HAIFA UNIVERSITY B.A. HONORS
PROGRAM

CYBERTERRORIST'S MANUAL FOR THE INTERNET

A REASERCH PAPER SUBMITTED TO :

INBAR FOUNDATION
Centre for Special Studies

BY :

Robert Kohn
I.D. 016024465

December , 29th 1996.

TABLE OF CONTENTS

Introduction[*]

At first it was only one of the minor projects of the United State's Defense Advanced Research Projects Agency (DARPA) then an ad hoc network connecting universities . Suddenly , in 1995 it became , in US Vice President Al Gore's words , a revolution[1] .

Every revolution has its protagonists and Cassandras ; the **Internet** Revolution is no exception to this rule . The former see it as a panacea for all ills and difficulties of the late twentieth century . The latter herald the advent of an anti - utopia , a brave new world in which **cybercriminals** and **cyberterrorists** roam , using the **Net** as their platform .

The danger is clear and present , nevertheless , it is mostly discussed by journalists , scholarly attention being seldom lavished on it . The danger assessments of scholars and journalists alike are developing along two distinct lines . The first , mostly discussed by the newspeople , warns about the existence of on-line bomb recipes on the **Net** enabling anyone to duplicate the most spectacular *coups* of the " Second Wave " terrorists . Articles of the " bomb recipe " paradigm appeared in newspapers as diverse as the *USA Today*[2] and the Hungarian *Magyar Hirlap*[3] . The

[*] The paper was written during my freshman year of my BA in 1995.

[1] Al Gore , " The Information Superhighway : What it Will Mean , " in The World Almanac and Book of Facts 1995 , ed. Robert Famighetti (New Jersey : World Almanac , 1995) , pp. 35-36.

[2] Bruce Frankel and Gary Fields , " New Teen Fad : Building Bombs , " USA Today , 5 June 1996.

[3] " Netszerver , itt keresik az esztergomi bomba keszitojet , " Magyar Hirlap (Budapest) , 27 August 1996 .

second thread is that of the **information warfare** , which , being inspired by the " hacking industry " and computer viruses , deals with the use of computer technology , mostly softwares , as a means of destruction . As examples for the " **information warfare** " paradigm we should mention Matthew G. Devost's presentation at the *Second International Conference on Information Warfare*[4] , and Barry C. Collin's remarks at the *11th Annual International Symposium on Criminal Justice Issues*[5].

The above mentioned sources are valuable as " warning shots " , however , they deal only with a very narrow aspect of a much broader spectrum . The only attempt to give a broader perspective on **cyberterrorism** was the testimony of Jerry Bermann , of the Center for Democracy and Technology before the US Senate Subcommittee on Terrorism , Technology and Government Information[6].

The purpose of my paper is to demonstrate that a revolution in the modus operandi of the terrorists is to be expected , in every domain of their activity , due to the proliferation of their " war " into the **cyberspace** . Our argument rests on Clausewitz's maxim elaborated by Heidi and Alvin Toffler that each age is characterized by its dominant warform and that the " modes of destruction " of a given age reflect its " modes of production "[7] .

In order to achieve a practical demonstration , the operational *repertoire* of the terrorist will be presented in its entirety , every domain being tackled through a

[4] Matthew G.Devost , " Political Aspects of Class III Information Warfare : Global Conflict and Terrorism , " Second International Conference on Information Warfare (Montreal : 18 - 19 January 1995) , http://us.okbmei.msk.su:80/FAQ/InfoWars/montreal.html

[5] Barry C. Collin , " The Future of CyberTerrorism , " 11th Annual International Symposium on Criminal Justice Issues , http://www.acsp.uia.edu:80/OICJ/CONFS/terror02.htm

[6] Jerry Berman , Testimony of Jerry Berman , Executive Director Center for Democracy and Technology Before the Senate Judiciary Committee / Subcommittee on Terrorism , Technology and Government Information (SL : 11 May 1995) , http://www.cdt.org:80/policy/terrorism/internet_bomb.test.html

[7] Heidi and Alvin Toffler , War and Anti - War , (London : Warner Books , 1994) , pp. 104 -105.

contrasting of the present state of the art with the potential , **Internet** facilitated developments .

Chapter One tackles the “ off the shelf “ information and technologies readily available in the cyberspace . Chapter Two concentrates on information and technologies not yet available but entirely feasible judged by the present trends . Chapter Three presents some modi operandi for dealing with the menace .

Because of the technical nature of the subject a few methodological remarks are indispensable .

Since most of our sources are electronic the majority of the footnotes will be given as **addresses** (**e-mail** or **Internet**) and **filenames** . Due to the unpredictable lifespan of the sites we recommend the use of **address** , **FTP** and **search engine** (in this order) for referencing . The files referred to are available *ad acta* and gladly sent on request . For the convenience of the readers without a background in computer networks , intelligence and military a short glossary will be included . The definition of the term **terrorism** is omitted due to the “ intractable problem of the definition “ . For an in depth definition of he term we recomend Conor Gearty’s 1996 published treatise[8] .

[8] Conor Gearty , ed. Terrorism (Sydney : Dartmouth , 1996) , pp. xi - xxiv .

Chapter One : The cyberterrorist's arsenal - off the shelf information and technologies available on the Net

As we already mentioned , the purpose of this chapter is to investigate how existing information and technologies on the **Internet** can be applied to the operational repertoire of the terrorist .

With all the practical complexities , the operation of every terrorist organization can be divided in five broad categories . The first is characterized by the crystallization of the ideology and recruitment of the cadre . The second is that of the build up of the force consisting of indoctrination , training and obtaining the resources . The third is that of the intelligence and counterintelligence . The fourth is that of the operations . The fifth , propaganda .

Arguably this taxonomy is an arbitrary one , in practice there are no clear lines of demarcation between the various categories . Nevertheless we will use it , for the sake of simplicity , as an analytical tool .

Beginings : Making of an ideology - Recruitment of cadre

Leading fiction writers of our grossly materialistic Second Wave , paradoxically enough , focused much of their attention on the relationship between the emerging urban terrorism and the proliferating militant ideologies . Dostoyevsky's *Devils* and Joseph Conrad's *Secret Agent* were the trend setters in this domain . However , it took another half a century until Albert Camus , in his 1954 essay , *The Rebel* established the true relationship between the urban guerrilla and his/her ideology :

" There are crimes of passion and crimes of logic . The boundary between them is not clearly defined . We are living in an era of premeditation and perfect crime . Our criminals are no longer helpless children who could plead love as their excuse . On the contrary , they are adults and they have a perfect alibi : philosophy "[9].

Ideologies , either imported or endemic , were always considered necessary by organizers and prospective leaders of terrorist groups . The spreading of the ideologies until the recent times was done in fairly *gemeinschaftliche* ways . Close knitted students circles , family ties and even romantic relationships transmitted the ideology and recruited new members to the ranks of the " freedom fighters " . As late as the last decades of the twentieth century , handwritten proclamations , like those of the intifada and the Eastern European *samizdats* augmented this informal system . In sum , personal contact was considered a prerequisite for " winning hearts and minds " .

The **Internet** can change all this .

[9] Albet Camus , The Rebel , quted in Phillip Robertson , A Short Essay on the Transmission of Ideas , http://fileroom.aaup.uic.edu:80/RSG/pform40unabomb.html

Old methods can be very much refined if know-how accumulated by intelligence agencies is made available through the information superhighway . Besides

" civilian " techniques such as Dale - Carnegie's and Thomas Wang's , there is a plethora of de jure or de facto declassified material available[10] . The best example is the CIA's *Psychological Operations in Guerrilla Warfare* manual , originally published in Spanish for the use of the contras in Nicaragua[11] .

But this is only the tip of the ice berg .

The tools of tomorrow for spreading militant ideologies on the **Net** are the **newsgroups** , the **Internet Relay Chat** and the teleconferencing . Basically all these tools enable peoples living in distant places to come together and share ideas . Whatever the mode of communication : written messages , write-chat conferences or real time two way video conferencing the meaning is the same . The propagandist can reach large target populations , try out " pilot-ideologies " , identify the potential cadres and recruit them . The flexibility of creating closed sub-groups or **face2face** makes the screening and the compartmentalization very easy . However , the greatest bonus is security . The very mass of data passing through the **information superhighway** makes interception virtually impossible . Operational security can be enhanced by simple switching of **servers** , **usernames** ecc .

Newsgroups like alt.anarchy , alt.discordia and others are the most likely points of departure for such attempts .

All this , however , is not somewhere in the distant future . According to Mike Mokrzycki , preaching of the Holy War by Algerian extremists , Holocaust denial by

[10] Thomas Wong , American Communication Training (Campbell : TransCore Strategies , 1996) , http://www.transcore.com

[11] CIA , Psychological Operations in Guerrilla Warfare , http://entisoft.earthlink.net:80/psyops.htm

neo-nazis are as a common phenomena on the **Net** as the advocating by some activists to kill abortion providers[12] . As for on line recruitment of cadres , Kurt Saxons U.S. Militia with its on line founding charter and admission forms is just one of the many[13] .

As we have seen , it does not take more than a few hours on the **Net** for the prospective **cyberterrorist** to find the like minded people able and willing to act . The build up of the force can already be started .

Build up of the force : Indoctrination - Training - Resources

The distinguishing between the phases of recruitment at one hand and indoctrination at the other is a purely analytical one . Practically both exist in a dialectical interdependence . Initial indoctrination is a prerequisite of the successful recruitment , which in its turn will be followed by more indoctrination .

Classical means of indoctrination like group discussions , mass meetings and internal propaganda can be greatly enhanced by the resources of the **Internet** . Easy access to on line news agencies , **electronic journals** and libraries make the provision of the propaganda material much easier than in the past . A further advantage of using on line resources is in the preserving of the anonymity of the " researcher " . Instead of the tell - tale library cards with long lists of compromising titles , the use of electronic databases promises total anonymity if the open terminals of public libraries or the **cybercafe** facilities are used .

[12] Mike Mokrzycki , " Battleground of Bits and Bytes , " The Jerusalem Post , 19 April 1995 , p. 5.
[13] Kurt Saxon , U.S. Militia , http://www.ipser.com:80/usmilitia/

Classical means of indoctrination will be soon overshadowed by the new ones provided by the **information superhighway** . Instead of the real , and potentially dangerous meetings and group discussions , teleconferencing sessions can be held encompassing people from every continent . The participants can be presented with all the audio - visual material available at a conventional meeting .

This leads us to the **multimedia** packages . Instead of the handwritten or stenciled underground papers of the past , multimedia packages will be sent to the recruits . Moreover , the individually sent packages can be tailored to the personality of the recruit , leading to further enhancement of the propaganda effect .

Another powerful tool of indoctrination is the use of the customized news services . Leading news service providers offer customization services for those with a special interests in certain domains , regions ecc. However , the main danger of customization is its presenting of a distorted or biased picture of the reality . Basically the same practice was/is followed by the press organs of totalitarian dictatorships . Today , anybody with an access to the " custom " option of providers such as NEWSSTAND or AJR/Newslinks can duplicate Big Brother's game[14] . Daily news customized by the group's propagandist and **e - mailed** to members can be especially useful for the " political education " of the recruits . The brainwashing effect is especially devastating on persons deprived of other sources of information .

Training of the force in the military and conspirational skills of a terrorist force can be a torturous process . The solution of the past was to use the services of ex-military or intelligence personnel and/or " advisors " of friendly organizations or states . The **Internet** can make the obtaining of the know - how much more simple .

[14] ARJ/newslink , http://www.newslinkorg:80

There is a plethora of information available on the Net and the main problem may be the selection the authentic information out off the chaff . As always , the best source is the military . There is a good collection of , supposedly declassified , U.S. Army Field Manuals available on the Net . Titles range from *M249 Light Machine Gun in the Automatic Rifle Role* (FM 23 - 14)[15] to *Light Antiarmor Weapons* (FM 23 -25)[16] . Information on Survival and patrolling skills , first aid , marksmanship is available from similar sources . **Homepages** of security agencies , special forces and U.S. Army units offer valuable information . Then , translating of the know - how into practice is a matter of political will and , of course , resources .

Resources , in the opinion of Montecuccoli , is a simple matter . His maxim of " money , money and money " as the three necessary resources of waging wars is still widely cited today . The **cyberterrorist** , in order to launch her/his war will need it to.

The classical way of obtaining money for the financing of the revolution was

bank robbing , racketeering and kidnapping . The fad of the days is narco - terrorism . **Internet** can revolutionize this field too .

To begin with there is a legion of useful advices on credit card fraud , ATM machine fraud and counterfeiting on the **Net** . Jolly Roger's *Anarchy Cookbook v.666**

will teach the prospective terrorist how to do it .The same source teaches us how to pick locks and how to grow marijuana[17] . The former is such a popular topics that we have a whole discussion group dealing with it and assuring the blooming of the

[15] U.S. Army , FM 23 - 14 : M249 Light Machine Gun in the Automatic Rifle Role , (SL : U.S. Army , 1994) , http://155.217.020.55/atdl/docs/fm/23-14/fm2314.htm

[16] U.S. Army , FM 23 - 25 : Light Antiarmor Weapons , (SL : U.S. Army , 1994) , http://155.217.020.55/atdl/docs/fm/23-25/fm2325.htm

[17] Jolly Roger , Anarchy Cookbbok v.666* , http://www.cyberbeach.net:80/~mbabcock/HPA/JollyRoger

trade[18] . The later leads us back to the narco - terrorism . The popular MCW Homepage gives us three recipes how to make LSD (besides other useful tips to be discussed later)[19] .

But this is only small change . Electronic burglary and bank robbing is another *bona vaca* already making headlines thanks to the efforts of the hacker community . The **Net** opened a whole new dimension for money laundering too , and fund transfers from far away sponsors can be done in with relative ease .

Intelligence : Defensive - Offensive - Tradecraft

Defensive intelligence is a vital need for the new **cyberterrorists** from the first step in the trade . Field security , information denial , screening of the cadre ecc. measures are to be taken in order to avoid detection by the police and intelligence agencies . Once the tradecraft was learnt by trial and error , from friendly organizations or from such classics as Marghiella's *Mini - Manual for the Urban Guerrilla* . Today the **Net** offers its assistance in three domains of the art and science of the intelligence ..

The first domain to be considered is the know - how . The *NSA Employee's Security Manual* provides useful information on what the law - enforcement agencies are looking for and some tips about information denial[20] . A more useful source is the *Ten Spy - Busting Secrets* compiled by a certified protection professional and fraud

[18] alt.lockpicking

[19] SA , " LSD Recipes # 1 - 3 , " The MCW Digest , http://www.xmission.com:80/~seer/mcw/lsd.html

[20] NSA , NSA Employee's Security Manual , http://www.tscm.com:80/NSAsemanual1.htm

examiner Kevin D. Murray . It gives the basics on how information denial , eaves - dropping detection and most important for the **cyberterrorist** - computer security[21] .

The second domain is background investigation of the recruits in order to enable the group to fend off infiltration attempts by the dreaded *agent provocateur* .

Offensive intelligence in the form of gathering , evaluation and research has to be conducted in order to select targets , prepare operations in the domain of operations proper and fund rising activity (bank robbing , burglary) . The importance of the intelligence was stressed by Marighella and victims of terrorist incidents often report on surveillance teams observed prior to the attack . The most widely publicized case is the kidnapping of Sir Geoffrey Jackson , which was committed only after meticulous intelligence gathering mainly in form of physical surveillance[22] . Here , as in the case of the defensive intelligence , the use of on line data - bases and other resources is important for intelligence gathering , even if **HUMINT** , quantitatively , is more significant for terrorists than for the nation - states .

Intelligence tradecraft , according to William Hood is " a compound of commonsense , experience and certain universally accepted ... practices "[23] . Operational methods and **SOP**s are among the most jealously guarded secrets of the intelligence agencies . Surprisingly enough the **Net** is jammed with information on certain domains of the trade and virtually silent on others .

The plethora of information on eavesdropping and surreptitious entry is such that the on line manuals have their files compressed in order to make them conveniently transferable . The above mentioned *Anarchy Cookbook v 666** ,

[21] Kevin D.Murray , Ten Spy - Busting Secrets , http://www.tscm.com:80/murray/html
[22] Anthony J. Scotti , Executive Safety and International Terrorism (New Jersey : Prentice Hall , 1986) , pp. 42-43.
[23] William Hood , Mole (London : W.W. Norton & Company , 1982) , p.14.

Hobbit's *Simplex Lock In - Depth Evaluation* and David Richards' *The Big Book of Mischief* are just a few of the available sources[24] .

On the other hand **SOP**s on physical surveillance , **safe houses** , **dead - letter boxes** are difficult to find and the existent material is mostly chaff .

The third , and perhaps most important domain is that of secure communications through encryption software available on the **Net** . Secure communications are vital as a means of information denial to the enemy , being it a hostile nation or police agency . Cipher books were mostly replaced in the cloak and dagger arsenal of the nation - states by modern machines , descendants of the Third Reich's famous **Enigma** .Today's small sized secure communication systems using frequency hopping , burst transmissions ecc. are used by the armed forces of the nations but are generally denied to non - state actors because of secrecy and price . Big Brother is keeping the cards close to his chest .

With the explosive proliferation of the personal computers and the advent of the **Internet** this state monopoly is diminishing . **Shareware** / **freeware** encryption softwares are making their debut on the Net , with the most famous of them all P.R. Zimmerman's **PGP**[25] . The best indication for the efficiency of this and other encryption softwares is the panicky reaction of certain security officials demanding state access to the keys and subordinating their export to regulations concerning lethal military *materiel* . Their main argument is that a lap-top computer with a cellular phone link to the **Internet** can provide the cyberterrorists a means of mobile secure communication on par with the most advanced Army equipment .

[24] Hobbit , Simplex 5-button Combination Locks:*Hobbit*'s in - depth evaluation , http://www.cyberus.ca:80/~sgi/locks.txt

[25] Phillip R. Zimmerman , The Official PGP User's Guide , http://web.mit.edu/network/pgp.html

Operations - Soft and Hard

Operations , soft and hard , are what is considered " terrorism proper " , more precisely the most visible , even spectacular , part of the urban guerrilla's activity . The terms soft and hard are used instead of the more conventional lethal/non - lethal dichotomy . The problem with the later is that even a non-lethal weapon like a computer virus if deployed against an air liner's on board computer can lead to hundreds of fatalities . In our usage " hard terrorism " is used for measures aimed at the physical neutralization of the target , " soft terrorism " being a denominator of the " indirect approach " .

Kidnapping , bombing , assassination and paramilitary operations (raids , ambushes ecc.) form the operational *repertoire* of the " hard terrorism " . They are the very *raison d'etre* of the indoctrination , training and intelligence efforts made by the urban guerrilla to further his/her political goals . Having covered the ways in which the **Internet** revolutionizes the above mentioned domains we should now turn to the field of logistics , namely the providing of the tools of trade .

On line bomb making recipes are the long time favorites of journalists . Manuals as Jolly Roger's *Cookbook* , Richards' *Big Book of Mischief ,* the Unknown Author's *Terrorist's Handbook*[26] and BHU's *Pyrotechnics Cookbook v1.0*[27] are the most notorious publications . These manuals contain all the nuts and bolts of the trade from specialty fuses to advanced explosives to delivery systems . It is worthwhile

[26] Unknown Author , The Terrorist's Handbook , http://www.et.tudelft.nl:80/~koerkamp/tthb/

[27] BHU , Pyrotechnics Cookbook v1.0 , http://eran.db.eran.edu:80/~sarmowsp/FILES/anarcook.txt

mentioning that despite the " for entertainment only " labels , these are basically " how to do " manuals with detailed practical information . More on line information can be obtained on discussion groups concentrating on pyrotechnics and hobby rocketry[28] .

However , it is generally overlooked that most of this information was long ago available in print , some , like the *OSS Sabotage Manual* laying on the shelves of public libraries for more than fifty years . The innovation is mainly in the ease and anonymity of access .

Improvised firearms are described in the same sources in a much more laconic way . Apparently the ease of obtaining firearms in the U.S. makes improvisation a no - issue . Much is said on the **Net** on improvised suppressers (silencers) , alas , from the point of view of the prospective cyberterrorist , mostly chaff . On the other hand , the recent revitalization of the crossbow by the elite forces was not missed by the on line armourers . The already mentioned prolific author , Kurt Saxon of *Weaponeer* fame provides us with detailed blueprints of conventional and even more exotic , repetition crossbows similar to those used long ago in the Far East[29] .

The line is closed by a long list of specialty bullets and projectiles of every imaginable kind , mostly garage designed replicas of special ammunitions used by secret services and elite units . Explosive and poisoned bullets , armor piercing and Teflon coated "cop killers " are described in the above cited sources , together with " special ammunitions " for slingshots , blowguns and wristrockets .

[28] rec.pyrotechnics

[29] Kurt Saxon , Repeating Crossbow , http://www.ipser.com:80/xbow/plan01

It should be mentioned that similar , and more authoritative , information can be obtained from the firearm oriented sites on the **Internet** , a plethora of which exists , some of them under the aegis of the American firearms industry[30] .

The recent interest in non - lethal weapons systems and information warfare led to the coining of the buzz - word : " soft terrorism ". As a matter of fact there is nothing new about the idea of the " soft kill " , sabotage operations of the past were very much in the same category . Two main categories of " soft terrorism " will be considered . The first , sabotage by physical means . The second , information warfare .

As already mentioned , sabotage is an age old art targeting hardware instead of personnel . Today's **cyberterrorists** have inexhaustible resources of know - how about sabotage in the pranksters discussion groups , data bases and " revenge manuals " . Some of the advices are unrealistic , some outright childish . Nevertheless , at least part of the data is useful in creating havoc . Ian Knowles' *New Job* , for instance , describes highly efficient ways of sabotaging office machinery such as fax machines , phones and photocopiers[31] . The Last Viking's specialty is sabotaging computers[32] . Still others vandalize ATM machines and other bank facilities .

While most of these sound rather funny , they have a great potential of disrupting normal life and are less likely to provoke draconian countermeasures by the state , than bombings or assassinations .

The plethora of technical information on the **Internet** makes it rather simple to obtain blueprints and/or descriptions of machinery , power lines , industrial processes ecc. all targets of choice for saboteurs .

[30] American Firearms Industry Home Page , http://www.amfire.com:80

[31] Ian Knowless , New Job , alt.revenge

[32] Last Viking , Disk Drive Killer , alt.revenge

Discussing the art and science of information warfare is beyond the scope of our paper . It is enough to mention that it was realized long ago by futurologists , journalists and military thinkers that with our growing dependence on computers and networks , a new dimension of warfare is developing . Much publicized penetrations by hackers into classified data bases , criminal cases of employee revenge and blackmail makes the information warfare an issue of today rather than of the future . Terrorists , instead of blowing up a major financial , political or military center may decide to sabotage their computers by soft means . The disruption caused will be highly similar . Tactics and tools of the information warfare are numerous ; appendix 2 provides a short typology .

Propaganda

Terrorist activity , as any other warform , is not a goal in itself . It is only a means of achieving political goals . The propaganda is the link between the two , translating actions into political dividends .

Terrorist's propaganda is very much dependent on the existence of a relatively free media as a platform of its activity . Governments , by resorting to such measures as overt and covert censorship , disinformation and " media management " were able , until now , to disrupt the terrorist's propaganda .

The old means of the past : pamphlets , underground papers , placards are still with us , but the **cyberterrorist** will soon adapt their electronic equivalents . Despite the restrictory measures of some states , for example : China ,Vietnam and - Germany , the **Net** is and hopefully will remain the realm of free speech . As such , it is / will be used by the **cyberterrorist** to circumvent government imposed news moratoria and other restrictive measures .

Electronic pamphlets can be distributed by mailing lists or by the means of computer viruses . **Cyberjournals** can be located in the servers of far away countries , even continents . But the greatest promise of them all is the real-time , on line news coverage .

The camera totting Hizbullah fighter will be replaced by terrorists armed with video cameras and cellular linked lap top computers capable to transmit the scoops of their own deeds directly to the major news networks of the world . The messages can be camouflaged by using the latest encryption technologies paralyzing state censorship.

With the successful propaganda the **cyberterrorist** closed a full circle . The process started with spreading the ideological seeds , followed by recruitment and the build up of the force . After intelligence and operational activity the results were fed into the propaganda machine bolstering the ideology and making the process self - sustaining .

And as we have demonstrated , in every phase the use of the resources and facilities of the **Net** proved to be a force - multiplier . The question , thus , is unavoidable : are there any limits ?

Chapter Two : Arsenal of Future - Information and Technologies not yet Available

Judged by the sheer mass of the information available on the **Internet** and its explosive development it is difficult to ponder about “ limits of the growth “ theories .

One can hardly escape the feeling that the Net is one giant oracle , able to provide any information if one knows how to ask . Nevertheless , at least from the perspective of the **cyberterrorist** there are still huge blind spots .

Weapons of Mass Destruction

The lyrics of Wilfred Owen , the terrible sights of Ypres and Kurdistan and the remembrance of Enola Gay may lead us to the conclusion that weapons of mass destruction are an invention of the twentieth century’s *anomie* . However , military historians are telling us that from the ancient times chemical and biological weapons were used in great frequency . Greek fire , smoke and catapulting of corpses into besieged cities are only few of the most often encountered “ weapons systems “ .

With the advent of the nation - state , their use become its monopoly , broken only by the 1995 Tokyo nerve gas attack committed by the followers of Shoko

Asahara . Today's terrorists intending to arm themselves with doomsday machines have three main weapons systems to choose off . Chemical weapons are the easiest to build , preparation of agents as Sarin is well within the capabilities of a chemist and the ingredients are commercially available . Biological weapons can be obtained from laboratories , however their effect is even more unpredictable than that of the chemical ones . Nuclear weapons of the radiological type can be built from material available on the black market , whereas fission and/or fusion weapons are " very difficult for a terrorist group to make , steal or buy "[33] .

The **cyberterrorist** , trying to obtain know - how from the **Net** will find preciously little . MCW Digest offers us information on U.S. Army standard operation proceedings of sending biowar agents through mail or Federal Express and even cites a case when " a package containing a deadly virus known as Crimea - Congo " was lost . The article even gives a description of the canisters , facilitating their recognition and interception[34] .

As for the field of the chemical warfare , the same source teaches us how to make sarin (the agent used in the Tokyo gas attack), and the above cited bomb manuals (e.g. The Terrorist's Handbook) usually have a chapter or two on lacrimogenes (tear gas)[35] .

Practical information on nuclear weapons is not to be found on the Net , sites tackling the topic contain no more information than any popular science publication . One of the most widely publicized sites is a rather harmless , purely descriptory one[36]

.

[33] Bruce W. Nelan et al. , " The Price of Fanaticism , " Time , 3 April 1995.

[34] SA , " BioWar by Mail , " The MCW Digest , http://www.xmission.com:80/~seer/mcw/biowar.html

[35] Unknown Author , The Terrorist's Handbook , http://www.et.tudeleft.nl:80/~koerkamp/tthb/

[36] Outlaw Labs. , Documentations and Diagrams of the Atomic Bomb , http://www.nada.kth.se/~nv91-asa/atomic.html

In sum , in the realm of weapons of mass destruction the Net offers no more information than any good municipal library . However , such information can be made available at any given moment by hackers breaking into classified databases , rouge scientists or as a form of employee revenge . The penetration of Israeli hackers into the French Ministry of Defense's computers and the posting of top secret U.K. government documents by the Texas University server are only showing the trend[37] .

Real time satellite imagery

Good maps are rather abundant on the **Net** , from free and commercial **websites** alike . Even satellite imagery was made available by the **USGS**[38] . Here for a nominal fee everybody can get a glimpse from high above of her/his house , neighborhood or a top secret installation from another continent . Overhead imagery can be of great help for terrorists planning attacks against installations with good perimetral camouflage such as military bases , secret research facilities and high security penitentiaries .

[37] SA , " Texas University Posts Top Secret UK Govt Info on Web , " Newsbytes , 25 March 1996.

[38] USGS , http://edcwww.cv.usgs.gov:80/dclass/dclass.html

However , due to security considerations and technological constrains , real time satellite imagery is not yet available on the **Net** . With the increasing commercialization of the space industry , it is perfectly possible that commercial

observation satellites of the future will supply real time overhead imagery for such diverse uses as traffic control , forest fire watching . irrigation control ecc. From this , it is only a short step to the cellular linked , lap top armed terrorist following the route of a top secret motorcade in live broadcast and preparing for his/her raid .

Safe money transfer

It should sound weird that such a profane act as money transfer may have a bearing on the " revolution " but the fact is that safe transfer of money through the **Net** is a problem not solved yet . Despite the various methods used , such as code words coupled to the credit card numbers , encryption and alike , no convenient method has won general acceptance .

For the **cyberterrorist** , removing this technological / organizational constrain can revolutionize the unholy business of extortion , racketeering and their like . By this newly gained flexibility terrorist will be able to receive ransoms , run narco - terrorist enterprises ecc. without the fear that their money translated into bits may disappear because of some hacker turned **cybercriminal** is lurking in the shadows of the **cyberspace** .

Chapter Three : Counterterrorism in the Cyberspace

Counterterrorism as opposed to antiterrorism is trying to deal with the terrorist before it strikes and it is the weakest seam in the nation - state's armor . Predicting the *foci* of development , target populations and operational plans of the terrorist menace is a difficult task , especially in the liberal democratic state . Today we are in a rare position of seeing the emergence of a new battleground of terrorist warfare , the **Internet** , a development which will change the outlook of terrorism as a whole . Thus , it is imperative to gain the initiative in this new and most important domain and prepare our defenses before " the hydra of carnage " strikes .

Promotion of the freedom of speech and free exchange of ideas is the very *raison d'etre* of the Net . Thus , restrictory practices , such as those of the German , Chinese and other governments should be considered only as a last ditch defense . So instead of killing of the patient together with the bacteria a more careful approach is to be made .

The first step should be the identification of those informations and technologies which can facilitate terrorist activities . No clear-cut definition is possible , since the Net is like the television camera in Major - General Richard Clutterbuck's words " a weapon lying in the street . Either side can pick it up and use it ."[39] We nevertheless attempted in chapter one to highlight some of the sources of danger . Anarchists' ,

militia's , pranksters' and political extremists' discussion groups and sites , on line " how to " manuals are among the most visible *foci* of the organizing activities . These sites should be monitored by search engines looking for specific words , phrases and names and the results evaluated by human analysts . However , due to the sheer mass of new material surfacing every day on the Net , this task could be Sisyphean .

The second step may be a more in depth treatment as compared to the horizontal sweep of the former . False flag and/or *agent provocateur* operations , nothwithstanding with the moral questions they rise , should be used to identify the die hards of the target population , those who are ready to rally under any flag . This net can capture some of the **cyberterrorist** organizers in search of business - partners and allies .

The third step should be that of psychological warfare . The capture of those involved in organizing terrorist groups and activities on the Net should be given maximal publicity . Accounts of the efficiency of the screening methods should be exaggerated . This way an impression will be given to prospective **cyberterrorists** that the first step into the *terra incognita* may be the last in the trade , due to prompt disclosure .

The fourth step should be done in close cooperation with the **server** managers

.

Servers should impose age verification , as in the case of pornographic materials , in order to avoid children's access to the " how to manuals " . Frankel and Fields from

[39] Maj. - Gen. Richard Clutterbuck , Living with Terrorism (London : Faber , 1975) , p. 147 , quoted in Philip Schlessinger , " Terrorism , the Media , and the Liberal - Democratic State : A Critique of Orthodoxy , " Social Research , 48 (Spring 1981) , p. 82.

the *USA Today* report on a " New teen fad : Building bombs " and recall several accidents leading to death and injury . The wide publicity given to the Oklahoma City bombing , the Unabomber saga and the ease of obtaining know - how from the **Internet** proves to be a deadly combination . Although this syndrome is not directly connected to cyberterrorism , it can be seen as a phenomena adumbrating it[40] .

[40] Bruce Frankel and Gary Fields , " New Teen Fad : Building Bombs , " USA Today , 5 June 1996.

Conclusion

The purpose of this paper was to demonstrate that due to the advent of the **Internet** , and in the midst of all the changes it is introducing into our lives , the face of terrorism is undergoing a metamorphosis not less significant .

Our point of departure was the presentation of information and technologies already available on the Net , ready to be exploited by the emerging **cyberterrorist** . A short glimpse was given to the future of the **cyberterrorism** in the form of technologies under development and emerging know - how . The closing chapter was devoted to the question of counterterrorism proposing a four step approach to the problem .

These and other modi operandi are necessary to prepare ourselves for the onslaught of the **cyberterrorism** . Perhaps seen by many as an infringement of the right to free speech , these steps are necessary in our opinion to preserve it . Governments should be given this alternative otherwise sooner or latter they will resort to censorship and other restricting practices . The **cyberterrorist** will be defeated , but in this Pyrrhic victory , the freedom of speech and the **Internet** will be the first causalities .

Bibliography

BOOKS

Hebrew :

Harkabi , Yehoshafat . Milhama veEstrategia [War and Strategy] . Zahal : Hozaat " Maarachot " / Misrad haBitachon - hozaa laOr , 1990.

English :

Chomsky , Noam and Herman , Edward . The Political Economy of Human Rights . Nottingham : Spokesman Books , 1979.

Clutterbuck , Richard . Living with Terrorism . London : Faber , 1977.

Conrad , Joseph . Secret Agent . New York : Penguin , 1994.

Davis , Angela . An Autobiography . New York : Random House , 1974.

Dostoevsky , Fedor Mikhailovich . The Devils (The Possessed) . Harmondsworth : Pengiun , 1969.

Foley , Charles (ed.) . The Memoirs of General Grivas . London : Longmans , Green and Co. , 1964.

Gearty , Conor , ed. Terrorism . Sydney : Darthmouth , 1996.

Gore , Al . " The Information Superhighway : What it Will Mean . " In The World Almanac and Book of Facts 1995 , pp. 35 - 36. Edited by Robert Famighetti . New Jersey : World Almanac , 1995.

Guevara , Ernesto Che . Venceremos ! . London : Weidenfeld and Nicolson , 1968.

Bolivian Diary . London : Villiers Publications Ltd. , 1968.

Hood , William . Mole . London : W.W. Norton & Company , 1982.

Israeli , Raphael . PLO in Lebanon : Selected Documents . London : Weidenfeld and Nicolson , 1983.

Johnson , Paul . A History of the Modern World . London : Weidenfeld and Nicolson , 1983.

Khaled , Leila . My People Shall Live . London : Hodder and Stoughton , 1973.

Klare , M.T. and Kornbluh , P. (eds.) . Low Intensity Warfare . New York : Pantheon Books , 1988.

Klein , Hans Joachim . The German Guerrilla . Cienfuegos Press & Soil of Liberty , 1978.

Laqueur , Walter and Alexander Yonah . The Terrorism Reader . Ontario : Nal
Penguin Inc. , 1978.

Laqueur , Walter . The Guerrilla Reader . New York : NAL Books , 1977.

MacStiofain , Sean . Revolutionary in Ireland . Edinburgh : R. & R. Clark Ltd. , 1975.

Mao Zedong . Selected Works of Mao Tse - Tung . Peking : Foreign Languages Press , 1967 .

NorthWestNet. The Internet Passport . New Jersey : Prentice Hall PTR , 1995.

Paletz , D.L. and Schmid , A.P. (eds.) . Terrorism and the Media . London : SALE , 1992.

Ra’anan et al. (eds.) . Hydra of Carnage . Toronto : Lexington Books , 1986.

Rapoport , D.C. (ed.) . Inside Terrorist Organizations . London : Frank Cass & Co. Ltd. , 1988.

Seale , Patrick . Abu Nidal : A Gun for Hire . New York : Random House , 1992.

Stern , Susan . With the Weathermen . New York : Doubleday & Company , Inc. , 1975.

Toffler , Alvin . The Third Wave . London : Bantam Books , 1980.

Powershift . London : Bantam Books , 1990 .

Toffler , Alvin and Toffler , Heidi . War and Anti - War . London : Warner Books , 1993.

Other :

Clausewitz , Carl Philipp Godfried von . A Haborurol [On War] . Budapest : Zrinyi Katonai Kiado , 1987 .

Ijad , Abu . Heimat oder Tod . Der Freiheitskampf der Palastininser [Homeland or Death . The Palestinians' War for Freedom] . Dusseldorf : Econ , 1979.

ARTICLES

English :

Frankel , Bruce and Fields , Gary . " New Teen Fad : Buildibg Bombs ." USA Today , 5 June 1996.

Hawkes , Nigel . " Extremists spread propaganda and terror on Internet ." Times of London , April 13 , 1995, p. 6.

Mokrzycki , Mike . " Battleground of Bits and Bytes . " The Jerusalem Post , April 19 , 1995 , p. 5.

Nelan , Bruce et al. " The Price of Fanaticism ." Time , 3 April 1995.

S.A. " Texas University Posts Top Secret UK Gov Info on Web . " Newbytes , 25 March 1996.

Schlessinger , Philip . " Terrorism , Media and the Liberal - Democratic State : A Critique of Orthodoxy ." Social Research , 48 (Spring 1981) , 74 - 99.

Other :

" Netszerver , itt keresik az esztergomi bomba keszitojet . " Magyar Hirlap (Budapest) , August 27 , 1996.

Electronic :

American Firearm Industry Home Page . http://www.amfire.com:80

ARJ/newslink . http://www.newslink.org:80

Berman , Jerry . Testimony of Jerry Berman , Executive Director Center for Democracy and Technology Before the Senate Judiciary Committee / Subcommittee on Terrorism , Technology and Government Information . http://www.cdt.org:80/policy/terrorism/internet_bomb.test.html

BHU . Pyrotechnics Cookbook v1.0 . eran.db.eran.edu:80/~sarmowsp/FILES/anarcook.txt

Camus , Albert . The Rebel . Quoted in Phillip Robertson , A Short Essay on the Transmission of Ideas . http://fileroom.aaup.uic.edu:80/RSG/pform40unabomb.html

CIA. Psychological Operations in Guerrilla Warfare . http://entisoft.earthlink.net:80/psyops.htm

Collin , Barry C. " The Future of CyberTerrotism ." 11th Annual International Symposium on Criminal Justice Issues . http://www.acsp.via.edu:80/OICJ/CONFS/terror02.htm

Devost , Matthew G. " Political Aspects of Class III Information Warfare : Global Conflict and Terrorism ." Second International Conference on Information Warfare (Montreal : 18 - 19 January 1995) . http://us.okbmei.msk.su:80/FAQ/InfoWars/montreal.html

Outlaw Labs . Documents and Diagrams of the Atomic Bomb . http://www.nada.kth.se/~nv91-asa/atomic.html

Hobbit . Simplex 5 - Button Combination Locks : *Hobbit*'s in depth Evaluation . http://cyberus.ca:80/~sgi/locks.txt

Knowless , Ian . New Job . alt.revenge

Murray , Kevin D. Ten Spy - Busting Secrets . http://www.tscm.com:80/murray/html

NSA. NSA Employee's Security Manual . http://www.tscm.com:80/NSAsecmanual1.htm

rec.pyrotechnics

Roger , Jolly . Anarchy Cookbook v.666* . http://www.cyberbeach.net:80/~mbabcock/HPA/JollyRoger/

Saxon , Kurt . Repeating Crossbow . http://www.ipser.com:80/xbow/plan01

Saxon , Kurt . U.S. Militia . http://www.ipser.com:80/usmilitia/

S.A. " BioWar by MAIL ." The MCW Digest . http://www.xmission.com:80/~seer/mcw/biowar.html

S.A. " LSD Recipes # 1 - 3 ." The MCW Digest . http://www.xmission.com:80/~seer/mcw/lsd.html

Unknown Author . The Terrorist's Handbook . http://www.et.tudelft.nl:80/~koerkamp/tthb/

U.S. Army . FM 23 - 14 : M249 Light Machine Gun in the Automatic Rifle Role , (SL : U.S. Army , 1994) . http://155.217.020.55/atdl/docs/fm/23-14/fm2314.htm

U.S. Army . FM 23 - 25 : Light Antiarmor Weapons , (SL : U.S. Army , 1994). http://155.217.020.55/atdl/docs/fm/23-25/fm2325.htm

U.S. Army . " U.S. Army Operational Concept for Terrorism Counteraction , " TRADOC PAM 525 - 37 , March 19 , 1984 . gopher.icspr.umich.arm

USGS . http://edcwww.cv.usgs.gov:80/dclass/dclass.html

Viking , Last . Disk Drive Killer . alt.revenge

Wong , Thomas. American Communication Training (Campbell : TransCore Strategies , 1996) . http://www.transcore.com

Zimmerman , Phillip R. The Official PGP User's Guide . http://web.mit.edu/network/pgp.html