategy.

In the latter case, the goal is not only "counter terrorism in all its forms and manifesta-
tions on the Internet", but also with more active approach to "use the Internet as a tool for
countering the spread of terrorism."29 Wider in the UN systems, cyber security is regularly
recognized as a central feature that will be constantly developed in the international agenda
for international security.

In the UN system, the International Telecommunication Union (ITU) has highest
responsibility for the practical aspects and applications of the international cyber security.

The ITU mission statement embraces the issue of cyber security in direct terms. The
purpose of the organization is to develop conÞdence in the use of cyberspace through
enhanced online security. Achieving of the cyber security and cyber peace are some of the
most critical concerns in the ICT development, and ITU takes concrete measures through
its Global Cybersecurity Agenda (GCA).30

In September 2008, the ITU and the International Multilateral Partnership Against
Cyber Threats (IMPACT) signed an agreement under which GCA is located in IMPACT
headquarter in Cyberjaya, Malaysia.31

Organization for Economic Cooperation and Development (OECD)

Issued in 2002 by the Directorate for Science, Technology and Industry of the OECD,
Guidelines for the Security of Information Systems and Networks have become a standard
reference point for national and international cyber security initiatives. Non-binding guide-
lines adopted by 19 of the 30 members of the OECD as well as Brazil, and the European
Union. The Guidelines apply to all participants in the new information society and

sug-

27 See UN Security Council Resolution 1373: reference to `use of communications technologies by
terrorist groups' (28 September 2001, para. 3(a)):
http://www.un.org/News/Press/docs/2001/sc7158.doc.htm.
UN Security Council Resolution 1624 refers to the need to `prevent terrorists from exploiting sophisticated
technology, communications and resources'(14 September 2005, p.2):
http://daccessdds.un.org/doc/UNDOC/
GEN/N05/510/52/PDF/N0551052.pdf?OpenElement.

28 UN Security Council Counter-Terrorism Committee:
http://www.un.org/sc/ctc/index.html. See also
UN Security Council, `Report of the Counter-Terrorism Committee to the Security Council on the implementa-
tion of resolution 1624 (2005)' (S/2006/737, 15 September 2006), paras 6, 16, 43:
http://daccessdds.un.org/
doc/UNDOC/GEN/N06/520/37/PDF/N0652037.pdf?OpenElement.

29 The Use of Interent for Terrorist Purposed: United Nations OfÞce on Drugs and Crime - Viena,
(September 2012, p.vi),
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.
pdf.

30 ITU Global Cybersecurity Agenda (GCA, Framework for International Cooperation in Cybersecu-
rity), ITU 2007, http://www.ifap.ru/library/book169.pdf

31 Curbing Cyberthreats-IMPACT:
http://www.itu.int/osg/csd/cybersecurity/gca/impact/index.html

CONTEMPORARY MACEDONIAN DEFENCE
                    67
♠   INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

    gest the need for a greater awareness and understanding of security issues and the need to
    develop a "culture of security".

        The guidelines are based on nine complementary principles that organize and
    implement a safety culture: Awareness (the need for security of information systems and
    networks); Responsibility (all participants are responsible for the security of the informa-
    tion systems and networks); Response (participants should act on security

incidents in

   timely and co-operative manner); Ethics (respect the legitimate interests of
other users and

   promotion of best practice); Democracy (security measures should be compatible
with the

   basic values of a democratic society); Risk assessment (broad assessment of
threats and

   weaknesses as a basis for risk management); Security design and implementation
(security

   measures should be an essential feature of information systems and networks);
Security

   management (comprehensive approach involving all stakeholders at all levels,
addressing

   threats as they appear); Reassessment (continuous review, revision and
modiÞcation of

   security measures as risks evolve).32

         Other cyber security initiatives include a series of OECD reports on
informa-

   tion security and privacy, including topics such as national guidelines for
information

   security, OECD guidelines for policies to identify radio frequency and many
others,

   33 and Þnally the Working Party on Security of Information and Privacy (WPSIP),
which

   aims is to provide a "foundation for developing national co-ordinated policies."
34

         Organization for Security and Co-operation in Europe (OSCE)

         OSCE's interest in the challenges of cyber security is increasing. In
December 2004,

   the OSCE Ministerial Council decided to dedicate to the "extent of use of the
Internet by

   terrorist organizations," including a number of activities, such as recruiting
of the terrorists,

   foundation, organization and propaganda.35 Two years later, the foreign
ministers called for

   greater international cooperation and utilizing more effort to protect "vital
critical informa-

   tion infrastructures and networks from the threat of cyber attacks."

         The participating countries were asked to closely monitor Web pages of
the terrorist

   and extremist organizations and to exchange information with other governments
in the

   OSCE and other relevant forums and it is asked "more active participation of
civil society

institutions and the private sector in preventing and countering the use of the Internet for
terrorist purposes." 36 OSCE's Permanent Council has also been a venue for debate and
discussion concerning cyber security. 37 In June 2008, for example, Estonian Defence

32 OECD, Guidelines for the Security of Information Systems and Networks: Toward a Cul-
ture of Security (Paris: OECD, 25 July, 2002), pp. 9-12: http://www.oecd.org/document/42/0,3343,
en_2649_34255_15582250_1_1_1_1,00.html

33 OECD Resources on Policy Issues Related to Internet Governance: http://www.oecd.org/documen
t/21/0,3343,en_21571361_34590630_34591253_1_1_1_1,00.html

34 OECD Working Part on Information Security and Privacy: http://www.oecd.org/document/46/0,33
43,en_2649_34255_36862382_1_1_1_1,00.html

35 OSCE Ministerial Council Decision 3/04: Combating the Use of the Internet for Terrorist Purposes,
7 December 2004: http://www.osce.org/documents/mcs/2004/12/3906_en.pdf

36 OSCE Ministerial Council Decision 7/06: Countering the Use of the Internet for Terrorist Purposes,
5 December 2006: http://www.osce.org/documents/mcs/2006/12/22559_en.pdf

37 OSCE Permanent Council: http://www.osce.org/pc/

Minister Jaak Aaviksoo spoke about immense amount of work that has to be done in the the Þeld of cyber security.38

The OSCE's Forum for Security Co-operation (FSC) also contributed to the organization's involvement in the Þeld of cyber security. Although the FSC's work has been concentrated largely on arms control, disarmament and conÞdence-building measures,39 lately, the forum began to be more interested in cyber security. In October
2008, FBS (in joint session with the Permanent Council) decided to convene an OSCE workshop on a Comprehensive approach to improving cyber security in March 2009.40 Finally, the OSCE supports national efforts, such as the Armenian Forces on Cyber Crime and Cyber Security.41

Council of Europe (CoE)

        Contribution of the CoE in the international cyber security policy is
primarily through
the Convention on Cyber Crime, which was opened for signature in November 2001 and
which entered into force in July 2004. It is important to note that, although the
Convention
was signed by 46 countries, including Canada, Japan, SouthAfrica and the U.S., until
today
it has been ratiÞed by only 26 countries, including Macedonia, Albania, Croatia,
Estonia,
Hungary, Lithuania, Romania and Slovenia, 11EU states have yet to ratiÞed the
Convention
and Þve CoE member states have not even signed (including Russia). Convention was
signed
and ratiÞed by countries that are not members of the CoE (Canada, Japan, South
Africa
and USA).42 Sixteen other countries that are not members of the Council of Europe
are
reported as "known to use the Convention as a guideline for their national
legislation"
(including Brazil and India).

        The CoE Convention on Cybercrime is important for several aspects. First, the
Convention addresses the illegal activities and practices that features across
spectrum
of cyber security threats. Second, the Convention establishes common standards and
procedures that are legally binding on its signatories. Third, the Convention is
open to
the Member States of the CoE and others, which increases its authority as an
interna-
tional instrument. Finally, the Convention introduced requirements for handling data
and access that have led to concerns about the privacy law and civil liberties.

     G-8

        The main contribution of the G-8 in international cyber security policy is a
Sub-
group of High-Tech Crime, created as a subset of Lyon Group in 1996 to combat trans-

        38 OSCE Permanent Council, `OSCE can play important role in cyber security,
says Estonian defence

Minister', Vienna, 4 June 2008: http://www.osce.org/pc/item_1_31483.htm

        39 OSCE Forum for Security Co-operation: http://www.osce.org/fsc/
        40 OSCE FSC/PC 36th Joint Meeting, FSC Decision No. 10/08, `OSCE Workshop
on a Comprehensive
OSCE Approach to Enhancing Cyber Security', 29th October 2008:

http://www.osce.org/fsc/

        41 OSCE, `OSCE ofÞce organises discussion in Yerevan on cyber security
threats', 21 March 2006:
http://www.osce.org/item/18450.html

        42 Council of Europe Convention on Cybercrime:
http://conventions.coe.int/treaty/Commun/Cher-

cheSig.asp?NT=185&CM=8&DF=&CL=ENG

    national organized crime. The purpose of this subgroup was to "enhance the
ability of the
    G-8 countries to protect, investigate and prosecute crimes committed using
computers,
    network communications, and other new technologies." The mission of the subunit
was
    subsequently extended to include the use of the Internet by terrorists and the
protection
    of critical information infrastructure. Subgroup is trying to deal with cyber
crime not only
    within the jurisdiction of the G8 countries, but also to create guidelines that
could take and
    implement other countries. The subgroup has created 24/7 network of contact for
high-tech
    crime and international Critical Information Infrastructure Protection (CCIP)
Directory.
    Subgroup has published its best practice documents and guidelines for assessment
of threats
    to computer and network security and has organized international training
conferences for
    cyber-crime agencies.

        Conclusion
        This paper gives a short overview of the term of cyber terrorism and
describes the
    most known cyber terrorist attacks. Taking in considerationthe fact that the
cyber terrorists
    are using smarter methods and tools to attack computer systems and government
institu-
    tions, and the main objective is to achieve their objectives; the national and
global security
    are subject to higher risk.
        The second part of the paper represents a response to the cyber security

challenges
    at national level and by various international organizations. NATO, for example, is a long-
    standing political and military organization, with extensive experience in the Þeld of cyber
    terrorism and cyber security.
            One of the limitations that occur during the acquisition of various cyber security
    measures is a balance to be made between security measures and civil liberties. There
    should be also a balance between the provision of speciÞc interests to a particular organiza-
    tion or government, and more general requirements for the beneÞt of all legitimate users
    to be formed an international communications and technological environment that will be
    unfriendly-orriented to the ambitions of cyber terrorists and extremists, cyber criminals
    and hackers.

70 CONTEMPORARY MACEDONIAN DEFENCE
♠INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

REFERENCES:

S. Best, DeÞning Terrorism:
http://www.drstevebest.org/Essays/DeÞning%20Terrorism.htm

www.symantec.com/avcenter/reference/cyberterrorism.pdf

M. Cereijo Cuba the threat II: Cyberterrorism and Cyberwar, 16 Maj 2006:
http://www.lanuevacuba.
  com/archivo/manuel-cereijo-110.htm

R. L. Dick, Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation,
  Before the House Energy and Commerce Committee, Oversight and Investigation Subcomittee
  Washington, DC, 05 April 2001,
http://www.fbi.gov/news/testimony/issue-of-intrusions-into-
  government-computer-networks

www.terror.net: How Modern Terrorism Uses the Internet, 21 February 2007:
http://www.asiantri-
  bune.com/index.php?q=node/4627

R. Lemos, Cyberterrorism: The real risk, 2002:
http://www.crime-research.org/library/Robert1.htm

D.Briere, P.Hurley, Wireless network hacks and mods for dummies, 2005, Wiley.

M. Bogdanoski, A. Risteski, & S. Pejoski, (2012, November). Steganalysis--A way
forward
   against cyber terrorism. In Telecommunications Forum (TELFOR), 2012 20th (pp. 681-
   684). IEEE.

A. Jahangiri, Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe
for
   Confusion: http://www.alijahangiri.org/publication/Cyberspace-Cyberterrorism-and-
   Information-Warfare-A-Perfect-Recipe-for-Confusion.htm

E. S. Othman, Hide and Seek: Embedding Audio into RGB 24-bit Color Image
Sporadically
   Using Linked List Concepts: IOSR Journal of Computer Engineering (IOSRJCE), Volume
4,
   Issue 1 (Sep-Oct. 2012), PP 37-44,
http://iosrjournals.org/iosr-jce/papers/Vol4-issue1/G0413744.
   pdf

E. Waak, The Global Reach of Privacy Invasion, Humanist, November/December 2002:

   http://www.thehumanist.org/humanist/articles/waakND02.htm

K. Curran&Others, Civil Liberties and Computer Monitoring, 2004:
http://www.jiti.com/v05/jiti.
   v5n1.029-038.pdf

B. Simons, , & E. H. Spafford, Inside Risks 153 , Communications of the ACM, 46(3),
March 2003

NATO Prague Summit Declaration Article 4(f), 21 November 2002:
http://www.nato.int/docu/
   pr/2002/p02-127e.htm.

NATO Communication and Information Systems Services Agency:
http://www.ncsa.nato.int/topics/
   combating_cyber_terrorism.htm

European Security and Defence Assembly, Cyber warfare (Assembly of the Western
European Union,
   Defence Committee Report C/2022.), 5 November 2008

NATO, Defence against cyber attacks, 26 June 2008:
http://www.nato.int/issues/cyber_defence/index.
   html.

NATO, Bucharest Summit Declaration, Art. 47, 3 April 2008:
http://www.nato.int/docu/pr/2008/p08-
  049e.html.

NATO, Defending against cyber attacks: what does this mean in practice?, 31 March
2008: http://
  www.nato.int/issues/cyber_defence/practice.html.

CONTEMPORARY MACEDONIAN DEFENCE
                  71
♠   INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL

          CCD-CoE, History and way ahead: http://www.ccdcoe.org/12.html
          CCD-CoE, Mission and Vision: http://www.ccdcoe.org/11.html
          UN General Assembly, The United Nations Global Counter-Terrorism
Strategy (A/Res/60/288, 20

          September 2006), paras 12(a), 12(b):
http://daccessdds.un.org/doc/UNDOC/GEN/N05/504/88/
          PDF/N0550488.pdf?OpenElement.
          The Use of Interent for Terrorist Purposed: United Nations OfÞce on
Drugs and Crime - Viena,
          (September 2012, p.vi),
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Ter-
          rorist_Purposes.pdf.
          ITU Global Cybersecurity Agenda (GCA, Framework for International
Cooperation in Cybersecurity),
          ITU 2007, http://www.ifap.ru/library/book169.pdf
          Curbing Cyberthreats - IMPACT:
http://www.itu.int/osg/csd/cybersecurity/gca/impact/index.html
          OECD, Guidelines for the Security of Information Systems and Networks:
Toward a Cul-
          ture of Security (Paris: OECD, 25 July, 2002):
http://www.oecd.org/document/42/0,3343,
          en_2649_34255_15582250_1_1_1_1,00.html
          OECD Resources on Policy Issues Related to Internet Governance:
http://www.oecd.org/document/2
          1/0,3343,en_21571361_34590630_34591253_1_1_1_1,00.html
          OECD Working Part on Information Security and Privacy:
http://www.oecd.org/document/46/0,3343,
          en_2649_34255_36862382_1_1_1_1,00.html
          OSCE Ministerial Council Decision 3/04: Combating the Use of the
Internet for Terrorist Purposes, 7
          December 2004: http://www.osce.org/documents/mcs/2004/12/3906_en.pdf
          OSCE Ministerial Council Decision 7/06: Countering the Use of the
Internet for Terrorist Purposes, 5
          December 2006: http://www.osce.org/documents/mcs/2006/12/22559_en.pdf
          OSCE Permanent Council: http://www.osce.org/pc/

OSCE Permanent Council, OSCE can play important role in cyber security, says Estonian defence
Minister, Vienna, 4 June 2008:
http://www.osce.org/pc/item_1_31483.htm
OSCE Forum for Security Co-operation: http://www.osce.org/fsc/
OSCE FSC/PC 36th Joint Meeting, FSC Decision No. 10/08, OSCE Workshop on a Comprehensive
OSCE Approach to Enhancing Cyber Security, 29th October 2008:
http://www.osce.org/fsc/
OSCE, OSCE ofÞce organises discussion in Yerevan on cyber security threats, 21 March 2006: http://
www.osce.org/item/18450.html
Council of Europe Convention on Cybercrime: http://www.i-policy.org/2010/06/council-of-europe-
convention-on-cybercrime.html
Council of Europe Convention on Cybercrime: http://conventions.coe.int/treaty/Commun/ChercheSig.
asp?NT=185&CM=8&DF=&CL=ENG
Council of Europe, Global reach of the Council of Europe Convention on Cybercrime: http://www.coe.
int/t/dc/Þles/themes/cybercrime/WorldMapCybercrime_E_2008_10_06.pdf
Meeting of G8 Justice and Home Affairs Ministers, G8 Sea Island Summit, 11 May 2004: http://www.
usdoj.gov/criminal/cybercrime/g82004/g8_background.html
Cyber Security Organization Catalog, Group of Eight (G8): http://www.cistp.gatech.edu/catalog/one-
Org.php?id=3

72 CONTEMPORARY MACEDONIAN DEFENCE
DarthVader@umich.edu
skywalker@indiana.edu
princess.leia@iupui.edu
Ewok@iupui.edu
C-3PO@vt.edu
stormtrooper@uct.vw.com
♠