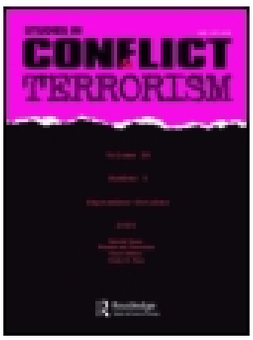

Routledge
Taylor & Francis Group

Studies in Conflict & Terrorism

ISSN: 1057-610X (Print) 1521-0731 (Online) Journal homepage: http://www.tandfonline.com/loi/uter20

Cyberspace-A New Medium for Communication, Command, and Control by Extremists

Michael Whine

To cite this article: Michael Whine (1999) Cyberspace-A New Medium for Communication, Command, and Control by Extremists, Studies in Conflict & Terrorism, 22:3, 231-245, DOI: 10.1080/105761099265748

To link to this article: http://dx.doi.org/10.1080/105761099265748

Cyberspace—A New Medium for Communication, Command, and Control by Extremists

MICHAEL WHINE

Community Security Trust
London, England

Information and Communication Technologies (ICTs) are extending the arena within which extremists and terrorists operate. Among the most active participants are Islamists and the Far Right, whose increasingly networked formats are enhanced by such technologies. These provide them with new benefits: interconnectivity; anonymity; cheapness; power enhancement; new audiences. Islamists and Jihadists are turning to the Internet to recruit, and to issue religious injunctions to the world-wide Muslim community. The stealthy growth of the U.S. militias was aided by the Internet, and white supremacists and neo-Nazis in the U.S., Europe, and elsewhere increasingly see it as the last communication medium free of interference, and which they can use to best effect. Although all use it to communicate, they are poised to use it for command and control.

During the 1970s and 1980s political extremism and terrorism frequently focussed on "national liberation" and economic issues. The collapse of the Soviet bloc and the ending of its covert funding and encouragement of terrorism led to a decline in the militant and violent left-wing terrorist groups that were a feature of the age. The 1990s however have seen the development of a "new terrorism."[1] This is not to say that state-backed terrorism has ceased, but rather that the spectrum of terrorism has widened.

This new extremism is frequently driven by religious fervor, is transnational, sanctions extreme violence, and may often be millenialist. The new terrorism may seek out military or government targets but it also seeks out symbolic civilian targets and the victims have mostly been innocent civilians (Alfred P. Murrah Building, Oklahoma City; World Trade Center, New York; AMIA Headquarters, Buenos Aires).

Growing concern about the development of this new terrorism has been paralleled by concern about the employment of the new Information and Communication Technologies (ICTs). ICTs offer a new dimension for political extremists and terrorists. They allow the diffusion of command and control; they allow boundless new opportunities for communication, and they allow the players to

Received 2 April 1999; accepted 19 April 1999.
Address correspondence to Michael Whine, Community Security Trust, Commonwealth House, 1-19 New Oxford Street, London WC1A 1NF, England.

Studies in Conflict & Terrorism, 22:231–245, 1999

1057-610X/99 $12.00 + .00

target the information stores, processes, and communications of their opponents. The information revolution is enhancing the importance of all forms of networks, and it favors their growth by making it possible for diverse and dispersed actors to communicate, consult, coordinate and operate together across greater distances and on the basis of more and better information than before.

The developments in communications technologies, from fax machines to e-mail, facilitate what has been called "netwar," or offensives conducted by often geographically separate, diverse, interconnected non-state actors rather than by hierarchies. So far netwar appears to be of greater interest to extremist advocacy groups and terrorists. Because there are no physical limits or boundaries it has been adopted by groups who operate across great distances or transnationally. The growth of such groups, and their growing powers in relation to those of nation states, suggests an evolving power-based relationship for both. Military strategist Martin Van Creveld has suggested that war in the future is more likely to be waged between such groups and states rather than between states and states.[2]

As James Adam describes it:

> The arrival of the Internet has provided the first forum in history for all the disaffected to gather in one place to exchange views and reinforce prejudices. It is hardly surprising, for example, that the right-wing militias favourite method of communication is e-mail and that forums on the Internet are the source of many wild conspiracy theories that drive the media.[3]

Two of the groups which have quickly grasped the advantages of networking via the new information technologies are the Far Right and Islamic fundamentalists. The Far Right is increasingly active in the U.S.A. and Europe and seeks to return to some imagined past world in which an armed, racially pure, white man can live untroubled by the police, the Inland Revenue, and the world banking system. The Islamist diaspora, now spread worldwide, seeks a "return" to divine-ruled states (or even one transnational state) in which all Muslims will live under the norms and laws of the Saudi Arabian peninsula in the sixth and seventh centuries of the Common Era. These types of organizations, comprised of geographically far-flung, radical, non-state components make them ideal users of networks and proponents of Netwar.

Government Concerns

The Foreign Ministerial Conference on Terrorism, held in Paris in July 1996, suggested inter-governmental consideration of limiting encryption to allow, when necessary, lawful government access to data and communications in order to prevent and investigate acts of terrorism, while protecting the privacy of legitimate communications, and to intensify the exchange of operational information, especially as regards the use of communications technologies by terrorist groups.[4]

At the policing level within Europe the inter-governmental process has been paralleled by a series of conferences under the auspices of the European Commission and Europol, the police liaison body. In April 1997, Europol circulated a communication to European police forces which requests that they monitor illegal content on the Internet, seek out "reporting" points, investigate cross border links, exchange information, reconcile national laws, cooperate on investigations, and that self-regulation of the Internet be encouraged.[5]

In Britain, concern has grown to the point where responsibility for Internet intelligence gathering has now been passed to the Defence Research Agency, with its large computing capacities, and which now carries out a wide range of information and monitoring activities in furtherance of its corporate aim to investigate subversive and illegal material.[6] An agreement was expected in late 1998 between Internet Service Providers (ISPs) and the police allowing the latter unrestricted automated access to information held on the ISP's computers in order to monitor criminal, pedophile, and terrorist activity, but the parties failed to reach an agreement and resumed discussion in early 1999. Not surprisingly, the proposal has caused alarm in some circles, and criticism from the office of the Data Protection Registrar, which has pointed out that current legislation does not permit "fishing expeditions" and should only be used for investigating particular crimes.[7]

It is in America, however, that information and communication technology usage is greatest, and where fear of its misuse by extremists has gone furthest. The open nature of American society and its governmental systems makes it especially vulnerable. Alarm bells have been ringing for some years as a consequence of continued hacking into government and commercial computer systems, and by the increasing sophistication of domestic extremists and terrorist groups.[8]

Why Extremists Use ICTs

ICTs provide a range of benefits that previously did not exist. First, they allow interconnectivity; that is, communication and networking, which may be both external and internal. An example of external networking may be found on the website of Hezbollah, which publishes a daily diary of the terrorist attacks its members have carried out in Southern Lebanon. The site also urges anybody with an opinion about the organization's anti-Israel activities to get in touch. A spokesman was recently quoted as saying:

> The service is very important for the morale of our resistance fighters. They are always happy to know that people around the world are backing them.[9]

Neo-Nazi groups were among the first to seize upon the benefits of cyberspace and German neo-Nazis have been communicating with one another, and organizing their activities, via the ThuleNetz (Network) since the 1980s.

> Provided with passwords such as Germania or Endsieg (Final Victory) from a post office box, personal computer screens will display a calendar of forthcoming neo-Nazi events and list contact numbers of leading right-wingers. . . . On Remembrance Sunday, police saw in action for the first time, computer planned co-ordinated neo-Nazi action, involving the widespread use of secret codes and radio communication. . . . "The advantage of electronic mail boxes is that they are free of censorship and bug-proof," said Karl Heinz Sendbuhler of the National Democratic Party.[10]

Examples of internal networking occurred when news of the killing of Combat 18 member Christopher Castle by two of the group's leaders, in Essex in February 1997 was posted on the Internet site of the American National Socialist White People's Party within twelve hours. Also published were details, accusations, and counter-accusations of the bombing campaign which preceded it.[11] The simultaneous raids in America and Canada on the offices of Resistance Records, the major producers of white supremacist and skinhead music and tapes, and the home of George Burdi, its founder, were reported on the Internet within hours, giving a warning to their supporters.[12]

The U.S.-based Stormfront carries links to Spanish, Canadian, and German contacts and the British national revolutionary group, International Third Position, posts messages from Polish, Flemish, Romanian, Slovakian, and American Far Right nationalist groups.[13]

A second benefit of ICTs is that cyberspace allows covert communication and anonymity, and anonymity is probably the most noticeable trend in terrorist acts of recent years. Milton John Kleim Jr., the former self-styled "Net Nazi Number 1," wrote of these powers, before he renounced his Nazi views that:

> All my comrades and I, none of whom I have ever met face-to-face, share a unique camaraderie, feeling as though we have been friends for a long time. . . . This feeling of comradeship is irrespective of national identity or state borders.[14]

A number of Islamist sites provide passworded communications to members and close sympathizers. The United Islamic Students Association in Europe provides a site for members only, suggesting that instructions for militant student activity may be included in the postings.[15] Hamas is known to conceal its communications and its use of electronic messages clearly presents problems for security agencies. A recent article in Jane's *Foreign Report* suggested that the Israeli security services have been unable to crack the codes used by Hamas:

> Without offering evidence, investigators in the security service, Shin Beth, assert that a full range of instructions for terrorist attacks, including maps, photographs, directions, codes and even technical details of how to use the bombs are being transferred through the

> Internet. They suspect that many of the instructions are sent from Britain, where they say that the Islamist/Palestinian organization, Hamas, has its main European base.[16]

Similarly, a "Kahlid Ibrahim" sought to purchase classified and unclassified U.S. government software and information about the Indian Atomic Research Center. Ibrahim tried to hide his identity by using anonymous Hotmail accounts, although it is stated that he always posted from the same ISP in New Delhi. He eventually identified himself as a member of the Islamist Harkat Al Ansar terrorist group. [17]

Terrorist groups are known to share information and to collaborate with one another through cyberspace. Since such collaboration is inherently risky, and inter-group communication is a target for national security services, the use of encryption has increasingly been adopted. The encryption might be used both to "anonymize" and to authenticate communications. The digital basis of cyberspace communication makes it an ideal vehicle for encrypted communication.[18]

The concept of "leaderless resistance," promoted by American Far Right leader, Louis Beam, but developed by terrorist groups much earlier, shows disturbingly, but with great relevance for understanding netwar in the Information Age, the importance of doctrine and secrecy. His particular doctrine downplays hierarchy in favor of a network of "phantom cells." Such cells, communicating covertly in a networked format, can be more defensively robust, and more offensively flexible:

> Utilising the leaderless resistance concept, all individuals in groups operate independently of each other, and never report to a central headquarters or single leader for directional instruction. . . . Participants in a programme of leaderless resistance through phantom cell or individual action must know exactly what they are doing and exactly how to do it. . . . All members of phantom cells or individuals would tend to react to objective events in the same way through usual tactics of resistance. Organs of information distribution such as newsletters, leaflets, computers etc. which are widely available to all, keep each person informed of events allowing for a planned response that will take on many variations. No one need issue an order to anyone.[19]

The stealthy growth of the American militia movement, unobserved by government and law enforcement agencies until recently, has been considerably aided by the ICTs. According to Ken Stern:

> The rapid formation and growth of the militia movement were due in part to new technologies that made communication quicker, easier, and cheaper. Least important of these was talk radio. Most important were the Internet and, to a lesser degree, fax networks.[20]

The ability of German neo-Nazi groups in the early 1990s to organize violent demonstrations against asylum seekers and foreign "guestworkers," throughout the newly united country, without seeming to have any national organizing structure was enhanced by the use of ICTs. It was recently estimated that more than one hundred German neo-Nazi groups send e-mails and post messages regularly on the Internet, some using encryption in a German variant of Pretty Good Privacy called Kryptografil.[21]

British neo-Nazis have also taken up the Internet in recent years realizing that it offers a degree of anonymity. The National Socialist Movement and Combat 18 (formerly a stewarding group for the British National Party which progressed from intimidation and violence to terrorism before its virtual demise) recently registered their sites in North America, and the former posted terrorism manuals, using a Canadian site to mask their identity (see later).

The writer of the National Front journal, *The Nationalist,* recently discussed the benefits that ICTs were bringing to this group:

> All over the world anyone with access to the Internet can find a full range of information regarding the National Front at the touch of a button. And despite the best efforts of our opponents, so far our site has remained functional 24 hours a day, seven days a week since its inception. . . . If our opponents were successful in say, pressurising one of our service providers into dropping our site, we could be back on-line at our main Internet address within half an hour. . . . New friends from around the world have been made and important contacts have been established, particularly in the United States, where we regularly liaise via E-mail with a major nationalist organization, with a possible view to future long-term co-operation. The Internet will be the main political campaigning tool of the next decade and beyond.[22]

A third reason for using the Internet is that it is cheap. For the price of a computer and a modem an extremist or would-be terrorist can become a player in national and world events. ICTs lower the threshold for participating in illegal acts and without state backing extremists will look for cost-effective instruments. As computers become increasingly inexpensive, small, and user-friendly, cyberspace crime and terrorism will become "democratized." Soon almost anyone will be capable of participating, as the technology and the techniques become available.

The use of small, cheap laptop computers in storing terrorists' plans was illustrated by Ramzi Ahmed Yusuf, the mastermind of the World Trade Center bombing, who had worked out his operational plans to bomb American airlines in the Pacific on his machine. Abd-al-Rahman Zaydan, a Hamas terrorist leader, was convicted by the Nablus Military Court in January 1995 on the basis of information stored in his personal computer database that linked dozens of terrorist squads and activists in Israel, Jordan, and Germany. Following Zaydan's arrest, Hamas's method of operation (and its covert use of ICTs) was uncovered, and terrorists were apprehended.[23]

Fourth, ICTs act as a force-multiplier, enhancing power and enabling extremists to punch above their weight. They can now have a reach and influence that was previously reserved for well organized, state-funded terrorist organizations. Communication technology represents, in many respects, the "death of distance" and the national borders that once separated the attackers from their targets have ceased to exist.

Even the smallest groups are aware of the powers of the force-multiplier effect. Another small British national revolutionary group with an international perspective is the National Revolutionary Faction (the product of a split within the International Third Position):

> The new homepage has put us in touch with an increasing number of National Revolutionary activists worldwide. If you have access to a computer, then why not check it out for yourself at: http://www.geocities.com/Athens/Troy/8854.[24]

Fifth, ICTs enable extremists to reach their target audience when other outlets and media are denied them, and to reach new audiences, particularly the young and educated. Kashmiri extremists overcame newspaper resistance to covering their terrorist campaign against the Indian authorities by use of the Internet, and the Mexican Zapatistas very quickly became sophisticated users of the Internet in order to spread their message around the world.[25]

The Afghan Taliban publish their ideology on-line, believing that the Western media will distort or refuse to publish their messages.[26] The Far Right in particular use ICTs for this reason. In several European countries hate-filled postings by neo-Nazi groups would be illegal if published in hard copy; the absence of sanctions, or protocols on the Internet, allow the postings.

The Internet has enabled the Far Right to reach across national boundaries and by-pass laws banning hate material, as in Britain, France, Germany, and Scandinavia, and has therefore become a priority from the point of view of their doctrine.

> The emergence and rapid growth of the information superhighway computer network as a vast global communications forum is dramatically transforming the nature of the international struggle for truth in history and for our basic freedoms.[27]

The Net strategy of Milton Kleim, a former leading member of the American neo-Nazi National Alliance, defined the Far Right's approach:

> The Net strategy USENET . . . is the only relatively uncensored (so far) free-forum mass medium which we have available. The State cannot yet stop us from "advertising" our ideas and organizations on USENET, but I can assure you that this will not always be the case. NOW, is the time to grasp the WEAPON which is the NET, and wield it skilfully and wisely while you may still do so freely. . . .

> Crucial to our USENET campaign is that our message is disseminated beyond "our" groups: alt politics, nationalisation, white, alt: politics, white-power, alt. revolution. counter, alt. skinheads, and to a certain extent, alt: revisionism. . . . We MUST move out beyond our present domain and take up positions on "mainstream" groups. . . .
>
> Remember our overall USENET strategy must be to repeat powerful themes OVER AND OVER AND OVER. We cannot compete with the Jews' media, of course, as our propaganda dissemination is but a very small fraction of the everywhere pervasive leftist propaganda. However, our ideas possess an energy that truth alone contains.[28]

Communication, Command, and Control

As terrorism has become increasingly transnational, the networked organization form has expanded. Now that terrorism is increasingly sub-state, or semi-detached, networking and inter-connectivity are necessary to find allies, and influence others, as well as to effect command and control. ICTs have facilitated this, and have also enabled multiple leaders to operate parallel to one another in different countries. It therefore might be said that a shift is taking place from absolute hierarchies to hydra-headed networks, which are less easy to decapitate. An analogy, using the Palestinian example, may be that the more networked form of Hamas is replacing the hierarchical structure of the PLO. In many ways the Afghan War was a seminal event in promoting the networked form in that it showed that fluidly organized groups, driven in this case by a religious imperative, could defeat an experienced hierarchically structured army.

Geographical dispersion, both physical and in cyberspace, provides extra security; a rigid hierarchical structure is more easily penetrated and neutralized. Israel, for example, has not yet found a way to deal with Hamas's decentralized and internationalized command and control structure, which uses encrypted Internet messages. The investigation by the Federal Bureau of Investigation into terrorist activity in the U.S. indicated that part of Palestinian Islamic Jihad's command and control system was located in Tampa, Florida. Likewise, Hamas allegedly has some of its fundraising infrastructure in London and the U.S.A., and publishes its main Arabic journal, *Filistin al Muslima*, in London.

Islamist terrorists may be said to fit the network ideal; many supportive expatriate communities are based in sympathetic or neutral states enabling political activists and terrorists to operate within the safe haven that modern democracies provide. It should be noted that it is not intended here that the term "Islamists" should refer only to terrorist organizations, but rather to those Muslim militants who believe that Islam is incomplete without its own state in which Shariah provides the system of governance, and who campaign for its imposition. Among Islamists, it is the Jihadists (religious warriors) who are of particular interest for this article. Hasan al Banna, Sayyid Qutb, and Abdul Ala Maududi, and the organizations they founded, Ikhwan al Muslimoon and Jamaat Islami, and the ideological off-shoots these have spawned give rise to the "Jihadist" ideology.

Jihad in the modern Islamist sense knows no political space, or state; its space is that of the Umma, the community of Muslims, wherever they may be. Although the concept of Jihad may be interpreted on different levels, it often incorporates violence when applied to Islamists:

> The ultimate experience is of course Jihad, which for Islamists means armed battles against communists (Afghanistan) or Zionists (Palestine) or, for the radicals, against renegades and the impious.[29]

The Algerian Armed Islamic Group (the GIA) is one example of a networked Islamist organization. Allegedly responsible for a bombing campaign in France, it appears to have had a command and control center in Britain for some years prior to the expulsion of some members by the British authorities. At the same time sympathizers were also safe-housing some of its weapons and explosives in Belgium.

Algerian terrorists have been able to communicate with their sympathizers and members by use of the Internet and have used the services of Muslim "news-agencies," which republish their postings. Foremost among them is MSANEWS. On their site were published communiqués from the GIA, Front Islamique de Salut (FIS) and many other Islamists. (It should be noted, however, that MSANEWS also posts articles and communiqués from non-Islamist Muslim and non-Muslim sources, that it has condemned terrorism, and that it no longer re-posts communiqués of organizations which advocate terrorism.)[30]

The site of the Campaign for the Defence of Legitimate Rights (CDLR), the Saudi opposition group, also contains postings from groups not directly connected with it, as do London-net@Muslimsonline and the pro-Iranian Muslimedia International, which like others, re-posts interviews with Osama bin Laden, the exiled Saudi terrorist leader. As with some other Islamist groups, Muslimedia International also promotes antisemitism and Holocaust denial and provides links with the American Holocaust denier, Michael Hoffman II and his Campaign for Radical Truth in History, thereby highlighting the interconnectivity possibilities between totally different ideologies sharing a perceived common enemy.

An Islamist site that particularly aims its message to the outside world is that of Hizb-ut-Tahrir, the Islamic Liberation Party. Imperial College, London, hosted their first U.K.-based site, but following complaints to the college authorities the site was closed down. They now post in their own name and as Khilafah, and provide Internet-based access to their hard copy material, literature, and their regional activities.[31] Al-Muhajiroun (The Emigrants) whose U.K. leader, Omar Bakri Mohammed, was the founding leader of Hizb-ut-Tahrir in Britain, and from which he split claiming differences with the Middle East-based leadership, also provides details of its activities, as well as lists of its hardcopy publications and contacts. During 1998 Mohammed reported the communiqués of Osama bin Laden, for whom he claims to act as a spokesman. As a consequence of his endorsement of the bombings of the U.S. embassies in Dar-es-Salaam and Nairobi, his postings are no longer carried by MSANEWS.[32]

Hamas and its supporters and sympathizers have been among the most prolific users of the Internet. MSANEWS provides a list of Internet resources about Hamas including copies of its covenant, its official communiqués (at Assabeel On-line), and communiqués of its military wing, the Izz al-Din Al-Kassam Brigades. Information about Hamas, in fact, may also be accessed in various ways: via MSANEWS, via the Palestine site, and via the Islamic Association for Palestine. Hamas's own site, which posts in Arabic, is the Palestine Information Centre.[33]

Religious luminaries from one country sometimes act as the higher legal and moral authority in another country. Sheikh Yusuf al-Qaradawri of the Egyptian Ikhwan al-Muslimoon (Muslim Brotherhood) lives in Qatar and serves as the Imam (religious leader) for the Palestinian Hamas; Sheikh Ibn Qatada, a Jordanian Palestinian living in London, serves as the Imam for the Algerian GIA; Sheikh Abu Hamza, an Egyptian national and former Afghan Jihad volunteer, serves as a propagandist for the Algerian GIA and Imam for the Yemeni Jihad group, but lives in London. Their messages of guidance and support find an outlet most frequently now via ICTs. Thus Abu Hamza's "Fatwa IRAQ2 15/02/98," issued after the February 1998 showdown between Iraq and the U.N., was published on his Supporters of Shariah website.[34]

While some commentators have argued that modern cultural forces, such as ICTs, serve to undermine Islamization in Muslim society, it is also equally easy to argue that they provide a new and growing medium by which Islamism is disseminated. Even if they do not reach the poorer sections of Muslim society, they certainly reach many educated expatriate communities, among whom they find support. The growing number of advertisements, on the Internet and in Muslim papers and journals, for conferences to discuss the use of the Internet to promote Islam, or Islamism, supports the thesis that many activists and religious teachers see these developments as positive ones to be recommended and encouraged.

Combining religious injunctions with strategic commands is a noticeable feature of such Islamist leaders, and their groups. Calls to carry out Jihad are frequently cloaked in religious and pseudo-religious language, but the implication is clear for the target audience. Thus, for example, Osama bin Laden's Ladenese Epistle, which was originally faxed to his London contact Khalid al Fawaz and then posted to MSANEWS in August 1996 by the London-based Saudi dissident groups CDLR and MIRA, is recognized as providing general guidance for anti-American terrorism.[35]

The Nida'ul Islam site, based in Australia, promotes an uncompromising message of both Jihad and of suicide terrorism. A recent posting, "The Islamic Legitimacy of the Martyrdom Operations," states that martyrdom is forbidden in Islam, but approvingly cites those martyrs who willingly gave their lives for Muslim causes and then transposes these causes to contemporary issues. It attempts to demonstrate with quotes from the Quran and the Sunnah that Islamic bombing assaults and martyrdom attacks are legitimate Islamically and that these fall within the framework of Islam.[36]

Azzam Publications, named after Abdullah Azzam, a Palestinian who be-

came a military leader in Afghanistan and who was assassinated in Pakistan in 1989, has also published calls for Jihad volunteers:

> The Saudi Government does not intend to help the Muslims is Kosova and it has prevented its nationals from going there to fight. This means that the Jihad in Kosova is now a greater responsibility on Muslims with western nationalities. . . . Redistribute this e-mail message all over the world . . . telephone the nearest Saudi Embassy or Consulate to protest against this crack-down and tell everyone to do so until it jams the lines of the Saudi Consulates around the world . . . e-mail the Saudi Embassy in Washington with messages of protest . . . begin to prepare yourselves to go and fight in Kosova to make up for the lack of manpower that was heading there from Saudi Arabia. Wait for the Kosova bulletin from Azzam Publications.[37]

Among the Far Right, the U.K.-based national revolutionary group, The International Third Position, illustrates graphically the adoption of ICTs to enhance a position. The group is tiny, but its foreign contacts are numerous, widespread, and growing. In the space of just over one year its Final Conflict Email Newsletter has grown in size and scope to reflect the news of, and messages from, its world-wide contacts:

> AMERICAN THIRD POSITIONISTS
>
> Can comrades in America please contact the above address or send and E-mail to the E-mail address below if they would like to help build the Third Position in America. Our Comrades there wish to build grass roots support, possibly put out literature and work with Third Positionists, Distributists and Nationalists of a good nature in the USA. This is the only Third Positionists group recognised by us in America. Third Position Youth (third@friko6.onet.pl).[38]

Final Conflict also acts as a "news agency" for Holocaust deniers (in much the same way as MSANEWS does for Islamists), many of whom are also Far Right extremists. The Email Newsletter re-posts communiqués from David Irving and Fredrick Toben's Australian Adelaide Institute, which, like the California-based Institute for Historical Review, attempts to provide a scholarly veneer for denial:

> HISTORIC SYMPOSIUM HELD IN AUSTRALIA
>
> For your itnerest (sic) the program of our recently held symposium The Final Intellectual Adventure of the Twentieth Century.[39]

Clearly, it was impractical for some invitees to attend, and it is known that others were refused permission to visit Australia by its Department of Immigration, but the easy access to Internet and video links facilitated conference presentations which otherwise might not have taken place.

The supply of bomb manuals from America (where they are easily available), to Europe (where they are not), by fax and Internet was made public after the wave of bomb attacks on Austrian politicians and civic dignitaries in the early 1990s. However, a recent example of the Far Right's use of the Internet to post a detailed terrorism manual was provided by the British neo-Nazi, David Myatt, of the National Socialist Movement. His "Practical Guide to Aryan Revolution" was posted at the end of November 1997 from the site of Canadian Bernard Klatt in order to evade police scrutiny. The chapter headings included: Methods of Covert Direct Action, Escape and Evasion, Assassination, Terror Bombing, Sabotage, Racial War, How to Create a Revolutionary Situation, Direct Action Groups, etc.

The contents provided a detailed and step-by-step guide for terrorist insurrection with advice on assassination targets, rationale for bombing and sabotage campaigns, and rules of engagement. Although he may have committed no indictable offense in Canada, Klatt was forced to close down his site in April 1998. Myatt is currently the subject of a British criminal investigation for incitement to murder and to promote race hatred.[40]

Police forces in Britain and France also recently investigated an international neo-Nazi network which issued death threats against French celebrities and politicians from their British-based Internet site. Hervé Guttuso, the French leader of the Charlemagne Hammer Skins was arrested in Essex at the same time eight members were arrested in the South of France. The French members of the network were charged with making death threats, and Guttuso was the subject of a French extradition request to the British courts. According to the French Interior Ministry, police in Toulon traced the London address of the Internet site, which was being accessed about 5,000 times a month. The investigation enabled the police to identify 1500 people sympathetic to the neo-Nazi group in various countries including Britain, Greece, Canada, America, and Poland. The investigators found that the Charlemagne group appeared to be one of the largest and best organized neo-Nazi groups yet uncovered, with a coordinated international structure and logistical centers for disseminating violent racist propaganda, based principally in Britain and America. Although the group gave a postal address in London as their center, their material was disseminated via Klatt's FTC Net, (as have been the postings of Marc Lemire, Paul Fromm, Doug Christie, The Heritage Front, and other neo-Nazi and white supremacist groups).[41]

The British Far Right may have been slower to realize the command and control possibilities of ICTs than their U.S. or German co-ideologes, but they appear to be catching up. Although in recent years it is the violent skinhead music scene that has provided the main medium through which they promote liaison, it is clear that for some the future lies with ICTs.

Conclusion

The use of ICTs to enhance command, control, and communication is especially apparent among Islamist extremists and the Militia movement and Far Right in America. This clearly reflects the higher ICT access in North America.[42] And,

although Western governments fear, perhaps rightly, that their national infrastructures may be a target for information warfare or cyber-terrorism, the evidence so far is that sub-state groups use ICTs mainly for propaganda, secure communications, intelligence gathering, and funds management.[43]

It has been noted by one observer that the Internet has not replaced other communications media for the Far Right, and that its largest use in this regard has been to advertise the sale of non-Internet related propaganda such as books, audio tapes, and videos. Nor has the Internet led to an increase in mobilization, and the Seattle-based Coalition For Human Dignity observed that Far Right events in the U.S. which were heavily promoted only on the Internet, were in fact failures.[44]

A recent despairing posting by Harold Covington of the National Socialist White People's Party reinforces the point that for some on the American Far Right the Internet has become an end in itself. Surfing the Net has replaced real action:

> It is a measure of how degenerate and weak our movement has become that some people actually think this is a good thing. Not only do we want risk-free revolution, we now want people-free revolution. Here lies the great danger of the computer for everyone who uses it. It allows us to live and work interacting with a MACHINE rather than with people, and for white males who already have a problem in the cojones department, it provides the final, terminal escape from reality and from any demand that they ACT.[45]

However, it does not pay to be complacent; extremists and terrorists are increasingly information technology literate. Continuing research by Les Back, Michael Keith, and John Solomos of Goldsmiths College, London has shown that what is significant for the Far Right and its use of the Internet is that it:

> possesses the potential to offer the relatively small numbers of people involved a means to communicate, develop a sense of common purpose and create a virtual home symbolically . . . the Internet combines both intimacy and remoteness. These properties make it uniquely suitable for maintaining relationships among groups that are prone to attrition, because forms of association can be established at a social and geographical distance.[46]

These properties also make the Internet uniquely suitable for maintaining relationships among transnational groups, or geographically separated groups with mutual interests, who are borderline legal (or illegal) and subject to travel and publishing constraints. As demonstrated above, international terrorist groups, as well as the law enforcement agencies concerned with their control, have recognized the potential for new information technologies to enhance such groups' nascent networking efforts. Vigilance is required; the command and control and communication advantages the Internet offers terrorist groups must not be underestimated.

Notes

1. Bruce Hoffman, *Inside Terrorism* (London: Victor Gollancz, 1998); Harvey W. Kushner, *The Future of Terrorism: Violence in the New Millenium* (London: Sage, 1998).

2. Martin Van Creveld, *The Transformation of War* (New York: Free Press, 1991).

3. James Adam, "Clinton's Dreams Die a Dirty Death," *The Sunday Times*, London, 27 July 1997.

4. *Agreement on 25 Measures*, Ministerial Conference on Terrorism, Text of Agreement, Paris, 30 July, 1996, http://www.state.gov/www/global/terrorism/measures.html; *Combating Terrorism: The Paris Ministerial Fact Sheet*, 30 July 1996, http://www.state.gov/www/global/terrorism/fr-achievenments.html.

5. *Communication on Criminal Use of the Internet*, European Commission/Europol, 9 April 1997.

6. *Controlling Unsuitable Material,* Department of Trade and Industry, Internet Study, Sema Group Consulting, 11 April 1996.

7. Duncan Campbell, "Police Tighten the Net," *The Guardian*, London, 17 September 1998; David Bamber, "Police Seek to Intercept E-mails Without Warrant," *The Sunday Telegraph*, London, 24 September 1998.

8. *Presidents' Commission on Critical Infrastructure Protection, Report Summary*, Page 3, October 1997, http://www.pecip.gov/summary.html.

9. "Hizbollah on the Internet," *The Daily Telegraph*, London, 19 February 1997.

10. "Neo-Nazis Go Hi-Tech with Electronic Mailboxes," *The Guardian*, London, 19 November 1993.

11. Nswpp@earthlink.net, 10 March 1997.

12. "Resistance Records Raided," mlemire@interlog.com, 9 April 1997.

13. Stormfront, http://www.nna.stormfront.org; International Third Position, http://www.dialspace.dial.pipex.com/town/place/rbg93; Final Conflict, http://www.dspace.dial.pipex.com/final.

14. Author's emphasis. Crawford Kilian, "Nazis on the Net," *The Georgia Straight, Vancouver*, 11–18 April 1996.

15. http://www.tawheed.org/newsnviews.

16. "Cyber-terrorism," *Foreign Report*, London, 25 September 1997.

17. McKay, Niall, "Do Terrorists Troll the Net?," Wired News, http://www.wired.com/news/print.

18. K. Soo Hoo, S. Goodman, L. Greenberg, "Information Technology and the Terrorist Threat," *Survival,* International Institute for Strategic Studies, London (Autumn 1997), p. 13a.

19. Louis Beam, "Leaderless Resistance," *The Seditionist*, USA, Issue 12, February 1992.

20. Kenneth Stern, *A Force Upon the Plain* (Norma and London: University of Oklahoma Press, 1997), p. 224.

21. B. Schroder, *Outlook,* BBC World Service Broadcast, 24 January 1996.

22. A. Ashcroft, "NF: Marching along the Informative Super-Highway," *The Nationalist*, Issue No.2, London, October 1998.

23. Hamas Database Discovered: linked to Jordan, Germany, Kol Israel Radio, Israel, 31 January 1995, as cited in Foreign Broadcast Information Service Daily Report, Near East and South Asia, FBIS -NES-95-021, February 1995, p. 41.

24. "The Revolution Enters Cyberspace," *Catalyst—The Official Bulletin of the NR Faction,* London, October 1998.

25. Michael Vatis, Deputy Assistant Director and Chief, National Infrastructure Protection Centre, Federal Bureau of Investigation, Proceedings Report, Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses (Washington, DC: Potomac Institute for Policy Studies, 16 April 1998), p. 4.

26. http://www.taliban.com.

27. "Revisionist Global Computer Outreach: IHR Cyberspace Connection Reaches Millions World-Wide, Generates Widespread Attention, Provokes Bigoted Rage," *Journal of Historical Review* 15 (July/August 1995).

28. Milton John Kleim, Jr, *On tactics and strategy for USENET*, 1995, bb748@FreeNet.Carlton.CA.

29. Olivier Roy, *The Failure of Political Islam* (London: IB Tauris, 1994), p. 57.

30. AIG's Algeria News: GIA's Letter to the French, http://www.net/~msanews/MSANEWS/199606/19960629.l.html, 2 July 1997.

31. http://www.Hizb-ut-Tahrir.org/aim.htm and http://www.khilafah.com.

32. http://www.ummah.org.uk/Almuhajiroun.

33. http://www.palestine-info.org/.

34. Supporters of Shariah, Vol. 1l1, March 1998, http://www.ummah.net/sos/march98.htm.

35. http//www.mynet./~MSANEWS/199610/19961013.10html, 26 June 1997

36. http://www.islam.org.an/articles/16/martyrdom.html.

37. http://www.webstorage.com/mazzam.

38. *Final Conflict News Email,* Issue 587.

39. *Final Conflict News Email,* Issue 465, 11 August 1998.

40. D. Myatt, "A Practical Guide to Aryan Revolution," http://www.ftcnet.com/~ehs/readm18htm.

41. "Un réseau néonazi mis au jour," *Le Figaro*, Paris, 18 February 1998; Susannah Herbert, "France Calls on Britain to Extradite 'Neo-Nazi'," *The Daily Telegraph*, London, 19 February 1998; Ben Macintyre, "Internet neo-Nazi suspect arrested in Britain," *The Times*, London, 19 February 1998.

42. Households having computers: 40% in U.S.; 30% in Germany; 20% in Britain. Source: *The Sunday Times Business News,* London, 9 July 1998, p. 32.

43. Andrew Rathmel, "Cyber-Terrorism: The Shape of Future Conflict," *RUSI Journal*, London, October 1997.

44. D. Burghart, "Cyperh@te: a Reappraisal," *The Dignity Report* 3(4) (1996).

45. Harold Covington, "The 'Nazi Computer Club'," nswpp@ix-netcom.com, 15 May 1998.

46. Les Back, Mitchell Keith, John Solomos, "Nation and Race: The Developing Euro-American Racist Subculture, in *Racism on the Internet: Mapping Neo-Fascist Subcultures in Cyberspace,* ed. Jeffrey Kaplan and Bjorgo Tore (Boston: Northeastern University Press, 1998).