

Chapter 1

Terrorism and the Internet: Use and Abuse

Abraham R. Wagner

System Research & Development Corp. Los Angeles, CA 90067
E-mail: arw@it.org

1.1 Introduction

What began as an MIT doctoral dissertation in 1962, and a U.S. Defense Department experiment in communications in the years that followed, has evolved into a technological revolution now known as “cyberspace” and the Internet. It is indeed a revolution that goes far beyond communications. In terms of making media available to people worldwide, it is likely the most significant advance since Gutenberg’s invention of moveable type in the 15th century. Use of the Internet has literally exploded from a handful of scientists in the U.S. to a world where “net” access is almost universal. The net has become a medium for all – the good, the bad and the ugly, and terrorists are no exception. Terrorists, terrorist organizations and their sponsors have all become increasing users of the Internet for a variety of functions. Just as in years past, when terrorists relied on other technologies such as telephone, radio, the mails and other systems, they cannot be barred from net access and will continue to use net resources for their purposes. The present paper explores the evolution of the Internet; current terrorist uses of the net; and what may be possible in terms of counter-terrorist operations in this area.

1.1.1 *Evolution of Cyberspace and the Internet*

True revolutions in communications do not come along very often. Possibly the only thing that comes close in comparison to the Internet was

Morse's invention of the telegraph in the early 19th Century ¹. At the outset, e-mail and the web were not even a part of the vision. Cyberspace and the Internet began as another "project" between the U.S. Defense Department's Advanced Research Projects Agency (ARPA) and a research group around the Massachusetts Institute of Technology ². Leonard Klienrock's now famous MIT thesis presented a novel and remarkable new concept for communications, namely that "packet switching" would be a more efficient use of a network than "line switching" that had been the approach taken since the time of Morse ³. Klienrock's 1962 thesis did not lead immediately to the ARPANET or the Internet. Communications in general were not a high priority for ARPA in the 1960s, and the space race got most of the Agency's attention and funding. In those years the U.S. was sadly behind the Soviet Union, and was rushing madly to catch up. In late 1966 ARPA did propose a new communications program to the U.S. Congress, and sought additional funds for the next fiscal year to begin work on an experimental switched packet network. Given the pace of the U.S. Governmental process in those years, funds for the ARPA Communications Program were not actually available until 1968, at which the Agency solicited proposals from various contractors to build the first elements of the ARPANET ⁴. By

¹In May 1844 Samuel Morse sent his famous message "What hath God wrought" over a 37-mile telegraph line from Washington to Baltimore, funded by a 50,000 grant from the U.S. Army. Although ignored in the first few years, by 1851 there were 50 competing telegraph companies, and by 1866 Western Union (formed by a merger of several of these) had over 4,000 offices and had become the first communications giant in history.

²Formed during the Cold War, in an effort to fund a wide range of defense technologies of possible importance to the U.S., ARPA has been at the forefront of technical developments in a host of critical areas. Over the years, the word "Defense" has been added, then subtracted, and then added again to its name, and it is currently known as DARPA. In the early days of the net, the "D" wasn't there, so the net was known as the ARPANET. DARPA itself does no work internally. Its relatively small staff of technical experts is responsible for the direction of research funds to universities, contractors, national laboratories and others who perform the actual research tasks. The results have been nothing less than astounding. This approach has given rise to an entire information technology industry, and several others. For a good historical account, see Stephen Segaller, *Nerds 2.0.1: A Brief History of the Internet*, New York: TV Books, 1998.

³In simple terms, "line switching" means that the sender and recipient are somehow "connected" for the duration of their communication, and tie up the line for that period. Alternatively, the "packet switching" concept breaks all communications into uniform digital "packets" which are sent over available network resources, and then re-assembled by the recipient. No single line is tied up, and the network routs the packets in the most efficient way possible. In the analog world of the 1960s, it was an interesting concept, but of limited practical use. In the digital world of the 1990s, it became a multi-billion dollar revolution. It has changed both the technology and economics of communications as nothing else in history.

⁴ARPA's request for proposals, issued in July 1968, went to a range of companies. It is interesting to note that the "major" firms IBM and Digital Equipment Corp. both

BIDDING FORM 14, JULY 1964 GENERAL SERVICE ADMINISTRATION DSR PROC. 500 (41) GEN 1-14.501		REQUEST FOR QUOTATIONS (THIS IS NOT AN ORDER)		DATE	OF
1. BIDDING NO. DANCIS 69 Q 0002		2. DATE ISSUED 1968 July 29	3. BIDDING/QUOTE NO. 1001/2 (C-69-515)	4. DESIGNED FOR NATIONAL DEFENSE UNDER DEFA REG. 1 AND/OR DMS REG. 1 BIDDING	
5. BUREAU OF DEFENSE SUPPLY SERVICE-WASHINGTON Room 1D 245, The Pentagon Washington, D. C. 20310 Mr. Daniel B. Dawkins FOR INFORMATION CALL (Name and tel. no.) (By collect calls) OXFord 5-0494			6. BUREAU OF (Date) See Sample Contract		
7. BUREAU <input checked="" type="checkbox"/> FOR DISPATCH <input type="checkbox"/> OTHER (See Schedule)			8. DESCRIPTION (Company and address including ZIP code) See Sample Contract		
9. TO FIRM AND ADDRESS []					
10. PLEASE FURNISH QUOTATIONS TO THE BIDDING OFFICE ON OR BEFORE 4:30 p.m. Local time 8/29/68 SUPPLIES ARE OF DOMESTIC ORIGIN UNLESS OTHERWISE INDICATED BY SYMBOL. THIS IS A BIDDING FOR INFORMATION, AND QUOTATIONS FURNISHED ARE NOT OFFERS. IF YOU ARE UNABLE TO QUOTE, PLEASE SO ADVISE ON THIS FORM AND RETURN IT. THIS BIDDING DOES NOT CONSTITUTE THE GOVERNMENT'S INTENTION TO BUY ANY GOODS INCLUDED IN THE SUBMISSION OF THIS QUOTATION, OR TO PROCURE ON CONTRACT FOR SUPPLY OF SERVICES.					
SCHEDULE					
11. BID NO.	12. SERVICES/SERVICES	13. QUANTITY	14. UNIT	15. UNIT PRICE	16. AMOUNT
SERVICES NECESSARY TO COMPLETE THE WORK DESCRIBED IN THE SAMPLE CONTRACT, ATTACHED.					
Total Estimated Cost					
Fixed Fee					
Total Estimated Cost Plus Fixed Fee					
<p>NOTE: THE CERTIFICATION OF NONSEGREGATED FACILITIES IN THIS SOLICITATION. Bidders, offerors and applicants are cautioned to note the "Certification of Non-Segregated Facilities" in the solicitation. The certification provided that if the amount of the bid or proposal exceeds \$10,000, the bidder, offeror or applicant, by signing this bid or offer certifies that he does not and will not maintain or provide for his employees facilities which are segregated on a basis of race, creed, color or national origin, whether such facilities are segregated by directive or on a de facto basis. Failure of a bidder or offeror to agree to the certification will render his bid or offer nonresponsive to the terms of solicitations involving awards of contracts exceeding \$10,000 which are not exempt from the provisions of the Equal Opportunity clause. (Mar. 68)</p>					
17. THESE QUOTES INCLUDE APPLICABLE FEDERAL, STATE, AND LOCAL TAXES.					
METHOD FOR PROMPT PAYMENT: % 10 CALENDAR DATE, % 20 CALENDAR DATE, % 20 CALENDAR DATE, % CALENDAR DATE.					
NOTE: Reverses must also be completed by the offeror.					
18. NAME AND ADDRESS OF QUOTE (Street, city, county, State, including ZIP Code)		19. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION		20. DATE OF QUOTATION	
		21. BIDDER'S NAME AND TITLE (Type or print)		22. TELEPHONE NO. (Include area code)	

Fig. 1.1 ARPA Request for Proposals to build the ARPANet and the BBN proposal to build the first ARPANet nodes

declined to bid, stating their belief that this was an impossible task. The one proposal received, and subsequently funded, came from Bolt Beranek and Newman (BBN), of Cambridge, MA. Not surprisingly, the BBN personnel who wrote the proposal, and went on to build the ARPANET, were a group closely linked to MIT and had developed the switched packet concept for several years preceding. Even so, the BBN team had

September 1968 ARPA had funded a team at Bolt, Baranek and Newman of Cambridge, MA to build the first network processors and install them at UCLA and Stanford (See Figure 1.1). Despite their own doubts that such a system could actually be built, the first processors were installed in 1969, and connected by a 56 KB leased-line between these first nodes ⁵.

Year	Nodes	Events
1969	4	UCLA, Stanford, UCSB, Utah; net 56kb
1970	5	BBN added; net spans U.S.
1971	15	MIT, Rand, Harvard, others added
1974	62	TCP protocol developed
1977	111	Apple II launched as PC
1981	213	Microsoft has 40 employees
1983	562	TCP/IP protocols developed; Internet is born
1984	1,024	Domain names invented (.com)
1986	5,000	First bulletin board with GUI
1987	10,000	25-million PCs sold in US; net is T1 (1.54mb)
1989	100,000	ARPAnet de-installed; now Internet
1992	1,000,000	Mosaic browser developed
2004	Unknown	Internet is a global resource

Fig. 1.2 Nodes on the Net

Even after the initial prototypes had been built and demonstrated, the net did not expand with any great speed, and received little notice outside the scientific and research community. Electronic mail (e-mail) was not even part of the initial ARPAnet concept, and was in fact developed by one contractor employee on his own. Likewise media files and the “web” were never a part of the original concept as well, and it would be some years before these features that revolutionized communications and the media were developed. As Figure 1.2 illustrates, the early years of the net were characterized by relatively few “nodes” and users, largely institutions that were DARPA contractors. The exponential growth of the net was really the result of some other technology developments, the most important of which was the so-called personal computer, or PC. While most early efforts

serious doubts that the system could be built, particularly in the time frame ARPA had specified.

⁵Dr. Kleinrock, then at UCLA, was given the honor of attempting the world’s first login. In a well-known story, he typed in “LOGIN” at which point the system crashed. A recovery was successful, and the first nodes of the net were up and running, with two additional nodes (UCSB and Utah) added later in the year.

to build low-cost computers were failures, or at best resulted in machines that were popular only with hobbyists, the real “breakthrough” came in the form of the Apple II launched in 1977. Within a few years this was followed by the IBM PC, and included an operating system (Microsoft DOS) and applications such as a spreadsheet (VisiCalc) and word processing (Word) that made the PC a useful device for both offices and homes. By the late 1980s millions of PCs were being sold in the U.S. What remained to happen was a means to connect this vast and growing number of computers to the net. A few related technology developments, such as the local area net (LAN); the modem; and the emergence of commercial network service providers (such as Prodigy and AOL) gave the broad population a means to access the net, heretofore limited to a few ARPA researchers. With the passage of the Strategic Computing Act in 1988 the ARPAnet transitioned to the Internet, and funding was provided to advance the use of the net in a wide number of areas ⁶.

1.1.2 A Paradigm Shift and Exponential Growth in Cyberspace

As illustrated above the Internet explosion of the last decade, which is truly a paradigm shift in science and technology, is not the result of a single discovery or event. It is more the convergence of a few separate but related developments taking place at about the same time. It is possible to view this “explosion” in terms of four key technology developments.

Moore’s Law – Cheap Computers for Everybody: Named after Gordon Moore, a co-inventor of the integrated circuit and a founder of Intel, the world entered an era of increasingly cheap and powerful integrated circuits or processors. Intel’s original 8080 series of powerful, low-cost microprocessors and its successors over the years made possible the PC and a myriad of workstations, laptops, PDAs and other devices. The world entered the age of “free hardware.”

Packet Switching: The new era of switched packed communications envisioned by Len Kleinrock, Vint Cerf, Bob Kahn and others brought about a true communications revolution. The computers and the infrastructure were rapidly moving into place. Now they could all be connected into a worldwide network.

Digital Everything: At the same time computers, storage and communications were evolving, the information age was moving rapidly from an

⁶The principal sponsor of this law in the U.S. Senate was Senator Albert Gore, Jr. While Gore later misstated in his unsuccessful Presidential Campaign that he had “invented” the Internet, he was indeed largely responsible for its successful evolution, and the world is indebted to Sen. Gore for this.

analog world into a digital one. Data, voice, video, text, images, movies – it didn't matter. Whatever "it" was, it was now being done in a digital form. For the research community, the major obstacle for generations had been the analog-to-digital conversion. Almost overnight the problem of A/D conversion was vanishing. Analog anything was quickly vanishing.

Infinite/cheap Bandwidth: New developments in communications such as fiber optic cable, advanced RF systems and satellite transponders brought about an economic revolution, if not a technical one as well in worldwide availability of commercial bandwidth. The availability of order-of-magnitude greater, and high-quality bandwidth worldwide caused yet another revolution in the economics of telecommunication. The result was far lower costs, and for Internet users a truly remarkable phenomenon – virtually free worldwide communications. It was now possible to send e-mail, files, and other digital materials to any Internet address, at no marginal cost. Users only needed Internet access ⁷.

The combination of these factors has been a truly exponential growth in cyberspace. The world has moved from one that was only recently dominated by analog systems, paper files, and other technologies dating to biblical times to one now dominated by networked computer systems and digital everything. Communications, information, finance, control, national security and even our social lives are now involved with net-based systems to a greater or lesser extent – and greater in more cases daily. Aside from this being a technological revolution, it has truly become a social, cultural and economic one as well. Using the vernacular, people have really become "hooked" on these capabilities for a number of reasons:

- Free, asynchronous communications (e-mail) has become increasingly popular. It doesn't require the sender and receiver to be on-line at the same time.
- Net-based communications make things easier, not harder. Sending information, documents, photos, etc. immediately, for free, at the click of a mouse has great appeal. In the "old days" people had to print documents, ship documents and files, spend money, and it took time to happen. Better, faster and for free has become very popular – and for good reason.
- The explosive movement of much media to web-based systems has made possible free and low-cost access to a wide range of information. The entire concept of information science, libraries and

⁷The final results of this revolution in the economics of telecommunications have still not been seen. Most carriers evolved on the basis of being able to charge individual users for service. International telex, telephone, FAX, etc. were a major revenue base for these carriers. Since Internet users were now paying nothing to the carriers to send the same (or much more!) data a significant problem has evolved.

research has changed radically.

1.2 Terrorist Use of the Internet

While the first users of “the net” were researchers affiliated with DARPA and the U.S. DoD, Internet use has spread across the globe. Indeed, net use is not only found in the developed world, but even in the most desolate areas of the Third World, and users include people of all ages and from all walks of life – including terrorists. Indeed, as one analyst has written “Cyberspace is not only a nascent forum for political extremists to propagate their messages but also a medium for strategic and tactical innovation in their campaigns against enemies.”⁸

In many ways the Internet and similar networked systems are ideal for terrorist activities and operations. At the most general level, they provide capabilities for worldwide communications and security at exceedingly low cost. This concept is certainly no secret, and recent evidence demonstrates widespread net use by various terrorist organizations worldwide. The analysis below is focused on terrorist use (and abuse) of the Internet in four major areas:

- Use of the Internet for terrorist communications, essentially covert communications, and as a means for a new command and control infrastructure.
- Access to information via the Internet and world wide web (WWW), including for such requirements as information on potential targets as well as technical data in areas such as weapons construction
- Use of the Internet as a platform for the dissemination of propaganda on terrorist groups and causes, and the related objective of recruiting individuals into these organizations
- Terrorist attacks on the Internet, and capabilities connected to the net – commonly known as cyber warfare, as yet another avenue for terrorist attack.

In the Middle East, for example, both secular and Islamist terrorist organizations have increasingly employed net-based systems and practices to achieve their political ends. These capabilities not only provide the terrorists with greater flexibility and security, but also open up a much broader

⁸Col. (R.) Sami Barak, “Between Violence and ‘e-jihad’: Middle Eastern Terror Organizations in the Information Age,” in Lars Nicander and Magnus Ransdorp, *Terrorism in the Information Age – New Frontiers?* (Stockholm, Swedish National Defence College, 2004).

range of opportunities for targeting and attack, due to a diffusion of command and control ⁹.

1.2.1 *Terrorist Use of the Internet for Covert Communications*

It would be truly difficult to envision a more ideal medium for terrorist communications than the modern Internet ¹⁰. As with any other user, today's Internet offers the terrorist asynchronous worldwide service, with global access. The sender and recipient of an e-mail or net-based file transfer can be any place, at any time. How could any self-respecting terrorist ask for more? At the same time, Internet services are close to free and, as previously discussed, available bandwidth is virtually unlimited. For example, the Hamas terrorist organization has for a number of years utilized the Internet to send password-protected files and messages to their members relative to attacks, including maps, photographs, directions, codes and technical details for various operations ¹¹.

To fully appreciate the benefits that the Internet has brought to terrorists in this area it is necessary to consider the obstacles that such groups and individuals face in this area, generally known as "covert communications." As with other covert operatives, such as those in intelligence services or the military, there is a need to communicate reliably and effectively, while avoiding either detection (location) or having ones communications intercepted by hostile forces – which in the case of the terrorists are the intelligence services, military, and law enforcement agencies of target nations. In years past, terrorists and intelligence operatives alike have employed all sorts of methods to communicate, ranging from human (and some non-human) messengers to a wide array of technologies ¹². Virtually all of these

⁹See Michael Whine, "Cyberspace: A New Medium for Communication, Command and Control by Extremists," May 5, 1999 at www.ict.org.il.

¹⁰Digital cell phones and PDAs operating on GSM systems are a useful adjunct to the Internet, but do not offer the same level security and capability at the net. Indeed, the increasing ability of the world's intelligence services to access cell phones has not been lost on the terrorists. They continue to use them, but now do so in ways that minimizes their vulnerability. If nothing else, they change their SIM cards and related numbers with great frequency to avoid detection!

¹¹Col. (R.) Sami Barak, "Between Violence and 'e-jihad': Middle Eastern Terror Organizations in the Information Age," in Lars Nicander and Magnus Ransdorp, *Terrorism in the Information Age – New Frontiers?* (Stockholm, Swedish National Defence College, 2004). See also "Cyber Terrorism," *Foreign Report* (London), September 25, 1997. Hamas leader Abd-al-Rahman Zaydan was convicted in 1995 on the basis of information stored on his personal computer, which included a database linking Hamas squads and terrorists in Israel, Jordan and Germany. Reported in *Yediot Achronot*, January 1, 1996.

¹²Some of these have actually been quite clever, such as using coded messages on the

methods suffered from one or more serious problems:

- They were not reliable, or could not assure the recipient would receive the information, either in a timely manner or at all.
- Almost none were truly secure ¹³. Most telecommunications systems, particularly analog ones, have long been subject to geolocation and intercept by foreign intelligence services. Modern terrorists have come to appreciate this capability and have adjusted their operations accordingly ¹⁴.
- Highly specialized systems used by the military and intelligence services of advanced nations are not commercially available, and the secure systems that are commercially available are costly and relatively cumbersome.

Compared to the early methods, or even the very costly and sophisticated systems used by advanced nations, the Internet is a dream come true. As with any other user, the net provides asynchronous service with global access. The sender and recipient can be any place, at any time, and do not need to link up at a specific time, as would be the case with a telephone call. The cost of net access is close to nothing. For most terrorist communications, bandwidth is not a major issue, so dial-up access is sufficient, and can be accomplished using phone POPs and servers in distant locations. Laptops and other forms of personal computers are widely available throughout the world at low prices. Dial-in access to any number of Internet providers from almost any phone on earth is not costly either ¹⁵. For those terrorists without a computer or a phone line, the proliferation of Internet cafes enables them to access messages with ease. Beyond the low cost of net access, the Internet is probably more reliable than any other system in existence. It is a design feature of switched packet communications. The net degrades by using alternate paths and moving more slowly, rather than

weather forecasts of local radio stations to pass operational signals.

¹³As a practical matter, it has been known for centuries how to generate an unbreakable code for secure communications. This is known as a “one time pad.” Unfortunately, the process is administratively cumbersome, to say the least, since the code or pad needs to be changed for every message, and any message needs to be very short, and not exceed the key length on the pad.

¹⁴Following the attack on the La Belle Disco in Germany by Libyan terrorists, President Reagan authorized the release of communications intelligence information collected by the U.S. against Libya as a part of his justification for retaliatory air strikes against Libya. While it served the political purposes of the time, it also served as a “wake up” call to terrorists that the U.S. was indeed paying considerable attention to their communications, and it was necessary for them to change their mode of operations.

¹⁵Note for example the number of international dial-in points-of-presence or “POPs” that America on Line (AOL) maintains.

simply failing as in the case of line-switched or point-to-point systems ¹⁶.

Access to the Internet itself is accomplished in several ways, including to most common commercial methods and some adjuncts:

High bandwidth, direct connections: From the evidence available, few terrorists themselves have high-bandwidth DSL or similar sorts of direct Internet access that they use for covert communications purposes. It may be the case that specific individuals have some other job that provides them with direct high-speed access, although such cases are probably uncommon. Here it is important to distinguish terrorist operatives conducting covert communications from major terrorist organizations and their affiliates that maintain web sites for propaganda and other purposes, having established sites, servers and direct Internet connections. These are discussed further in Section 1.4 below.

Dial-up services: For the most part, terrorists rely heavily on dial-up services, either using land line or cellular telephone connections. Aside from cost and convenience factors, this method affords an additional layer of security. It is possible to dial a local access number or "POP" from virtually anywhere there is telephone service ¹⁷. The POP is little more than a modem with a phone line, and does not record the phone numbers of incoming calls. As a practical matter, a terrorist can dial a POP in virtually any city, and simply pay the long distance charges, and the net has no way of tracing where any given e-mail actually originated. In remote areas, where there is telephone service but no direct Internet service, this raises some risk, which terrorists appear to be avoiding now by sending disks with their e-mail and data elsewhere for transmission ¹⁸.

Internet Cafes: The proliferation of public Internet access, largely in Internet cafes, has proved popular with terrorists in the Middle East, Africa and elsewhere. Clearly an individual can enter an Internet café, check his or her e-mail at whatever account they are currently using, and depart. Aside

¹⁶In the lore of U.S. Defense Department history it has been said that the ARPAnet was built to provide reliable communications in the case of nuclear war. While it may provide this feature, it simply isn't correct. Switched packet communications began as an experiment in the optimization of network resources, which worked, and not as a program in communications survivability. See here Segaller, Nerds 2.0.1: A Brief History of the Internet., *op. cit.*

¹⁷The GSM systems in use in large parts of the world actually distinguish between voice and data calls, and in many cases only permit data calls on cell phones where there is an established account, rather than the "pre-paid" accounts, where there is no accounting for who has any given cell phone number. This is, however, not universal, and seems to be going away as carriers are fighting for business.

¹⁸Clearly this slows down the process, but avoids a major risk. It appears that this is the method currently being used by Osama bin Laden for much of his communications. Reports in the New York Times in July 2004 from a captured operative indicated that two sets of couriers were bringing his disks to Islamabad, Pakistan for transmission there.

from any appeal as a movie script, this method is certainly low-cost and relatively safe. There are some limitations in terms of file sizes, printers etc., but are quite useful for less complex communications.

Unwitting servers: Hacking into an unwitting server and using it as a covert mail host is a possible technique, but from most evidence is more of a hacker's exercise than a method employed by terrorists with regularity. By and large terrorists can be seen as reasonably intelligent Internet users, but not terribly sophisticated in terms of "hacking" and illicit net uses.

Wireless Internet, and other web-enabled devices: Wireless Internet access has just begun to proliferate in many "advanced" nations, and is not terribly advanced in the Third World as of yet. Certainly wireless access, using computers with 802.11 capabilities for example, will doubtless become increasingly popular with terrorists. It may indeed give new meaning to the term "T-Mobile hot spot." Wireless access has rapidly become available in a wide range of public places, such as coffee shops, airports and others. Such locations have all the advantages of the Internet café, as well as the prospect of greater bandwidth and easier file transfer. Anonymous access, paid for on an hourly, daily or some other basis is readily available, and gives the terrorist user immediate access to any account on any commercial service.

Of particular importance to terrorists, operational security is relatively easy, and can be accomplished in a number of ways. First, the simple proliferation of alias accounts and vast number of servers available throughout the world makes "hiding" among the millions of Internet users easy. As any student knows, getting yet another account on yahoo.com, hotmail.com, or any of the other public servers that have proliferated over the past few years takes only a moment and is cost-free. Such accounts can be used for only a few messages and then discarded in favor of yet other accounts in other alias names. Without good and timely collateral intelligence as to the creation of such accounts and names, it is virtually impossible to keep track of their use. Combined with the fact that the actual message content may be either encoded or using cryptograms of some type, the problem becomes even more difficult. The bottom line here is that it has become increasingly easy for terrorists to hide among the millions of Internet users.

Over the last decade there is evidence that various terrorist organizations have set up Internet servers of their own, in a number of foreign countries under what the intelligence services would call commercial cover. Front organizations are used to purchase net bandwidth and register the necessary domain names. These have been easier to detect, and current evidence suggests that the most sensitive of terrorist communications are conducted using alias accounts with the larger commercial services, discussed above. For some time terrorists and others used services known as

“third party remailers” which were Internet sites that would forward e-mail anonymously, and presumably thwart the ability to trace any particular message to its source. Currently such remailers have gone out of vogue, and the practice of simply using alias accounts appears to be working as well – or better for this purpose.

It is also possible for terrorists to easily encrypt e-mail and files sent over the Internet, using any number of readily available commercial products. This problem is discussed at greater length in Section 1.2.3 below.

1.2.2 *Finding Terrorist E-Mail*

Much of the foregoing discussion focused on the fact that the Internet and e-mail has quickly emerged as an ideal medium for terrorist communications. This raises the immediate question as to how the intelligence services and law enforcement agencies of nations attempting to combat terrorism can locate and hopefully intercept these communications. This is indeed a major intelligence problem, and an area where limited information is available in the public domain. At a general level, it is possible to note that the intelligence services of the U.S. and most Western nations were exceedingly slow to recognize this as a serious problem at all. Indeed, the potential for criminal or terrorist use of new technologies such as the Internet and cellular telephone was largely ignored and greatly under funded for much of the past decade. What exists now can likely be characterized as too little, very late ¹⁹.

While it is possible to fault the Intelligence Community for inadequate attention and insufficient investments in this area, it is also the case that in the long run it may not be possible to accomplish a great deal. There is a fundamental flaw in the American character that says every problem must have a solution, and some corollary that says the solution likely involves technology and money. In this case, it may be close to impossible to find covert terrorist communications sent via e-mail if done “properly.” Here properly means that the terrorists learn and adhere to good operations security (OPSEC) procedures. Access to such terrorist communications in the future will likely depend on errors, sloppy procedures, and collateral intelligence information. Examples here include the following:

Informant data on accounts: To the extent that e-mail account names and data are known only to a very few, and are changed with great regularity, it will be difficult to find the accounts and their communications

¹⁹Actual programs in this area are highly sensitive and Government officials are extremely reluctant to discuss them. The recent U.S. House and Senate investigations of the Intelligence Community, as well as the 9/11 Commission Report, have shed a good bit of new light on the extent of these failing.

²⁰ Where human sources, or other collateral intelligence sources provide such information, accessing the materials in the account becomes less problematic, although the materials in any given account may be encrypted, causing an additional burden.

Intercept of e-mail traffic in target areas: One technique that has been suggested is to look at the switched packet (IP) traffic being carried over commercial basebands in target areas. Without attempting an extensive technical discussion, it is a process that it not likely to yield significant results in the near term.

1.2.3 *The Impact of Encryption*

There are few technology developments that trouble the world's intelligence services more than the proliferation of commercial encryption products. For decades expert code breakers using the most powerful computers of the time had at least some advantages in dealing with the adversaries of the time. Indeed, for most of recent history encryption has been limited to sensitive government and military communications, and has generally been a commercial failure. There are a few obvious reasons for this. In the "analog era" any high-grade encryption systems were: (a) costly; and, (b) imposed an administrative and logistics burden on the user ²¹. Serious encryption required a hardware solution that was both an analog-to-digital converter, as well as a digital encryption device, which was essentially a special purpose computer.

The "digital revolution" discussed above has changed all of this quite radically. With voice, data, and every other type of media now in digital form, and generally in a computer connected to a powerful, high-speed processor, "mixing up the digits" isn't all that much of a problem. All that is really required is a decent encryption algorithm, and these have proliferated as well ²². At the same time user demands have changed as

²⁰It would be technically, legally and politically difficult to comb, for example, all accounts on AOL, Yahoo, or Hotmail seeking some that may have been used by terrorists. Where data in the accounts is encrypted, the situation becomes even more difficult. Indeed, there isn't enough electric power in the U.S. to decrypt all the encrypted material on the commercial Internet services today.

²¹Note that the famed World War II German "Enigma" code machine was originally developed by Scherbius for the commercial market. This was a completed failure, going bankrupt in the process, and his machine was taken over by Hitler's SS for military purposes.

²²For some years the U.S. stuck to a policy that is best described as silly, in trying to solve the problem by restricting export of encryption algorithms that were freely available on the Internet, and the export of commercial software products that were freely available at any software store. If a high school kid can buy it with their allowance, presumable the "bad guys" could do so as well! The net result was that foreign suppliers have come

well. Commercial firms and private citizens alike have become more sophisticated computer users, and are now demanding privacy and security. The increased use of the Internet for commercial transactions, many involving credit cards, and the corresponding proliferation of computer fraud have greatly heightened sensitivity in this area. The use of secure web protocols (e.g., <https://>) and encrypted file transfers is becoming commonplace. A few critical trends in this area are worthy of note:

- **No marginal cost to users:** Users of secure web protocols and even security certificates for Internet transactions are not incurring any real cost. While some security certificates need to be purchased on an annual basis, for a truly nominal cost, others are available on the net for free – with a quality equal to that of the types being sold.
- **No marginal effort involved:** Secure use of the Internet requires little or no additional effort on the part of users. Secure web protocols function automatically, and once security certificates are installed on a computer their use is largely automatic as well. The days when security required a dedicated “code clerk” and great inconvenience are long gone.
- **Transition to secure applications:** While the current generation of commercial software products is not quite there yet, the world is moving rapidly toward an era where encryption will be an integral part of most applications (e.g., word processing, spread sheets, communications, etc.), and files will be saved and transferred in an encrypted form ²³. Security will become seamless process largely transparent to the user.
- **Security at multiple levels:** In the not too distant future security will actually take place at multiple levels. Files generated by application software will be “saved” on hard drives and other media in an encrypted form; data transferred over the Internet and other local area nets will be encrypted for transmission, using security certificates or other secure protocols; and the Internet basebands themselves will be bulk encrypted. There are no major technical, economic or legal barriers. The era of encrypted everything is rapidly approaching.

For intelligence services and law enforcement agencies seeking to find terror-
to dominate this world market.

²³Just as it is impossible to market a word processing program without a spell checker, for example, future packages will contain file encryption as an essential feature. Consumers will demand it, and it costs the software vendor essentially nothing to add it in the package. Encryption will become seamless and transparent to the user.

ists, spies, criminals and others this is a troublesome future. It is no longer a world where only a small number of encrypted communications existed. Everything will be encrypted. That battle is over. The two remaining questions are:

- Can encrypted communications or files of interest be located at all?
- Will it be possible to decrypt terrorist communications in a timely and cost effective manner so that they are of use?

This is still an area where very little has been published addressing these critical issues in any serious way. It is, however, possible to consider how the available technologies are driving the longer-term answers. First, finding any communications of interest in what is becoming a vast sea of encrypted digital bits and packets will become an ever-daunting task. Using a brute force approach and trying to search a mass of data collected from the network carriers is not likely to be highly productive²⁴. At a minimum, it will be necessary to have some “external” indication of the source or recipient of the data. On the other hand, the closer it is possible to get to the source (or recipient) through various means, it is possible to narrow the search considerably. In July 2004, for example, the seizure of several computers used by the al Qaeda in Pakistan made it possible to examine the hard drives for stored messages and files²⁵.

The answer to the second question is even more problematical. Truly low-grade encryption is a thing of the past. The widespread availability of powerful digital processors and good encryption algorithms has put an end to this. The actual difficulty in “breaking” any encrypted file or message really relates to the specific algorithm and key length used²⁶. Even where access is technically possible, the resources required in terms of computer time and manpower are likely to be significant. This alone will severely limit the amount of access. For the world’s intelligence services this is clearly not a happy thought, but the golden era of largely unbridled access is over.

²⁴It is hard to find any good estimates of the actual volume of digital data on the net now, but some attempts put this currently on the order of several exabytes, and increasing rapidly.

²⁵This is not the first time that U.S. authorities or their colleagues in friendly states have been able to seize computers belonging to terrorists, drug lords, or other key targets. In several cases these targets have been either foolish or sloppy enough to leave files on these computers in a non-encrypted form. In others, their operators have furnished information during interrogation to enable decryption of the stored files.

²⁶In an effort to enable access to encrypted files, the U.S. has attempted to restrict the key length or number of “bits” in any commercial system. This has been largely abortive, and has simply served to drive the commercial security market offshore. Some of the best commercial software, for example, is now being marketed by some former KGB personnel, who have established themselves in Ireland – largely for tax reasons and business incentives provided by the Irish.

