

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1320646-0

Total Deleted Page(s) = 29
Page 45 ~ Referral/Consult;
Page 46 ~ Referral/Consult;
Page 111 ~ b6; b7C;
Page 124 ~ Referral/Consult;
Page 125 ~ Referral/Consult;
Page 126 ~ Referral/Consult;
Page 127 ~ Referral/Consult;
Page 128 ~ Referral/Consult;
Page 140 ~ b6; b7C; b7E;
Page 141 ~ b7E;
Page 142 ~ b7E;
Page 143 ~ b7E;
Page 144 ~ b7E;
Page 145 ~ b7E;
Page 146 ~ b7E;
Page 147 ~ b7E;
Page 148 ~ b6; b7C; b7E;
Page 149 ~ b7E;
Page 150 ~ b6; b7C; b7E;
Page 151 ~ b6; b7C; b7E;
Page 152 ~ b7E;
Page 153 ~ b7E;
Page 154 ~ b7E;
Page 155 ~ b7E;
Page 156 ~ b7E;
Page 159 ~ b6; b7C;
Page 160 ~ b6; b7C;
Page 161 ~ b6; b7C;
Page 162 ~ b6; b7C;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

288-NY-268557-19

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

CM

CM

SAC

REFERENCE: WHAT GO ARTICLE FOR PRICE UNIVERSITY

electronic Civil Disobedience

This page is an archive for the Electronic Disturbance Theater.

[Click here](#) for Electronic Disturbance Theater homepage and ECD actions.

11.xx.98 [Electronic Civil Disobedience and the World Wide Web of Hacktivism:
A Mapping of Extraparliamentarian Direct Action Net Politics](#) NEW!

10.31.98 New York Times: ['Hacktivists' of All Persuasions Take Their Struggle to the Web](#)

10.26.98 Ottawa Citizen: [E-Guerrillas in the mist](#)

10.15.98 *Electronic Disturbance Theater at Harvard Law School*

- [Presentation to Berkman Center for Internet and Society](#)
- [Notes on Internet and Society class](#)
- [Audio of Internet and Society class, Part 1](#)
- [Audio of Internet and Society class, Part 2](#)
- [Web site for Internet and Society class](#)

10.12.98 [Electronic Disturbance Theater Presentation, Audio File](#)

09.26.98 [Reason for moving main ECD page to the Thing's server](#)

09.10.98 [SWARM Chronology](#)

09.08.98 [Email Message from DISA to NYU Computer Security](#)

09.xx.98 [The Zapatista Tactical FloodNet](#)

09.xx.98 [The Ante-Chamber of Revolution: A Prelude to a Theory of Resistance and Maps](#)

08.05.98 [Bottom Up Information Warfare Theory and Practice Version 1.0](#)

08.01.98 [Paris Salon or Boston Tea Party: Recasting Electronic Democracy](#)

07.07.98 [Rhizomes Nomads and Resistant Internet Use](#)

06.17.98 [The Electronic Disturbance Theater and Electronic Civil Disobedience](#)

[Handwritten signature]

06:xx.98 *SWARM: An ECD Project for Ars Electronica '98*

05.05.98 *Die Umwandlung des Widerstands der Maschinenstürmer in einen virtuellen Widerstand*

05.01.98 *For Their Civil Disobedience, the 'Sit-In' Is Virtual*

05.01.98 *A Contribution to the Discussion of Electronic Civil Disobedience*

04.29.98 *Electronic Disturbance Theater Response to A Dirty War in Internet*

04.27.98 *A Dirty War in Internet (analysis)*

04.07.98 *Transforming Luddite Resistance into Virtual Luddite Resistance*

03.20.98 *On Electronic Civil Disobedience*

03.20.98 *Digital Zapatismo*

03.20.98 *How to Jam an Opponent's Fax Machine*

02.04.98 *Mexico Rebel Supporters Hack Government Home Page*

01.18.98 *Call Virtual Sit-ins at Five Mexico Financial Web Sites*

01.01.98 *Intercontinental Cyberspace Liberation Army Declares Netwar Against Mexican State*

09.xx.97 *Photos of U.S. Embassy in Mexico City*

08.xx.97 *Recombinant Networks*

08.xx.97 *The Drug War and Information Warfare in Mexico*

xx.xx.96 *Information Warfare section of The Revolution Will Be Digitized*

wray home



Electronic Civil Disobedience and the World Wide Web of Hacktivism:

A Mapping of Extraparliamentarian Direct Action Net Politics

by Stefan Wray

A paper for:

The World Wide Web and
Contemporary Cultural Theory Conference

Drake University, November 1998

Contents

Introduction
Computerized Activism
Grassroots Infowar
Electronic Civil Disobedience
Politicized Hacking
Resistance To Future War
Emerging Critiques of Direct Action Net Politics
Conclusion
End Notes

Introduction

In the next century when cyber-historians look back to the 1990s they will

recognize 1995 as the year of the graphical browser, the year the Internet began to be overshadowed by the Web. But they will probably also view 1998 as an important moment -- in the history of the browser wars. At a minimum, 1998 will be noted for the emergence of two terms that represent similar phenomena: electronic civil disobedience and hacktivism. In that year, a Net based affinity group called the Electronic Disturbance Theater pushed and agitated for new experimentation with electronic civil disobedience actions aimed mostly at the Mexican government. It engaged its FloodNet software and invited participation to an international set of artists, digerati, and political activists to make a "symbolic gesture" in support of Mexico's Zapatistas. While at the same time, in Britain, in Australia, in India, in China, on almost every continent there were reports of hacktivity. In the spring of 1998 a young British hacker known as "JF" accessed about 300 web sites and placed anti-nuclear text and imagery. He entered, changed and added HTML code. At that point it was the biggest political hack of its kind. Since then, and increasingly over the course of the year, there were numerous reports of web sites being accessed and altered with political content.

Taken together we may consider both the more symbolic electronic civil disobedience actions and the more tangible hacktivist events under the rubric of extraparliamentarian direct action Net politics, where extraparliamentarian is taken to mean politics other than electoral or party politics, primarily the grassroots politics of social movement. By no means was 1998 the first year of the browser wars, but it was the year when electronic civil disobedience and hacktivism came to the fore, evidenced by a front page New York Times article on the subject by the end of October. Since then the subject has continued to move through the media sphere. [1]

What this paper attempts to do is examine these emerging trends from a slightly wider angled lens. This paper puts forth five portals for consideration: computerized activism, grassroots infowar, electronic civil disobedience, politicized hacking, and resistance to future war. At first they were conceived as five portals into Hacktivism, but perhaps they better serve as five portals for looking at the wider world of extraparliamentarian direct action Net politics, although that phrase is admittedly awkward. Nevertheless, these five portals seem to provide a useful starting point for a more in-depth, yet to come, examination of the convergence of activism, art, and computer-based communication and media. In addition to starting to define, to frame, and to contextualize contemporary hacktivity, in terms of its roots, its lateral dimension, and its trajectory, this paper also asks some nascent questions of a political, tactical, technological, ethical, and legal nature and makes some preliminary claims about the likely direction of these various movements.

Computerized Activism

Computerized activism exists at the intersections of politico-social movements and computer-mediated communication. The origins of computerized activism extend back in pre-Web history to the mid 1980s. As an example, the first version of PeaceNet appeared in early 1986. PeaceNet enabled - really for the first time - political activists to communicate with one another across international borders with relative ease and speed. [2] The advent of newsgroup services like PeaceNet,

and wider dispersal of other Bulletin Board Systems, email lists, and gopher sites characterizes the cyber-environment within which most early on-line political activists found themselves. This largely text-based environment persisted up until as late as 1994 and 1995 when the first GUI browsers were introduced. Even today, while Web sites augment these earlier forms, email communication remains a central device in the international circulation of struggle and the creation and maintenance of international solidarity networks. [3]

During the early to mid 1980s the subject of computer-mediated communication (CMC) was taken up by scholars in, for example, psychology and sociology. When communication scholars began to examine CMC, and in particular when they began to assess the juncture of political communication and CMC, a number of academic treatments of "electronic democracy" were written in which politics is positioned narrowly within the confines of electoral or parliamentarian politics. [4] Among the earliest treatments of CMC from among communication scholars who entertain extraparliamentarian or grassroots politics is by Downing in "Computers for Political Change." [5] Not surprisingly, PeaceNet is one of his case studies. For purposes of tracing the origins of more current cross-border email exchange and its role in creating and maintaining international solidarity networks, Downing points to PeaceNet's establishment of international links in 1987. Among early adopters of these means of communication were people in the 1980s anti-nuclear and Central American solidarity movements.

By the late 1980s and the very beginning of the 1990s, the significance of cross-border, international, email communication began to be realized. The international role of email communication, coupled to varying degrees with the use of the Fax machine, was highlighted in both the struggles of pro-democracy Chinese students and in broader trans-national movements that lead to the dissolution of the Soviet Union. Shortly thereafter, we began to see scholarly work on this subject. Harasim's "Global Networks: Computers and International Communication" began to theorize about the role of international email communication in linking together the world. [6]

Computerized activism remained marginal to political and social movements until the explosion of the Internet in the early to mid 1990s and more so until the arrival of the graphical browser in 1994 and 1995. Now, in the post-Web Internet phase there is widespread use of these media forms by a plethora of grassroots groups and other political actors in countries all over the world. [7]

A common thread or understanding that runs through various types of politically based computer-mediated communication, from early BBS systems, to email listservs, and to sophisticated Web sites with fancy bells and whistles, seems to be an overarching dominant paradigm that privileges discourse, dialogue, discussion and open and free access. This observation becomes important when looking more at electronic civil disobedience and politicized hacking, because it is with this dominant paradigm of the Habermasian Web that these later forms conflict and cause friction.

So the first portal of Computerized Activism is important for understanding the roots of today's extraparliamentarian, more direct action focused, political CMC. It is the portal that has been with us the longest, and the portal within which most

political actors on the Net feel the most comfortable. Computerized activism, defined more purely as the use of the Internet infrastructure as a means for activists to communicate with one another, across international borders or not, is less threatening to power than the other types of uses we see emerging in which the Internet infrastructure is not only a means toward or a site for communication, but the Internet infrastructure itself becomes an object or site for action. This transgression, or paradigmatic shift in thinking, of moving away from believing the Internet solely as communication device to Internet as communication device and site for action is dealt with incrementally in the next four sections.

Grassroots Infowar

Grassroots infowar is an intensification of computerized activism. Infowar here refers to a war of words, a propaganda war. Grassroots infowar is the first step, the first move away from the Internet as just a site for communication and the beginning of the transformation from word to deed. Grassroots infowar actors emerge fully cognizant they are on a global stage, telepresent across borders, in many locations simultaneously. There exists a sense of immediacy and interconnectivity at a global level. More than a mere sharing of information and dialogue, there is a desire to push words towards action. Internet media forms become vehicles for inciting action as opposed to simply describing or reporting.

In the early 1990s, following the U.S. directed "smart" bombardment of Iraq and following the dissolution of the Soviet Union and the subsequent uselessness of Cold War rhetoric as a rationalization for foreign intervention, the U.S. military-intelligence community, along with its allies in financial-corporate sectors, needed to craft a new military doctrine. Their answer was Information Warfare and the threat of info-terrorism. State-side scholars at RAND, a think tank in Santa Monica, California, that often does the military's "thinking", set about devising new theoretical constructs that would lay the basis for their version of Information Warfare. In 1993, under the RAND banner, Ronfeldt and Arquilla wrote *Cyberwar is Coming!* This work sets out the distinctions between netwar and cyberwar and is cited by nearly every subsequent treatment of Information Warfare theory. [8] Where netwar refers more to the war of words, the propaganda war that exists on the Internet itself, cyberwar refers to cybernetic warfare, war dependent on computers and communications systems, the war of C4I - Command, Control, Communication, Computers, and Information.

Not long after RAND's theoretical intervention, pragmatic cases of netwar appeared. Among the most celebrated is the case of Mexico's Zapatistas and the international community of supporters that quickly brought that struggle on to the Internet. With the global pro-Zapatista Internet experience there began to be a rethinking or an interrogation of RAND's theoretical constructs, albeit from a more radical grassroots perspective. Some of this recasting has been brought forth in pieces by Harry Cleaver, a professor at the University of Texas at Austin and key person behind the Chiapas95 project, an email-based news and information distribution service. Probably Cleaver's most well known work in this regard is "The Zapatistas and the Electronic Fabric of Struggle." [9]

Despite some radical interventions and attempts to reframe dominant forms of

military and intelligence Information Warfare theory, most of the material, not surprisingly, is produced by the likes of RAND, the National Defense University, the Department of Defense, the US Air Force, or private sector initiatives. The meme of Information Warfare seems to have spread and been promulgated largely through network security paranoics and others keen on guarding digital property. But there are signs that Information Warfare is spreading to other areas. This year Information Warfare hit the international digital arts community by being the main subject of the annual Ars Electronic Festival in Linz, Austria. [10]

Theorizing about grassroots or bottom-up Information Warfare doesn't nearly get as much attention as the dominant models and as a consequence there is not much written on the subject. [11] The case of the global pro-Zapatista networks of solidarity and resistance offers a point of departure for further examination of grassroots infowar. One feature of Zapatista experience over the course of the last 5 years is that it has been a war of words, as opposed to a prolonged military conflict. This is not to say there isn't a strong Mexican military presence in the state of Chiapas. Quite the contrary is true. But fighting technically ended on January 12, 1994 and since then there has been a ceasefire and numerous attempts at negotiation. [12] What scholars, activists, and journalists, on both the left and the right, have said is that the Zapatistas owe their survival at this point largely to a war of words. This war of words, in part, is the propaganda war that has been successfully unleashed by Zapatista leaders like Subcommandante Marcos as well as non-Zapatista supporters throughout Mexico and the world. Such propaganda and rhetoric has, of course, been transmitted through more traditional mass communication means, like through the newspaper La Jornada. [13] But quite a substantial component of this war of words has taken place on the Internet. Since January 1, 1994 there has been an explosion of the Zapatista Internet presence in the forms of email Cc: lists, newsgroups, discussion lists, and web sites. [14]

A primary distinction, then, between earlier forms of computerized activism and forms of grassroots infowar is in the degree of intensity. Coupled with that is the degree to which the participants are noticed and seen as a force. Given the Zapatistas relatively high profile in Mexican society over the course of the last five years, and given the fact that they are technically a belligerent force negotiating with a government, the Internet activity surrounding them takes on a different significance than, say, for example, the Internet activity of the Sierra Club, Amnesty International, or other similar venture.

An important difference is that in grassroots infowar comes the desire to incite action and the ability to do so at a global scale. At the end of 1997, news of the Acteal massacre in Chiapas, in which 45 indigenous people were killed, quickly spread through global pro-Zapatista Internet networks. Within a matter of days there were protests and actions at Mexican consulates and embassies all over the world. [15] This incident, too, is now seen as a turning point in the stance by some toward the Internet infrastructure. While prior to this moment, there had been few if any incident reports of pro-Zapatista hacktivity, following there has been a shift, the beginning of the move toward accepting the Internet infrastructure as both a channel for communication and a site for action.

Electronic Civil Disobedience

Acting in the tradition of non-violent direct action and civil disobedience, proponents of Electronic Civil Disobedience are borrowing the tactics of trespass and blockade from these earlier social movements and are experimentally applying them to the Internet. A typical civil disobedience tactic has been for a group of people to physically blockade, with their bodies, the entranceways of an opponent's office or building or to physically occupy an opponent's office -- to have a sit-in. Electronic Civil Disobedience, as a form of mass decentered electronic direct action, utilizes virtual blockades and virtual sit-ins. Unlike the participant in a traditional civil disobedience action, an ECD actor can participate in virtual blockades and sit-ins from home, from work, from the university, or from other points of access to the Net. [16]

The phrase "Electronic Civil Disobedience" was coined by a group of artists and theorists called the Critical Art Ensemble. In 1994 they published their first book that dealt with this subject, "The Electronic Disturbance," followed two years later by "Electronic Civil Disobedience and Other Unpopular Ideas." [17] Both of these works are devoted to a theoretical exploration of how to move protests from the streets onto the Internet. They examine the tactics of street protest, on-the-ground disruptions and disturbance of urban infrastructure and they hypothesize how such practices can be applied to the Internet infrastructure.

Before 1998, Electronic Civil Disobedience remained largely as theoretical musings. But after the 1997 Acteal Massacre in Chiapas, there was a shift toward a more hybrid position that views the Internet infrastructure as both a means for communication and a site for direct action. This shift distinguishes more sharply the third portal of Electronic Civil Disobedience from the first and second portals.

Electronic Civil Disobedience is the first transgression, making Politicized Hacking the second transgression and Resistance to Future War the third. Each succeeding transgression moves the stance toward the Internet infrastructure further away from the public sphere model and casts it more as conflicted territory bordering on a war zone. Where the former more discursive model is perhaps a manifestation of Habermas's Paris Salon, the latter may have roots in the Boston Tea Party. [18]

The realization and legitimization of the Internet infrastructure as a site for word and deed opens up new possibilities for Net politics, especially for those already predisposed to extraparliamentarian and direct action social movement tactics. In early 1998 a small group calling themselves the Electronic Disturbance Theater had been watching other people experimenting with early forms of virtual sit-ins. The group then created software called FloodNet and on a number of occasions has invited mass participation in its virtual sit-ins against the Mexican government. [19]

EDT members Carmin Karasic and Brett Stalbaum created FloodNet to direct a "symbolic gesture" against an opponent's web site. FloodNet is a Web-based Java applet that repeatedly sends browser reload commands. [20] In theory, when enough EDT participants are simultaneously pointing the FloodNet URL toward an opponent site, a critical mass prevents further entry. Actually, this has been rarely attained. Given this, perhaps FloodNet's power lies more in the simulated

threat.

On September 9, 1998, EDT exhibited its SWARM project [21] at the Ars Electronic Festival on Information Warfare, where it launched a three-pronged FloodNet disturbance against web sites of the Mexican presidency, the Frankfurt Stock Exchange, and the Pentagon, to demonstrate international support for the Zapatistas, against the Mexican government, against the U.S. military, and against a symbol of international capital. [22]

But within several hours of activating project SWARM, FloodNet was disabled. On web browsers Java coffee cups streamed quickly across the bottom of the screen and FloodNet froze. Participants began to send email with word of trouble. Later that day a Wired writer learned from a Department of Defense spokesperson that the DOD had taken some steps against FloodNet. At the same time, an EDT co-founder received email that the Defense Information Systems Agency had complained about his ECD web site content. [23]

Globally, 20,000 connected to the FloodNet browser on September 9 and 10. This action reverberated through European media. It was later picked up by Wired, ZDTV, Defense News, and National Public Radio, among others. On October 31 EDT made the front page of the New York Times. The story continued to unfold. More interest from the media sphere. On November 22, EDT called for FloodNet against the School of the Americas. [24] As part of EDT's grande finale for the 1998 season, the group plans to release a public version of FloodNet at 12:01 a.m. on January 1, 1999.

Politicized Hacking

Again mentioning Mexico, in addition to the Electronic Civil Disobedience style action directed at the surface, at the web site entranceway, there have also been in 1998 actual hacks into Mexican government web sites where political messages have been added to those sites. [25] This particular tactic of accessing and altering web sites seems to have been the popular tactic for this year. Probably one of the most well known examples of this is the story of the young British hacker named "JF" who hacked into around 300 web sites world wide and placed anti-nuclear imagery and text. This method has been tried by a number of groups. October issues of the Ottawa Citizen and the New York Times did a decent job of capturing a number of these examples as they described this new trend. [26]

One main distinction between most Politicized Hacking and the type of Electronic Civil Disobedience just mentioned is that while ECD actors don't hide their names, operating freely and above board, most political hacks are done by people who wish to remain anonymous. It is also likely political hacks are done by individuals rather than by specific groups.

One of the reasons for the anonymity and secrecy is that the stakes are higher. Where proponents of forms of electronic civil disobedience actions are perhaps in an ambiguous area of law, certain types of political hacks used to varying degrees of success are unquestionable illegal. Few will question the legality of actually entering into an opponent's computer and adding or changing HTML code.

This distinction speaks to a different style of organization. Because of the more secret, private, low key, and anonymous nature of the politicized hacks, this type of activity expresses a different kind of politics. It is not the politics of mobilization, nor the politics that requires mass participation. This is said not to pass judgement, but to illuminate that there are several important forms of direct action Net politics already being shaped.

As touched on already, depending on the conception of politics, politicized hacking is either a recent phenomena or one that can be traced back to hacking's origins. For the purposes of creating a portal to look into this world of extraparliamentarian direct action Net politics, it may be useful to consider both perspectives. There is clearly something political about early hackers' desires to make information free. It probably would be useful to examine the history of early to mid 1980s hacking to look for more political origins of today's hacktivism. The computerized activism of the mid to late 1980s existed alongside the first generation of hackers. There may have been cross-over then.

The contemporary conception of hacktivism seems to concern itself more with overtly political hacking. It is such a recent development that journalists have only barely begun to discover it, while scholars have had little time to consider it. There are numerous web sites devoted to hacking, but very few are devoted to Hacktivism per se. Although, one web site devoted to Hacktivism was created in the fall of 1998 by a group called The Cult of the Dead Cow. [27]

An important fact to realize and emphasize is that hacktivism, current forms of politicized hacking, is very much in its infancy. It is too early to draw definitive conclusions or to make strong predictions as to the direction it will take. Perhaps we can point to certain trajectories and make some logical projections. But we need to remember that at this point there is no consensus or agreement. Maybe the entire notion of hacktivism confuses and challenges sets of values and hacker codes of ethics. Quite possibly there is some re-thinking happening and we might begin to see a new set of ethical codes for hacking. [28]

Resistance to Future War

Some call the 1990-1991 Gulf War the first Information War because of the heavy military reliance on information and communication technology. The Gulf War was a pinnacle of achievement for the weapons industry, a chance to battle test sophisticated hardware that had been developed and manufactured under the Reagan and Bush presidencies. The weapons systems were dependent, as were all communications, on a major telecommunications infrastructure involving satellite, radar, radio, and telephone. The "smart" bombs were just the most mentioned of the sophisticated weaponry that was showcased during the made-for-CNN war.

Although significantly under-reported by mainstream U.S. media, there was sizeable domestic opposition to the Gulf War, both prior to and especially during the first days of U.S. bombing of Iraq. In San Francisco the first three days of the Gulf War are referred to as the Three Days of Rage. During that period demonstrators filled, occupied, and controlled the streets and in some cases bridges

and highways in the greater San Francisco Bay Area. Similar disruptions happened up and down the west coast and all across the country. There was widespread grassroots resistance to the U.S. bombardment of Iraq in January 1991. [29]

One part of that history is the role of information and communication technology, not just for the military forces, but also for the grassroots resistance. If the Gulf War is indicative of a paradigmatic shift toward the practice of Information Warfare, then it's also useful to look at the way in which ICT enabled resistance to the war effort. Some people within the opposition to the 1990-1991 Gulf War used email to communicate and they learned about resistance in other cities through Bulletin Board Systems and newsgroups. Others without computer access used fax and telephone. But many people had no connection to computers and received nothing by fax, instead they came out into the streets because of seeing posters or by hearing announcements on TV or on radio, or through word of mouth. It is safe to say that the Internet played only a marginal role in spreading news and moving people into action. The opposition to the war also watched CNN just like everyone else.

But that was the end of 1990 and the very beginning of 1991, 8 years ago at the time of this writing, and in a pre-Web phase and even pre-Internet phase. Yes, by then the PC revolution had exploded and more and more people were buying modems, but the Gulf War is clearly positioned in the pre-boom days of the Internet in the United States. An interesting question is what would happen today, or moreover, what might happen tomorrow or in the near future, if presented with a similar set of circumstances. What if, for example, a Gulf War-like scenario emerged at the end of the year 2000 and the beginning of 2001? Suppose the United States decided to engage in what became an unpopular war, what might hacktivism look like in a condition of more generalized resistance? Or said another way, what might generalized resistance look like with the condition of hacktivism?

The above is what is meant to be asked by suggesting that Resistance to Future War is the fifth portal into direct action Net politics. Where might this all lead? Until now, incidents of hacktivity have been sporadic and basically unconnected. Hacktivist events have been singular and not connected to a set of simultaneous occurrences. Perhaps the Electronic Disturbance Theater's work demonstrates the possible of waging a campaign on the Internet, and sustaining a presence over a period of time. But the group's one goal of a SWARM has yet to be achieved. Maybe it is useful to think of the SWARM metaphor in the consideration of Resistance to Future War.

Perhaps a SWARM is a convergence of generalized resistance, referring to a situation in which there are not just isolated cases, or several pockets of opposition, but when there is across-the-board resistance occurring at a number of different levels and happening in cities and town all across the country, all at the same time. Such was the case during moments of domestic Gulf War resistance. There was simultaneous outpouring of people into the streets who engaged in quite a range of activity, both legal and illegal. A multitude of tactics were being used at the same time but without any central command or directing orders from above. Incidents of such upsurge are rare. But they undoubtedly will occur again. What will hacktivism look like then? What of it when hacktivism moves from isolated

incidents to a convergence of allied forces? Is this when hacktivism ceases to be and becomes cyberspatial resistance? While it may be too early to make accurate predictions, it seems true that the force or power of hacktivism has yet to be fully recognized or tested. Yet before getting lost in futuristic science fiction, consider some critiques.

Emerging Critiques of Direct Action Net Politics

There is no consensus among social and political activists regarding electronic civil disobedience, political hacking, hacktivism, or more generally extraparliamentarian direct action Net politics. It may in fact be too early to judge or to make definitive claims about these new tactics. But some critiques have co-developed along with the development of these new methods. They point to some basic questions over the effectiveness and appropriateness of these forms of electronic action.

In an emerging discourse on several email listservs, that is too complicated to treat fairly in such a short piece as this one, there have been periodic criticisms raised both generally and specifically about aspects of the above mentioned tactics. [30] By no means can this piece attempt to describe and comment on all criticisms being raised about hacktivism et al, but it can at least address several of the criticism raised that seem most important. As already stated there are critiques aimed at the effectiveness and the appropriateness of cyber-protests. In terms of effectiveness three closely related types of questions have appeared regarding political, tactical, and technical effectiveness. Concerning appropriateness there are ethical questions, that may be also considered as political questions, and of course there are legal questions. Some of the legal concerns raise issues of enforceability and prosecutability.

Political and tactical effectiveness are closely intertwined. Are these methods of computerized activism effective? The answer to which is that it depends on how effectiveness is defined. What is effective? If the desired goal of hacktivism is to draw attention to particular issues by engaging in actions that are unusual and will attract some degree of media coverage, then effectiveness can be seen as being high. If, however, effectiveness is measured in terms of assessing the actions ability to be a catalyst for fomenting a more profound mobilization of people, then probably these new techniques are not effective. This distinction then, perhaps, is important. Hacktivism is not likely to be an organizing tool and the end result of hacktivity is not likely to be an increase in the ranks of the disaffected. Rather hacktivism appears to be a means to augment or supplement existing organizing efforts, a way to make some noise and focus attention.

Technical critiques of hacktivism at the level of computer code are another way of addressing the efficacy of these new methods. Undoubtedly there will be disagreement as to how effective a particular technique is or isn't. But it seems that if new methods are created in an environment of experimentation, then valid critiques will be taken into consideration and used to redesign or alter plans and strategies. However, there are some technical critiques that are actually much more ideologically based than it would first seem. For example there is a certain tendency to reify bandwidth and from that viewpoint any action that clogs or

diminishes bandwidth is considered negative. So then, technical critiques can be value-laden with particular stances toward the Internet infrastructure.

Despite the current levels of political, tactical, and technical questions that are being raised about hacktivism et al, it seems to be an area that is in a period of expansion, rather than contraction. And it generally seems that this critique and questioning is healthy and useful for the refinement of the practice.

As just mentioned, some technical critiques are bound together with ideological pre-dispositions and are therefore also political questions, and perhaps even ethical questions of appropriateness. To judge blocking a web site, or clogging the pipelines leading up to a web site, is to take an ethical position. If the judgement goes against such activity, such an ethical position is likely to be derived from an ethical code that values free and open access to information. But there are alternative sets of values that justifies, for example, the blocking of access to web sites. These differences in beliefs over the nature of the Internet infrastructure are among people who are basically on the same side when it comes to most political questions. Some of these differences will probably be worked out as the subject and practice matures, while there may remain clear divisions.

Last but not least, the more prosecutorial minded are apt to pass judgement on the appropriateness or inappropriateness of certain forms of hacktivism based on where the actions stand with respect to the law. While it is true that some forms of hacktivity are fairly easy to see as being outside the bounds of law - such as entering in to systems to destroy data - there are other forms that are more ambiguous and hover much closer to the boundary between the legal and the illegal. Coupled with this ambiguity are other factors that tend to cloud the enforceability or prosecutability of particular hacktivist offenses. Jurisdictional factors are key here. The nature of cyberspace is extraterritorial. People can easily act across geographic political borders as those borders do not show themselves in the terrain. Law enforcement is still bound to particular geographic zones. So there is a conflict between the new capabilities of political actors and the old system to which the law is still attached. This is already beginning to change and legal frameworks, at the international level, will be mapped on to cyberspace.

This section does not do justice to the full range of critiques that can be identified and described. And further exploration of the subject of direct action Net politics should make sure such a deeper analysis is taken. The intention here has been more so to develop a greater understanding of these new forms of electronic action and to only mention a few overarching critiques so as to not give the impression that this is moving forward without resistance. Quite the contrary is true. It seems that hacktivity has met and will meet resistance from many quarters. It doesn't seem as if opposition to hacktivist ideas and practices falls along particular ideological lines either.

Conclusion

Several things seem to be clear at this point. The first is that hacktivism, as defined across the full spectrum from relatively harmless computerized activism to potentially dangerous resistance to future war, is a phenomena that is on the rise.

Second, as just eluded to, hacktivism represents a spectrum of possibilities that exists in some combination of word and deed. On the one end of the spectrum is pure word. On the other end of the spectrum is pure deed. Computerized activism hovers closer to pure word, while the successive portals moves closer toward pure deed. Third, along with this tendency towards transgression, towards giving value to actions that move beyond words and that sees the Internet infrastructure also as a site for action, there comes with this a critique and resistance. But, despite this critique hacktivism is likely to continue to spread, but perhaps modified to accommodate some of the criticism. Fourth, with its continued spread, modified by critique or not, hacktivism is also likely to continue to gain attention. While media coverage may eventually drop off if or when hacktivism becomes more commonplace, at this point the way in which hacktivism is being represented is still new enough to warrant media attention for the foreseeable near future.

What remains unclear about hacktivism emerges when we start to ask questions like: what does this mean and where is this going? While we can claim with a fair degree of certainty that hacktivism is on the rise, there is little way to tell where it will lead to and the significance or lack thereof that it will or might obtain. Moreover, there are aspects of hacktivism that still need to be explored. For example, the entire issue of extraterritoriality, of the Internet not being bound to any particular geographic region and the difficulties that poses for law enforcement, is one area that deserves further attention.

One reason why it is difficult to get a firm grip on hacktivism's direction, in addition to simply saying that it is too early to tell, is that hacktivism will evolve in response to changing global economic and political conditions. As it is hard to predict trends and directions in the global economy, it too, then, becomes hard to predict events that will be linked to those meta shifts.

Nevertheless, some people are trying to understand and make sense out of where hacktivism could go, although they might not be doing so using the particular word 'hacktivism' to describe this activity. Governments and corporations are keenly concerned, for example, about network security. To get some indications about the forecast for hacktivism in the 21st century it may be very useful to examine what these sorts of institutions are saying and how they are preparing to defend themselves.

It could very well be that governments might impose severe regimes that successfully curtail hacktivism. If so, 1998 might be seen at some point as the glory days, when hacktivist experiments were able to go largely unchallenged because the mechanisms of the state had not yet been in place to deal with the new phenomena. Or it could be that hacktivism is able to successfully remain several steps out in front of law enforcement efforts, or that too many people become involved that enforceability remains problematic. Again, it is difficult to know any of this.

Finally, while we can speak with some clarity about facets of hacktivism and also point to aspects of it that remain ambiguous and unforeseen, there is an overarching concern that comes from this discussion that deserves more attention. Specifically arising out of the consideration of the fifth portal, Resistance to Future War, what are the long term consequences posed for governments and states if

individuals, non-state actors, can engage in forms of cyberspatial resistance across traditional geo-political borders? This is important question raised by this discussion and one that demands more attention to answer properly. But it seems clear already that we are at the onset of a new way of thinking about, participating in, and resisting war. And that today's nascent hacktivity is part of the trajectory towards that new way.

End Notes

1. Amy Harmon, "Hacktivists' of All Persuasions Take Their Struggle to the Web," *New York Times*, 31 October 1998, sec. A1; Same in Carmin Karasic scrapbook (<http://custwww.xensei.com/users/carmin/scrapbook/nyt103198/31hack.html>)
2. John D. H Downing, "Computers for Political Change: PeaceNet and Public Data Access," *Journal of Communication* 39, no. 3 (Summer 1989): 154-62.
3. Harry Cleaver, "The Zapatistas and the International Circulation of Struggle: Lessons Suggested and Problems Raised," *Harry Cleaver homepage* 1998 (<http://www.eco.utexas.edu/faculty/Cleaver/lessons.html>)
4. Kenneth L. Hacker, "Missing links in the evolution of electronic democratization," *Media, Culture & Society* 18, (1996): 213-32; Lewis A. Friedland, "Electronic democracy and the new citizenship," *Media, Culture & Society* 18, (1996): 185-212; John Street, "Remote Control? Politics, Technology and 'Electronic Democracy'," *European Journal of Communication* 12, no. 1 (1997): 27-42.
5. John D. H Downing, "Computers for Political Change: PeaceNet and Public Data Access," *Journal of Communication* 39, no. 3 (Summer 1989): 154-62.
6. Linda M. Harasim, ed., *Global Networks: Computers and International Communication* (Cambridge, Mass.: MIT Press 1993)
7. There are many protest web sites. Trying a search on keywords "protest" and "web site" and there will be thousands of hits.
8. John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy* 12 (April-June 1993): 141-65.; (<http://gopher.well.sf.ca.us:70/0/Military/cyberwar>)
9. Cleaver, Harry "The Zapatistas and The Electronic Fabric of Struggle," *Harry Cleaver homepage* 1995 (<http://www.eco.utexas.edu/faculty/Cleaver/zaps.html>)
10. Gerfried Stocker and Christine Schopf, eds. *InfoWar* (Wien, Austria: Springer 1998); Ars Electronica Festival 1998 (<http://www.aec.at/infowar>)
11. Stefan Wray, "Towards Bottom-Up Information Warfare: Theory and Practice: Version 1.0," *Electronic Civil Disobedience archive* 1998 (<http://www.nyu.edu/projects/wray/BottomUp.html>)

12. Stefan Wray, "The Drug War and Information Warfare in Mexico," Masters Thesis, University of Texas at Austin, *Electronic Civil Disobedience archive* 1997 (<http://www.nyu.edu/projects/wray/masters.html>)
13. La Jornada (<http://serpiente.dgsca.unam.mx/jornada/index.html>)
14. Harry Cleaver, "Zapatistas in Cyberspace: An Accion Zapatista Report," *Harry Cleaver homepage* 1998 (<http://www.eco.utexas.edu/faculty/Cleaver/zapsincyber.html>)
15. No specific reference to this fact. But it is a matter of record.
16. Stefan Wray, "On Electronic Civil Disobedience," Peace Review 11, no. 1, (1999), forthcoming; *Electronic Civil Disobedience archive* 1998 (<http://www.nyu.edu/projects/wray/oecd.html>)
17. Critical Art Ensemble, *The Electronic Disturbance* (Brooklyn, NY: Autonomedia 1994); Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Brooklyn, NY: Autonomedia 1996); *Critical Art Ensemble homepage* (<http://mailer.fsu.edu/~sbarnes/>)
18. Stefan Wray, "Paris Salon or Boston Tea Party? Recasting Electronic Democracy, A View from Amsterdam," *Electronic Civil Disobedience archive* 1998 (<http://www.nyu.edu/projects/wray/teaparty.html>)
19. *Electronic Disturbance Theater homepage* (<http://www.thng.net/~rdom/ecd/ecd.html>)
20. Brett Stalbaum, "The Zapatista Tactical FloodNet," *Electronic Civil Disobedience homepage* 1998 (<http://www.nyu.edu/projects/wray/ZapTactFlood.html>)
21. Ricardo Dominguez, "SWARM: An ECD Project for Ars Electronica Festival '98," *Ricardo Dominguez homepage* 1998 (<http://www.thing.net/~rdom/>)
22. Electronic Disturbance Theater, "Chronology of SWARM," *Electronic Civil Disobedience archive* (<http://www.nyu.edu/projects/wray/CHRON.html>)
23. "Email Message From DISA to NYU Computer Security," *Electronic Civil Disobedience archive* (<http://www.nyu.edu/projects/wray/memo.html>)
24. Electronic Disturbance Theater's call for Electronic Civil Disobedience on November 22, 1998 (<http://www.thing.net/~rdom/ecd/November22.html>); (<http://www.thing.net/~rdom/ecd/block.html>)
25. "Mexico rebel supporters hack government home page," *Reuters*, 4 February 1998; Same in *Electronic Civil Disobedience homepage* (<http://www.nyu.edu/projects/wray/real.html>)
26. Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the

Web," *New York Times*, 31 October 1998, sec. A1; Same in *Carmin Karasic scrapbook* (<http://custwww.xensei.com/users/carmin/scrapbook/nyt103198/31hack.html>); Bob Paquin, "E-Guerrillas in the mist," *The Ottawa Citizen*, 26 October 1998 (<http://www.ottawacitizen.com/hightech/981026/1964496.html>)

27. *Hacktivism web page* (<http://www.hacktivism.org>); *Cult of the Dead Cow homepage* (<http://www.cultdeadcow.com/>)

28. While it is possible to point to certain early hacker ethical codes that, for example, privilege free and open access to all, there is not a monolithic hacker's perspective. Nevertheless, some whom call themselves hackers have criticized the FloodNet project because one of the things they allege it does is block bandwidth. This view can be said to be a digitally correct position.

29. The author knows about grassroots resistance to the 1990/1991 Gulf War because he was involved in anti-war organizing and action in the San Francisco Bay Area during this period.

30. Some of these listservs include: nyfma@tao.ca, damn-org@tao.ca, media-l@tao.ca, accion-zapatista@mcfeeley.cc.utexas.edu



This page is an archive for the Electronic Disturbance Theater.

[Click here](#) for Electronic Disturbance Theater homepage and ECD actions.

11.xx.98 [Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics](#) NEW!

10.31.98 New York Times: ['Hacktivists' of All Persuasions Take Their Struggle to the Web](#)

10.26.98 Ottawa Citizen: [E-Guerrillas in the mist](#)

10.15.98 [Electronic Disturbance Theater at Harvard Law School](#)

- [Presentation to Berkman Center for Internet and Society](#)
- [Notes on Internet and Society class](#)
- [Audio of Internet and Society class, Part 1](#)
- [Audio of Internet and Society class, Part 2](#)
- [Web site for Internet and Society class](#)

10.12.98 [Electronic Disturbance Theater Presentation, Audio File](#)

09.26.98 [Reason for moving main ECD page to the Thing's server](#)

09.10.98 [SWARM Chronology](#)

09.08.98 [Email Message from DISA to NYU Computer Security](#)

09.xx.98 [The Zapatista Tactical FloodNet](#)

09.xx.98 [The Ante-Chamber of Revolution: A Prelude to a Theory of Resistance and Maps](#)

08.05.98 [Bottom Up Information Warfare Theory and Practice Version 1.0](#)

08.01.98 [Paris Salon or Boston Tea Party: Recasting Electronic Democracy](#)

07.07.98 [Rhizomes Nomads and Resistant Internet Use](#)

06.17.98 [The Electronic Disturbance Theater and Electronic Civil Disobedience](#)

06:xx.98 *SWARM: An ECD Project for Ars Electronica '98*

05.05.98 *Die Umwandlung des Widerstands der Maschinenstürmer in einen virtuellen Widerstand*

05.01.98 *For Their Civil Disobedience, the 'Sit-In' Is Virtual*

05.01.98 *A Contribution to the Discussion of Electronic Civil Disobedience*

04.29.98 *Electronic Disturbance Theater Response to A Dirty War in Internet*

04.27.98 *A Dirty War in Internet (analysis)*

04.07.98 *Transforming Luddite Resistance into Virtual Luddite Resistance*

03.20.98 *On Electronic Civil Disobedience*

03.20.98 *Digital Zapatismo*

03.20.98 *How to Jam an Opponent's Fax Machine*

02.04.98 *Mexico Rebel Supporters Hack Government Home Page*

01.18.98 *Call Virtual Sit-ins at Five Mexico Financial Web Sites*

01.01.98 *Intercontinental Cyberspace Liberation Army Declares Netwar Against Mexican State*

09.xx.97 *Photos of U.S. Embassy in Mexico City*

08.xx.97 *Recombinant Networks*

08.xx.97 *The Drug War and Information Warfare in Mexico*

xx.xx.96 *Information Warfare section of The Revolution Will Be Digitized*

wray home

No helpful information was provided.
and return to:

FBI, Butte Information Technology Center
400 Main Street, Room #115
Butte, Montana 59701

BUTTE ITC RECORD #:

288-NY-268557

ANALYST: SUBJECT

Was the information provided helpful to your investigation? YES NO
If NO, please let us know how we could be more helpful to your
investigation:

b6
b7c

ACCOMPLISHMENT(S) resulting from information:

PERSON(S): (Enter total number applicable to each of the following)

FBI Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

Local Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

4 Subject(s) Arrested Located Identified

(Forward photo of Subject arrested with this Reply form)

Witness(es) Located Identified

New Witness(es) Located Identified

BUSINESS(ES): (Enter total number applicable to each of the following)

New Business(es) Identified

New Business Associates/Associations Identified

Financial Audit Trail(s) Enhanced

ASSET(S): (Enter total number applicable to each of the following)

(TYPES: C = CASH R = REAL PROPERTY P = PERSONAL PROPERTY)

Asset(s) Located Identified [VALUE: _____] TYPE: _____

Asset(s) Subject to Seizure/Forfeiture [VALUE: _____] TYPE: _____

Potential Economic Loss Prevented [VALUE: _____] TYPE: _____

OTHER: (Enter total number applicable to each of the following)

New Case(s) Initiated New Lead(s) Generated

COMMENTS:

288-NY-268557-20

| | |
|-------------|---------|
| SEARCHED | INDEXED |
| SERIALIZED | FILED |
| DEC 03 1998 | |
| 181 | |

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

288-NY-268557-22

| | | |
|-------------|----------|----------|
| SEARCHED | INDEXED | CM |
| SERIALIZED | FILED | CM |
| DEC 03 1998 | | |
| 20 | 20 | 20 |
| CM-S | CM-S | CM-S |
| 12/28/98 | 12/28/98 | 12/28/98 |
| UPLOAD | WHTHTR | BY |
| CM-S | CM-S | CM-S |

20
20
20

12/28/98
12/28/98
12/28/98

UPLOAD
WHTHTR
BY
CM-S
CM-S
CM-S

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/02/98

On December 01, 1998, SA [redacted] printed out the new web pages located at the Uniform Resource Locator of <http://www.thing.net/~rdom/ecd/ecd.html>, titled ELECTRONIC CIVIL DISOBEDIENCE. There was a link to a RealAudio broadcast of an interview between [redacted] and the ELECTRONIC DISTURBANCE THEATER. The interview was taped off of the Internet.

b6
b7C



Investigation on 12/01/1998 at New York

File # 288-NY-268557 Date dictated 12/02/1998

by SA [redacted] b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Tealau... 12/02/98

288-NY-268557-23

UPLOADED

WITH/TEXT ✓
WITH/OUT TEXT _____
BY CM
DATE 12-14-98

SEARCHED CM INDEXED CM
SERIALIZED CM FILED CM

DEC 11 1998
FBI - DQ
EMST/rr

AUSA, EC

b6
b7C

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/10/1998

To: New York

From: New York

C-37

Contact: SA [redacted]

Approved By: [redacted] EMS/TW

Drafted By: [redacted] :11m

Case ID #: 288-NY-268557 (Pending)

b6
b7C

Title: ELECTRONIC DISTURBANCE THEATER;
[redacted]

CITA

OO:NY

Synopsis: Summary of 12/10/1998 meeting with United States Attorney's Office for the Southern District of New York.

Details: Present at 12/10/1998 meeting were [redacted]

Chief, Major Crimes Unit, AUSA [redacted]

SSA [redacted]

[redacted] SA [redacted] and SA [redacted]

b6
b7C

The direction of the EDT investigation was discussed. [redacted] opined that the potential First Amendment aspects of the subjects' conduct is not problematic because the conduct violates 18 USC 1030 (assuming all elements can be proved). In other words, even though the EDT's conduct is a political protest the underlying conduct is illegal and therefore prosecutable.

The similarities between EDT's FloodNet attack and other hacks such as E-mail bombs were discussed. [redacted] requested information on prosecutions of similar attacks that abused publicly available computer resources on a victim system.

b6
b7C

The issue of damages to victim systems was also raised. [redacted] focused on the damage element of 18 USC 1030 and emphasized the necessity of obtaining a precise and detailed statement of quantified damage to each system.

Further investigation will require specific dollar damage statements from both Ft. Benning and DefenseLINK. These damage statements must differentiate between costs incurred in preparing for the attack and cost incurred repairing or limiting damage during or after the attack.

115-00165

To: New York From: New York
Re: 288-NY-268557, 12/10/1998

Additionally, the victims will be interviewed to outline the purpose of the systems effected by FloodNet and the impact on Department of Defense operations due to a potential denial of service attack.

◆◆

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/11/1998

To: FBI Headquarters

Attn: SSA [redacted]

NIPC, [redacted]

From: New York

C-37

Contact: [redacted]

Approved By: [redacted] *[Signature]*

b6

b7C

Drafted By: [redacted]

✓ Case ID #: 288-NY-268557 (Pending)

Title: ELECTRONIC DISTURBANCE THEATER,
et al.;
CITA
OO:NY

Synopsis: Request information on similar cases.

Details: As noted in EC dated 12/10/98, agents conducting the investigation entitled above met with representatives of the Office of the United States Attorney for the Southern District of New York. During that meeting [redacted] Chief, Major Crimes Unit noted that the EDT attack operates in a similar manner to an E-mail flood attack, in that it is an attack which abuses a publicly available function on the victim server.

X SAB

b6
b7C

[redacted] requested that information on any prosecutions of attacks similar to those orchestrated by the Electronic Disturbance Theater (such as a mail flood) be made available. Accordingly, New York requests that NIPC forward any such information to C-37.

♦♦

288-NY-268557-24

UPLOADED
WITH TEX: ✓
WITH PCF: ✓
BY CM
DATE 12-14-98

| | |
|------------------|---------------|
| SEARCHED _____ | INDEXED _____ |
| SERIALIZED _____ | FILED _____ |
| DEC 11 1998 | |
| BOND/ | EM/ |

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

Reference: SEC mailing list signups
SAC [redacted]

address book

User Signature

Mail To (Email Address)

listproc@listproc.thing.net

Mail CC (Email Address)

[redacted]

Mail From (Your Name)

chrislee

Return Address (Your Email Address)

chrislee@conninc.com

Subject

[redacted]

Message Text

subscribe ecd Chris Lee

File to attach:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

| | |
|----------------------|-----------------|
| SEARCHED | INDEXED |
| SERIALIZED CM | FILED CM |
| DEC 14 1998 | |
| FBI - NEW YORK | |

12/22 SGT/N

RESPONSE: NIPC request REC 11/20/98 12/22 SGT/N

From: [REDACTED]
To: [REDACTED]
Date: 12/11/98 7:53am
Subject: EDT

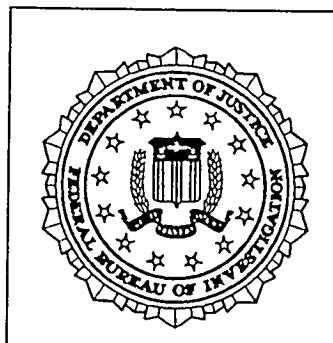
b6
b7C
b7E

[REDACTED] thanks, the info was great that you provided to me
pertaining to EDT. NIPC is now [REDACTED]

[REDACTED] Would you please
fax me a copy of the e-mail pertaining to the 12/22/98 threat.

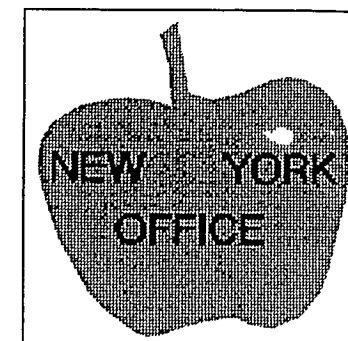
Thanks
IOS [REDACTED]

(V)
[Signature]



NEW YORK OFFICE

FAX



COVER SHEET

To:

Fax Number:

Number of Pages: 3 (including cover sheet)

Office Telephone Number:

Comments:

COPY OF ECD ANNOUNCEMENT OF 12/22/98 VIRTUAL SITE.

NO TARGET HAS BEEN ANNOUNCED YET.

b6
b7C

CONFIDENTIAL FBI FACSIMILE COMMUNICATION

The information contained in this facsimile message, and any and all accompanying documents, constitute confidential information. This information is the property of the Federal Bureau of Investigation. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking of any action in reliance on this information is strictly prohibited. If you received this information in error, please notify us immediately by telephone.

From: SA

Office Telephone Number:

Fax Number:

electronic civil Disobedience



Next Virtual Sit-in on
December 22
Anniversary of the Acteal massacre in Chiapas



Two recent News segments on
The Electronic Disturbance Theater
First one is a quicktime mov. from
[New Media News](#).



Also
[***How To Make Trouble
and Influence People***](#)



by Ian Walker
An hour long RealAudio on
Culture Jammers around the world.
Featuring interviews with
RT@Mark, Adbusters,
The Electronic Disturbance Theater,
and many more.



[**Mid-way into the Sit-In**](#)

[**at School of the Americas**](#)

[**on November 22**](#)

[**Fort Benning countered
by IP Blocking Address**](#)

We will post updates as more information flows in!



Recent Action Against
The Thing's
Support of FloodNet
VIOLATION OF THE VERIO
ACCEPTABLE USE POLICY
Read About It On Thing.news. [In Threads](#).

[**SWARM Chronology**](#)



Next Virtual Sit-in on December 22
Anniversary of the Acteal massacre in Chiapas.
About The Electronic Disturbance Theater.

See The Zapatista Tactical FloodNet for a discussion of FloodNet's functionality, interactivity, philosophy, and as a form of conceptual art.



- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

12/15/98

On December 15, 1998, SA [redacted] printed off the web page located at the URL <http://www.newmedianews.com/cgi-bin...archive/1998/11/13/TSwebprotest.dtl>. On December 4, 1998, SA [redacted] taped the audio interview of [redacted] which was available at the above referenced URL.

b6
b7c

288-NY-268557-28

| | |
|--------------------|------------|
| SEARCHED | INDEXED CM |
| SERIALIZED CM | FILED CM |
| DEC 15 1998 | |
| <i>[Signature]</i> | |

Investigation on 12/15/98 at New York

File # 288-NY-268557 Date dictated 12/15/98

by SA [redacted] b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

new media.wpd

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/15/98

On December 15, 1998, SA [redacted] received a diskette containing the WebTrends Web Log Analyzer Report for Ft. Benning from Robert Kane, RCERT, 2933 Thunderbird Drive, Sierra Vista, AZ. The report showed web statistics from November 20, 1998 at 05:00:00 through November 23, 1998 09:38:28.

b6
b7C

(X) *[Signature]*

UPLOADED
WITH TEXT ✓
WITH ATTACHMENT
BY CM
DATE 12-21-98

288-NY-268557-29

| | |
|---------------|----------|
| SEARCHED | INDEXED |
| SERIALIZED CM | FILED CM |
| DEC 15 1998 | |
| FBI - NY | |
| [Signature] | |

Investigation on 12/15/1998 at New York

File # 288-NY-268557 Date dictated 12/15/1998

by SA [redacted] b6
b7C



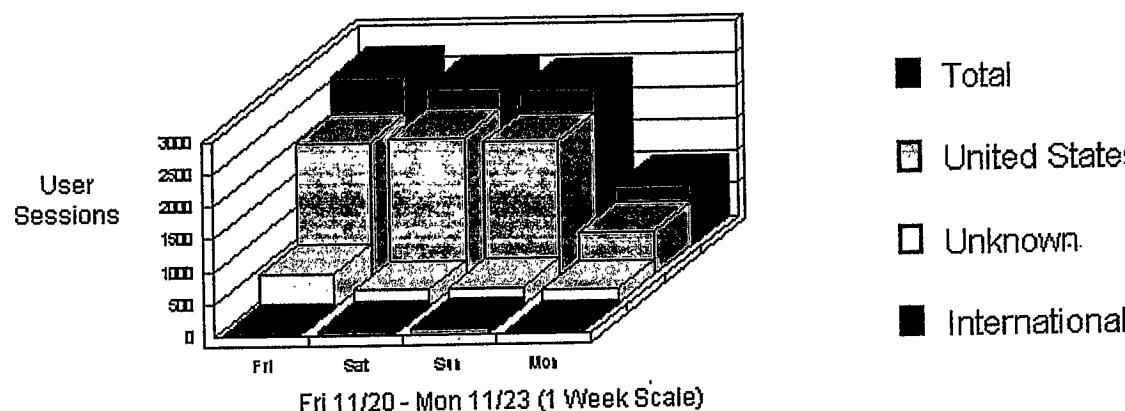
Default Report

Fort Benning

General Statistics

The User Profile by Regions graph identifies the general location of the visitors to your Web site. The General Statistics table includes statistics on the total activity for this web site during the designated time frame.

User Profile by Regions



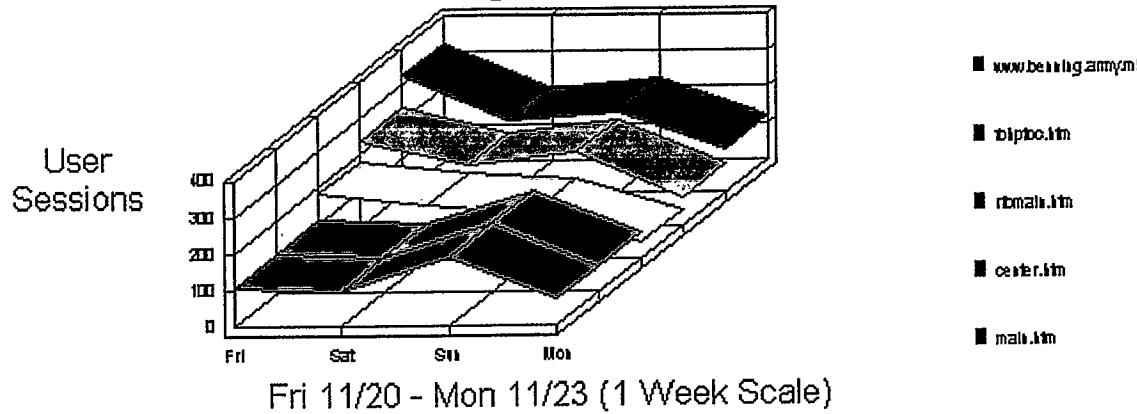
General Statistics

| | |
|---|--|
| Date & Time This Report was Generated | Wednesday December 09, 1998 - 12:39:00 |
| Timeframe | 11/20/98 05:00:00 - 11/23/98 09:38:28 |
| Number of Hits for Home Page | N/A |
| Number of Successful Hits for Entire Site | 142,764 |
| Number of Page Views (Impressions) | 38,011 |
| Number of User Sessions | 8,489 |
| User Sessions from United States | 81.91% |
| International User Sessions | 3% |
| User Sessions of Unknown Origin | 15.07% |
| Average Number of Hits Per Day | 35,691 |
| Average Number of Page Views Per Day | 9,502 |
| Average Number of User Sessions Per Day | 2,122 |
| Average User Session Length | 00:13:50 |

Most Requested Pages

This section identifies the most popular web site pages and how often they were accessed. The average time a user spends viewing a page is also indicated in the table.

Most Requested Pages



Most Requested Pages

| | Pages | Views | % Of Total Views | User Sessions | Avg. Time |
|---|---|---------------|------------------|---------------|------------|
| 1 | http://www.benning.army.mil/ | 1,199 | 3.15% | 866 | 00:01:51 |
| 2 | http://www.benning.army.mil/fbhome/tableofcontents/fbhptoc.htm | 1,008 | 2.65% | 682 | 00:02:55 |
| 3 | http://www.benning.army.mil/rtb/rtbmain.htm | 637 | 1.67% | 498 | 00:02:14 |
| 4 | http://www.benning.army.mil/usarsa/center.htm | 571 | 1.5% | 467 | 00:00:24 |
| 5 | http://www.benning.army.mil/usarsa/main.htm | 566 | 1.48% | 459 | 00:00:30 |
| 6 | http://www.benning.army.mil/usarsa/toprt.htm | 564 | 1.48% | 457 | 00:00:27 |
| 7 | http://www.benning.army.mil/usarsa/topctr.htm | 561 | 1.47% | 448 | 00:00:33 |
| 8 | http://www.benning.army.mil/rtb/rtbweb/rgrscl.htm | 558 | 1.46% | 462 | 00:02:43 |
| 9 | http://www.benning.army.mil/usarsa/topleft.htm | 558 | 1.46% | 453 | 00:00:49 |
| 10 | http://www.benning.army.mil/usarsa/right.htm | 558 | 1.46% | 453 | 00:01:49 |
| Sub Total For the Page Views Above | | 9,082 | 23.89% | N/A | N/A |
| Total For the Log File | | 38,011 | 100% | N/A | N/A |

Least Requested Pages

This section identifies the least popular pages on your Web site, and how often they were accessed.

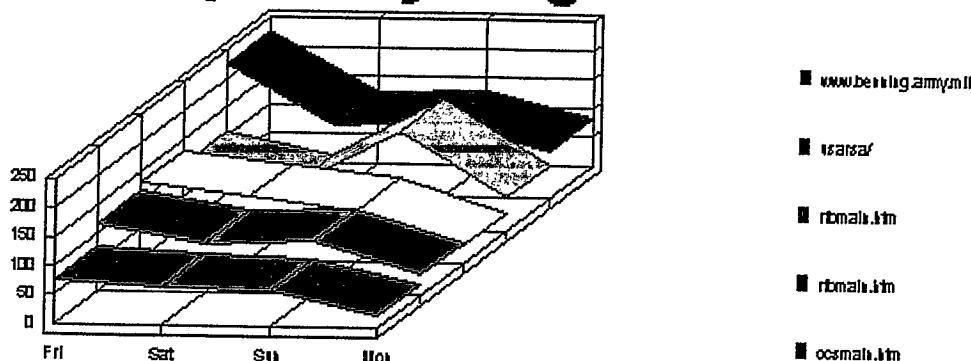
| Least Requested Pages | |
|------------------------------|---|
| | Pages |
| 1 | http://192.153.150.25/usarsa/CATALOG/CATALOG.HTM |
| 2 | http://www-benning.army.mil/fbhome/29thinf/PLGR.HTM |
| 3 | http://www-benning.army.mil/fbhome/29thinf/HHC229.HTM |
| 4 | http://www-benning.army.mil/rtb/history2/monbrick.htm |
| 5 | http://www.benning.army.mil/fbhome/acap/HOTLEAD FORM.html |
| 6 | http://secpoc.army.mil/seintranet/mso/mso.htm |
| 7 | http://secpoc.army.mil/seintranet/hrd/hrd.htm |
| 8 | http://www-benning.army.mil/fbhome/ocs/history/history.html |
| 9 | All Times&FActions>All Actions&FWWhere=CPOC">http://secpoc.army.mil/PP1/personnel/sf52_track/MGRrag_inbox.asp?FOrganization=AR&FCPACCode=AR&MONROE&FTimes>All Times&FActions>All Actions&FWWhere=CPOC |
| 10 | http://www-benning.army.mil/fbhome/11th/1-11INF/BNHQ/welcome.htm |

Top Entry Pages

This section identifies the first hit from a user visiting this site. This is most likely the home page but, in some cases, it may also be specific URLs that users enter to access a particular page directly. The percentages refer to the total number of user sessions.

Top Entry Pages

User Sessions



Fri 11/20 - Mon 11/23 (1 Week Scale)

Top Entry Pages

| | Pages | % of Total | User Sessions |
|----------------------------------|---|---------------|---------------|
| 1 | http://www.benning.army.mil/ | 6.57% | 558 |
| 2 | http://www.benning.army.mil/usarsa/ | 4.71% | 400 |
| 3 | http://www.benning.army.mil/rtb/rtbmain.htm | 4.22% | 359 |
| 4 | http://www.benning.army.mil/rtb/rtbmain.htm | 3.84% | 326 |
| 5 | http://www.benning.army.mil/fbhome/ocs/ocsmain.htm | 2.6% | 221 |
| 6 | http://www.benning.army.mil/ | 2.04% | 174 |
| 7 | http://www.benning.army.mil/rtb/rtbweb/rgrscl.htm | 1.69% | 144 |
| 8 | http://www.benning.army.mil/fbhome/vti_bin/fpcount.exe/fbhome/ | 1.55% | 132 |
| 9 | http://www.benning.army.mil/fbhome/dbback1.jpg | 1.48% | 126 |
| 10 | http://www.benning.army.mil/usarsa/main.htm | 1.48% | 126 |
| Total For the Pages Above | | 30.22% | 2,566 |

Top Exit Pages

This section identifies the pages users were on when they left the site. The percentages refer to the total number of user sessions that started with a valid Document Type. If the session started on a document with a different type (such as a graphic or sound file), the file is not counted as an Entry Page, and the session is not counted in the total.

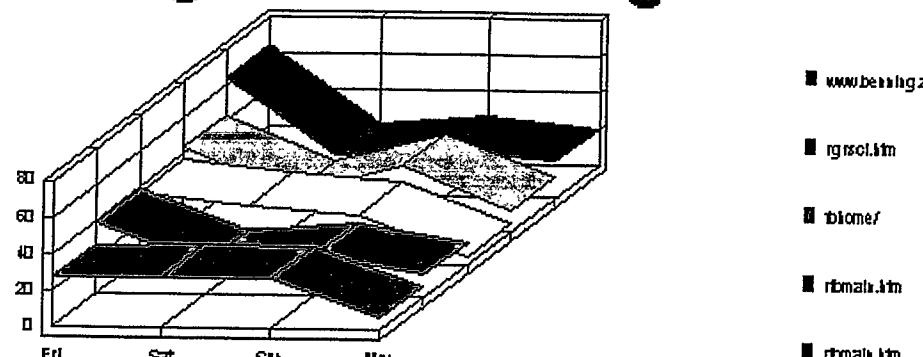
| Top Exit Pages | | | |
|---|---|-----------------------|--------------------------|
| | Pages | % OF Total | User Sessions |
| 1 | http://www-benning.army.mil/fbhome/_vti_bin/fpcount.exe/fbhome/ | 3.75% | 252 |
| 2 | http://www-benning.army.mil/fbhome/tableofcontents/fbhptoc.htm | 3.45% | 232 |
| 3 | http://www.benning.army.mil/ | 2.78% | 187 |
| 4 | http://www.benning.army.mil/rtb/rtbweb/rgrscl.htm | 2.3% | 155 |
| 5 | http://www-benning.army.mil/rtb/_vti_bin/fpcount.exe/RTB/ | 1.72% | 116 |
| 6 | http://www-benning.army.mil/rtb/rtbmain.htm | 1.71% | 115 |
| 7 | http://www-benning.army.mil/RTB/ranger/photo/photo.htm | 1.65% | 111 |
| 8 | http://www.benning.army.mil/rtb/rtbmain.htm | 1.62% | 109 |
| 9 | http://www-benning.army.mil/usarsa/_vti_bin/fpcount.exe/usarsa/ | 1.53% | 103 |
| 10 | http://www-benning.army.mil/fbhome/ocs/ocsmain.htm | 1.51% | 102 |
| Total For the Pages Above (only sessions starting on a valid document type are included) | | | 22.06% |
| | | | 1,482 |

Single Access Pages

This section identifies the pages on the site that visitors access and exit without viewing any other page. The percentages refer to the total number of user sessions that started with a valid Document Type. If the session started on a document with a different type (such as a graphic or sound file), the file is not counted as an Entry Page, and the session is not counted in the total

Single Access Pages

User Sessions



Fri 11/20 - Mon 11/23 (1 Week Scale)

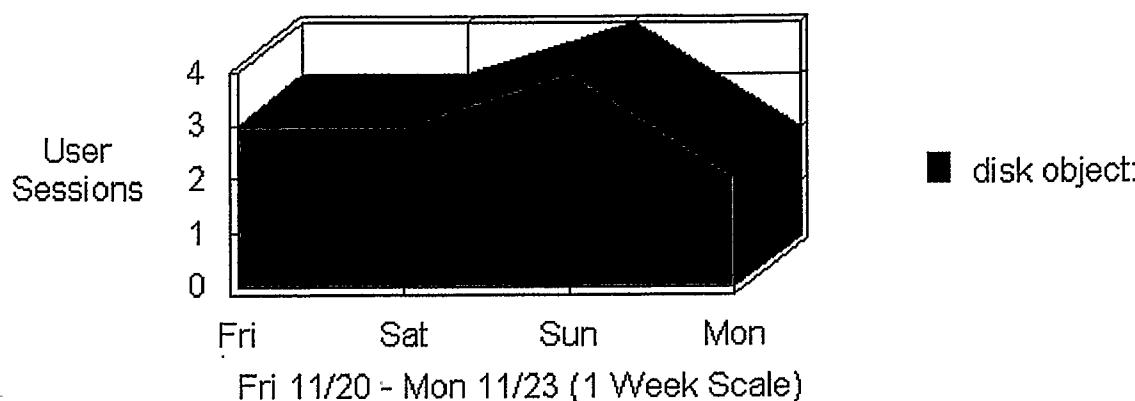
Single Access Pages

| | Pages | % of Total | User Sessions |
|----------------------------------|---|---------------|---------------|
| 1 | http://www.benning.army.mil/ | 4.64% | 133 |
| 2 | http://www.benning.army.mil/rtb/rbwweb/rgrscl.htm | 3.8% | 109 |
| 3 | http://www.benning.army.mil/fbhome/vti_bin/fpcount.exe/fbhome/ | 3.42% | 98 |
| 4 | http://www.benning.army.mil/rtb/rtbmain.htm | 3.14% | 90 |
| 5 | http://www.benning.army.mil/rtb/rtbmain.htm | 3.07% | 88 |
| 6 | http://www.benning.army.mil/fbhome/ocs/ocsmain.htm | 3.07% | 88 |
| 7 | http://www.benning.army.mil/fbhome/tableofcontents/fbhptoc.htm | 2.23% | 64 |
| 8 | http://www.benning.army.mil/rtb/vti_bin/fpcount.exe/RTB/ | 2.02% | 58 |
| 9 | http://www.benning.army.mil/rtb/vti_bin/fpcount.exe/RTB/ | 1.88% | 54 |
| 10 | http://www.benning.army.mil/ | 1.67% | 48 |
| Total For the Pages Above | | 28.99% | 830 |

Most Accessed Directories

This section analyzes accesses to the directories of the site. This information can be useful in determining the types of data most often requested.

Most Accessed Directories



Most Accessed Directories

| Path to Directory | Hits | % of Total Hits | Non Cached % | Non Cached K Xferred | User Sessions |
|-------------------|------|-----------------|--------------|----------------------|---------------|
| disk object: | 244 | 100% | 100% | 143K | 12 |

Top Paths Through Site

This section identifies the paths people most often follow when visiting the site. The path begins at the page of entry and shows the next six consecutive pages viewed.

Top Paths Through Site

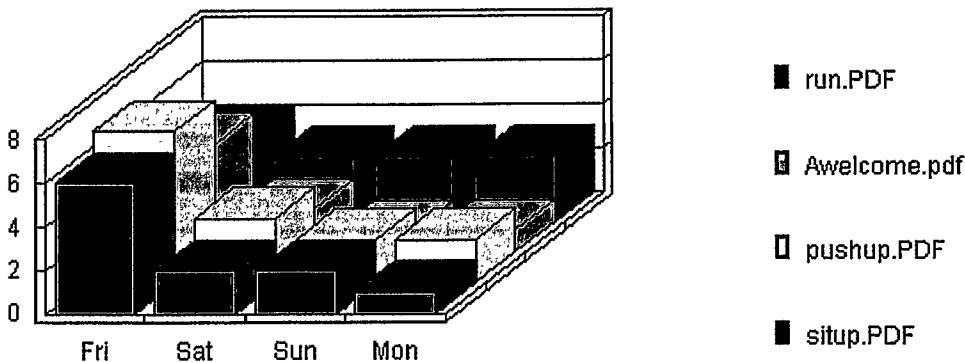
| | Pages | % of Total | User Sessions |
|----------------------------------|--|--------------|---------------|
| 1 | 1. http://www.benning.army.mil/usarsa/ 2. http://www.benning.army.mil/usarsa/_vti_bin/fpcount.exe/usarsa/ 3. http://www.benning.army.mil/usarsa/main.htm 4. http://www.benning.army.mil/usarsa/topleft.htm 5. http://www.benning.army.mil/usarsa/left.htm 6. http://www.benning.army.mil/usarsa/topctr.htm | 2.27% | 153 |
| 2 | 1. http://www.benning.army.mil/ | 1.98% | 133 |
| 3 | 1. http://www.benning.army.mil/rtb/rtbweb/rgrscl.htm | 1.62% | 109 |
| 4 | 1. http://www.benning.army.mil/fbhome/_vti_bin/fpcount.exe/fbhome/ | 1.45% | 98 |
| 5 | 1. http://www.benning.army.mil/rtb/rtbmain.htm | 1.34% | 90 |
| 6 | 1. http://www.benning.army.mil/rtb/rtbmain.htm | 1.31% | 88 |
| 7 | 1. http://www.benning.army.mil/fbhome/ocs/ocsmain.htm | 1.31% | 88 |
| 8 | 1. http://www.benning.army.mil/usarsa/ 2. http://www.benning.army.mil/usarsa/_vti_bin/fpcount.exe/usarsa/ | 0.98% | 66 |
| 9 | 1. http://www.benning.army.mil/fbhome/tableofcontents/fbhptoc.htm | 0.95% | 64 |
| 10 | 1. http://www.benning.army.mil/rtb/_vti_bin/fpcount.exe/RTB/ | 0.86% | 58 |
| Total For the Paths Above | | 14.1% | 947 |

Most Downloaded Files

This section identifies the most popular file downloads for the site. If an error occurred during the transfer, that transfer is not counted.

Most Downloaded Files

User Sessions



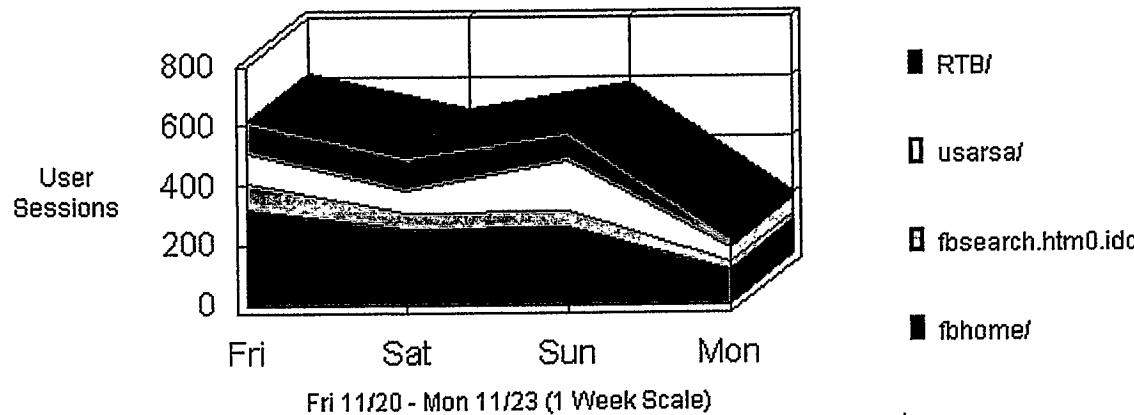
Most Downloaded Files

| | File | No. of Downloads | % of Total Downloads |
|-----------------------------------|---|------------------|----------------------|
| 1 | http://www.benning.army.mil/fbhome/training/fitness/run.PDF | 26 | 10.03% |
| 2 | http://www.benning.army.mil/fbhome/NCOA/Awelcome.pdf | 25 | 9.65% |
| 3 | http://www.benning.army.mil/fbhome/training/fitness/pushup.PDF | 24 | 9.26% |
| 4 | http://www.benning.army.mil/fbhome/training/fitness/situp.PDF | 21 | 8.1% |
| 5 | http://www.benning.army.mil/fbhome/TRAINING/FITNESS/pushup.PDF | 17 | 6.56% |
| 6 | http://www.benning.army.mil/fbhome/NCOA/Know.pdf | 14 | 5.4% |
| 7 | http://www.benning.army.mil/fbhome/NCOA/bwelcome.PDF | 13 | 5.01% |
| 8 | http://www.benning.army.mil/fbhome/11th/1-11inf/aqrD/Downloads/welcome.pdf | 13 | 5.01% |
| 9 | http://www.benning.army.mil/fbhome/NCOA/Pac_pldc.pdf | 10 | 3.86% |
| 10 | http://www.benning.army.mil/fbhome/TRAINING/eib/WEib97cn.zip | 9 | 3.47% |
| Total For the Files Above: | | 172 | 66.4% |

Most Submitted Forms and Scripts

This section identifies the most popular forms or scripts executed by the server. WebTrends counts any line with a Post command or a Get command with a "?" as a form or script, and shows only successful hits.

Most Submitted Forms & Scripts



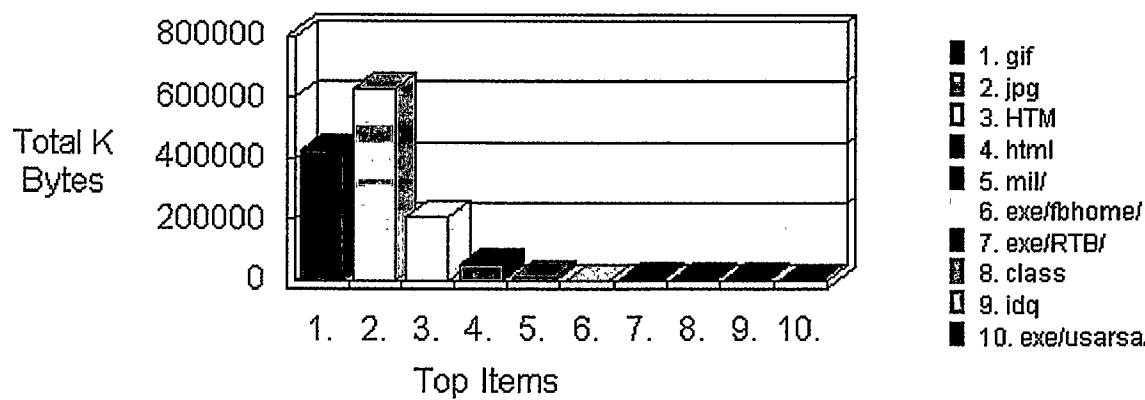
Most Submitted Forms & Scripts

| | Forms and/or Scripts | No. of Forms | % Of Total | User Sessions |
|----|---|--------------|------------|---------------|
| 1 | http://www-benning.army.mil/fbhome/ vti bin/fpcount.exe/fbhome/ | 1,133 | 36.76% | 947 |
| 2 | http://www-benning.army.mil/fbhome/ vti bin/fbsearch.htm0.idq | 461 | 14.95% | 218 |
| 3 | http://www.benning.army.mil/usarsa/ vti bin/fpcount.exe/usarsa/ | 407 | 13.2% | 390 |
| 4 | http://www-benning.army.mil/rtb/ vti bin/fpcount.exe/RTB/ | 361 | 11.71% | 339 |
| 5 | http://www.benning.army.mil/rtb/ vti bin/fpcount.exe/RTB/ | 293 | 9.5% | 280 |
| 6 | http://secpoc.army.mil/secpoc/ vti bin/fpcount.exe/SECPOC/ | 110 | 3.56% | 101 |
| 7 | http://www.benning.army.mil/fbhome/ vti bin/fpcount.exe/fbhome/ | 53 | 1.71% | 41 |
| 8 | http://www.benning.army.mil/dcd/ vti bin/fpcount.exe/dcd/ | 32 | 1.03% | 32 |
| 9 | http://150.226.212.101/FORMSLIB/ vti bin/fpcount.exe/Formslib/ | 26 | 0.84% | 19 |
| 10 | http://www-benning.army.mil/RTB/history2/monu.map | 24 | 0.77% | 8 |

Most Downloaded File Types and Sizes

This section identifies the accessed file types and the total kilobytes downloaded for each file type. Cached requests and erred hits are excluded from the totals.

Most Downloaded File Types



Most downloaded File Types

| | File type | Files | K Bytes Transferred |
|--|------------------|----------------|----------------------------|
| 1 | gif | 52,671 | 427,209K |
| 2 | jpg | 32,871 | 630,212K |
| 3 | HTM | 28,605 | 206,804K |
| 4 | html | 3,319 | 52,839K |
| 5 | mil/ | 1,426 | 13,518K |
| 6 | exe/fbhome/ | 1,194 | 795K |
| 7 | exe/RTB/ | 664 | 1,151K |
| 8 | class | 574 | 3,459K |
| 9 | idq | 472 | 3,331K |
| 10 | exe/usarsa/ | 426 | 823K |
| Total Files & K Bytes Transferred | | 122,222 | 1,340,137K |

Top Users

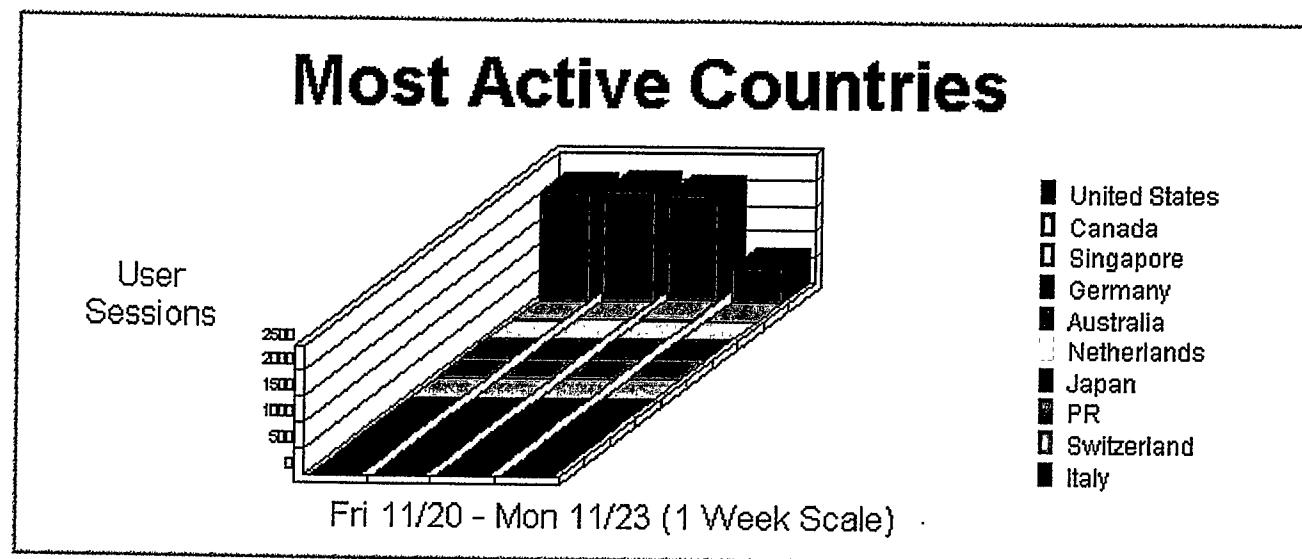
This section identifies the IP address and/or domain name and their relative activity level on the site. WebTrends cannot differentiate between different users using the same IP address.

| | User | Hits | % of Total Hits | User Sessions |
|---------------------------------|-------------------------------------|----------------|------------------------|----------------------|
| 1 | resnet-19-202.dorm.utexas.edu | 3,890 | 2.72% | 1 |
| 2 | ppp-206-170-2-69.sntc01.pacbell.net | 2,288 | 1.6% | 2 |
| 3 | sl6.thing.net | 1,694 | 1.18% | 2 |
| 4 | 150.114.70.93 | 661 | 0.46% | 1 |
| 5 | lpwa.com | 546 | 0.38% | 4 |
| 6 | xensei-ppp-0247.xensei.com | 530 | 0.37% | 1 |
| 7 | 143.77.166.231 | 492 | 0.34% | 1 |
| 8 | 129.72.206.32 | 476 | 0.33% | 3 |
| 9 | okcnase-97.ionet.net | 468 | 0.32% | 1 |
| 10 | ftsumter.acert.belvoir.army.mil | 443 | 0.31% | 3 |
| Subtotal for Users Above | | 11,488 | 8.04% | 19 |
| Total | | 142,764 | 100% | 8,489 |

Most Active Countries

This section identifies the top locations of the visitors to the site by country. The country of the user is determined by the suffix of their domain name. Use this information carefully because this information is based on where the domain name of the visitor is registered, and may not always

be an accurate identifier of the actual geographic location of this visitor (for example, while a vast majority of .com domain names are from the United States, there is a small minority of domain names that exist outside of the United States.)



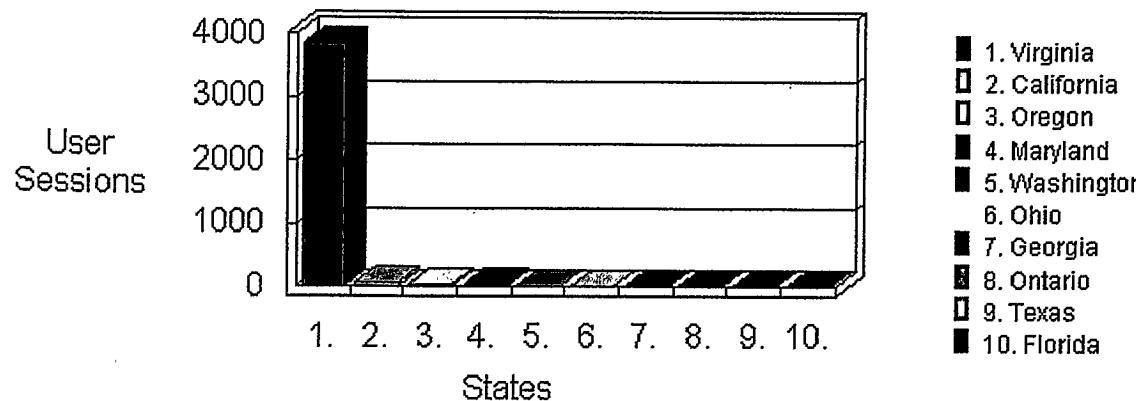
| | Countries | User Sessions |
|----|----------------|---------------|
| 1 | United States | 6,954 |
| 2 | Canada | 45 |
| 3 | Singapore | 21 |
| 4 | Germany | 20 |
| 5 | Australia | 17 |
| 6 | Netherlands | 15 |
| 7 | Japan | 13 |
| 8 | PR | 11 |
| 9 | Switzerland | 11 |
| 10 | Italy | 10 |
| 11 | UK | 9 |
| 12 | Sweden | 9 |
| 13 | Norway | 6 |
| 14 | Austria | 4 |
| 15 | Czech Republic | 4 |
| | Total | 7,149 |

North American States and Provinces

This section breaks down web site activity to show which of the North American States and Provinces were the most active on the site. This information is based on where the domain name of the visitor is registered, and may not always be an accurate representation of the actual geographic location of this visitor. This information can only be displayed if reverse DNS lookups

have been performed.

North American States & Provinces



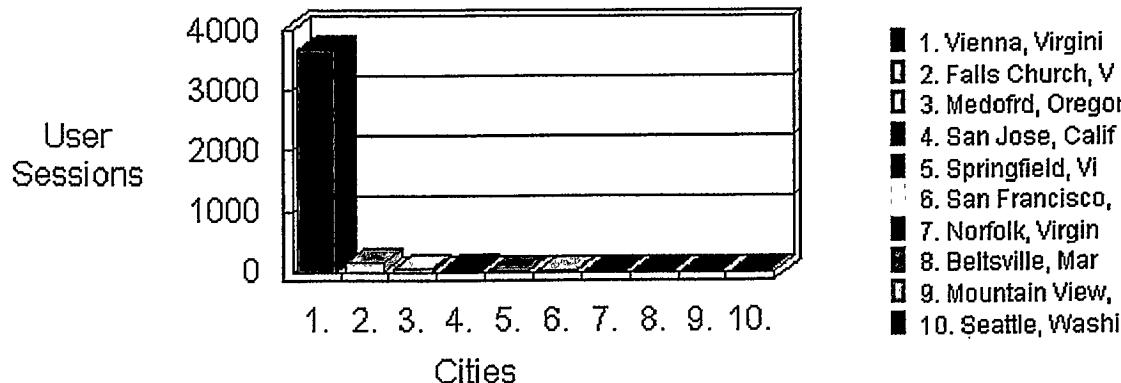
North American States & Provinces

| | State | User Sessions |
|----------------------------|------------|---------------|
| 1 | Virginia | 3,853 |
| 2 | California | 80 |
| 3 | Oregon | 41 |
| 4 | Maryland | 21 |
| 5 | Washington | 11 |
| 6 | Ohio | 7 |
| 7 | Georgia | 7 |
| 8 | Ontario | 6 |
| 9 | Texas | 5 |
| 10 | Florida | 4 |
| Total For the States Above | | 4,035 |

Most Active Cities

This section further breaks down the site's activity to show which cities were the most active on the site. This information is based on where the domain name of the visitor is registered, and may not always be an accurate representation of the actual geographic location of this visitor. This information can only be displayed if reverse DNS lookups have been performed.

Most Active Cities



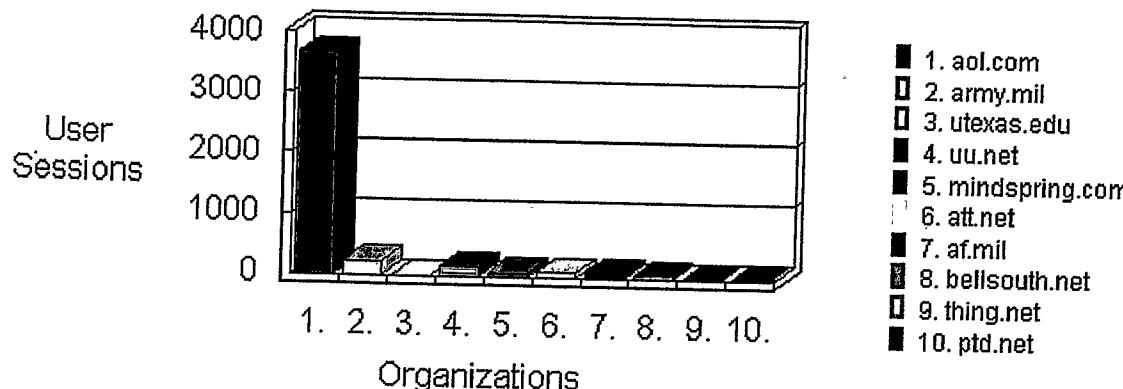
Activity by City

| | City, State | User Sessions |
|----|--|---------------|
| 1 | Vienna, Virginia, United States | 3,658 |
| 2 | Falls Church, Virginia, United States | 148 |
| 3 | Medofrd, Oregon, United States | 41 |
| 4 | San Jose, California, United States | 31 |
| 5 | Springfield, Virginia, United States | 26 |
| 6 | San Francisco, California, United States | 24 |
| 7 | Norfolk, Virginia, United States | 19 |
| 8 | Beltsville, Maryland, United States | 12 |
| 9 | Mountain View, California, United States | 10 |
| 10 | Seattle, Washington, United States | 7 |
| | Total For the Cities Above | 3,976 |

Most Active Organizations

This section identifies the companies or organizations that accessed the site the most often.

Most Active Organizations



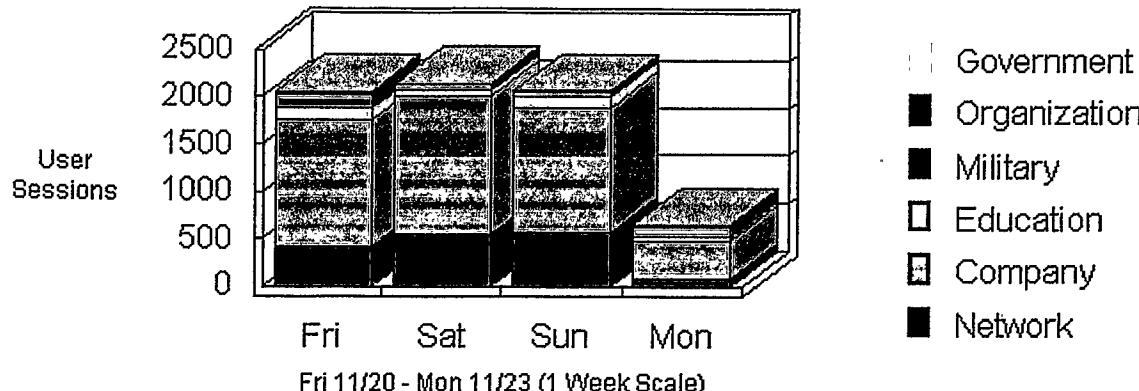
Most Active Organizations

| | Organizations | Hits | % of Total Hits | User Sessions |
|-------------------------------------|-----------------------------------|----------------|-----------------|---------------|
| 1 | America Online aol.com | 16,861 | 12.79% | 3,658 |
| 2 | army.mil | 5,743 | 4.35% | 226 |
| 3 | utexas.edu | 3,890 | 2.95% | 1 |
| 4 | Uunet Technologies Inc. uu.net | 3,882 | 2.94% | 148 |
| 5 | mindspring.com | 2,203 | 1.67% | 65 |
| 6 | att.net | 1,953 | 1.48% | 87 |
| 7 | af.mil | 1,801 | 1.36% | 76 |
| 8 | bellsouth.net | 1,748 | 1.32% | 46 |
| 9 | thing.net | 1,717 | 1.3% | 3 |
| 10 | ptd.net | 52 | 0.03% | 2 |
| Subtotal For Companies Above | | 39,850 | 30.23% | 4,312 |
| Total For the Log File | | 142,764 | 100% | 8,489 |

Organization Breakdown

This section provides a breakdown by types of organizations (.com, .net, .edu, .org, .mil, and .gov.) This information can only be displayed if reverse DNS lookups have been performed.

Organization Breakdown



Organization Breakdown

| | Organization | Hits | % of Total Hits | User Sessions |
|---|---------------------|----------------|------------------------|----------------------|
| 1 | Network | 39,818 | 38.86% | 1,614 |
| 2 | Company | 37,781 | 36.87% | 4,520 |
| 3 | Education | 13,885 | 13.55% | 350 |
| 4 | Military | 9,158 | 8.93% | 365 |
| 5 | Organization | 990 | 0.96% | 42 |
| 6 | Government | 823 | 0.8% | 30 |
| | Total | 102,455 | 100% | 6,921 |

Summary of Activity for Report Period

This section outlines general server activity, comparing the level of activity on weekdays and weekends. The Average Number of Users and Hits on Weekdays are the averages for each individual week day. The Average Number of Users and Hits for Weekends groups Saturday and Sunday together. Values in the table do not include errd hits.

Summary of Activity for Report Period

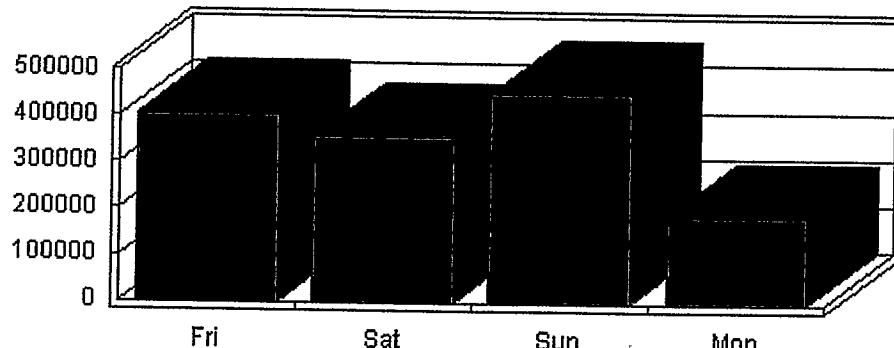
| | |
|---|-------------------|
| Average Number of <i>Users</i> per day on Weekdays | 1,792 |
| Average Number of <i>Hits</i> per day on Weekdays | 30,613 |
| Average Number of <i>Users</i> for the entire Weekend | 4,905 |
| Average Number of <i>Hits</i> for the entire Weekend | 81,538 |
| Most Active Day of the Week | Sun |
| Least Active Day of the Week | Tue |
| Most Active Day Ever | November 22, 1998 |
| Number of Hits on Most Active Day | 46,378 |
| Least Active Day Ever | November 23, 1998 |
| Number of Hits on Least Active Day | 19,360 |

Summary of Activity by Time Increment

This section helps you understand the bandwidth requirements of the site by indicating the volume of activity in kilobytes transferred. The table provides various measures of activity by unit of time for the report period (the unit of time depends on the amount of time covered by the report, and will be the day in most cases).

Bandwidth

Total K Bytes



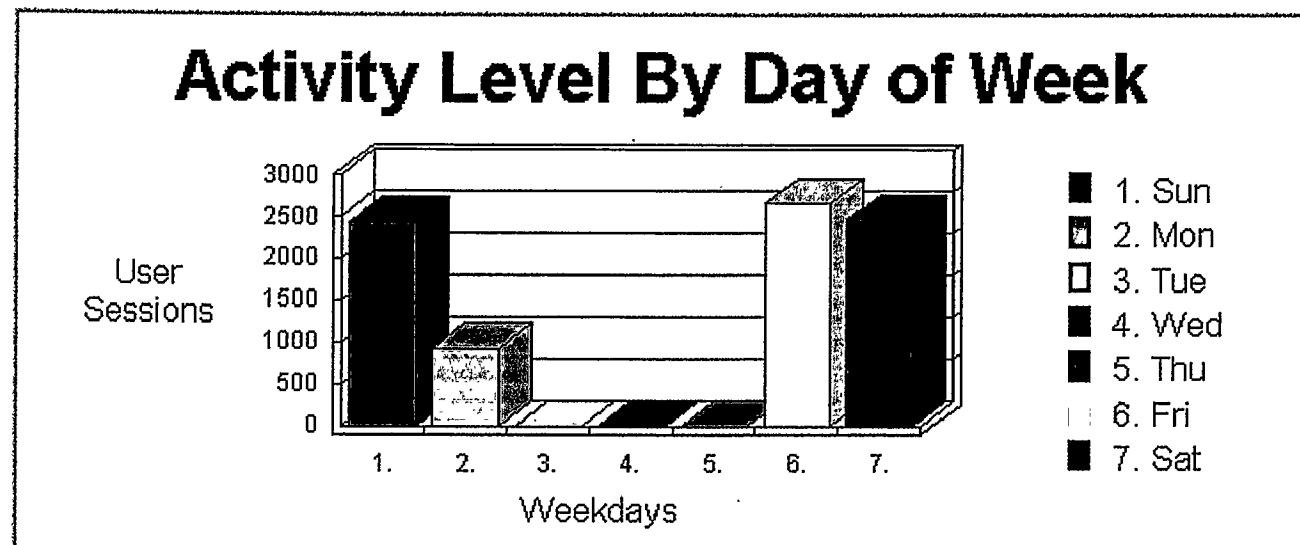
Fri 11/20 - Mon 11/23 (1 Week Scale)

Summary of Activity by Time Increment

| Time Interval | Hits | Page Views | KBytes Transferred | User Sessions |
|---------------|----------------|---------------|--------------------|---------------|
| 11/20 | 41,866 | 8,576 | 404,416 | 2,660 |
| 11/21 | 35,160 | 8,021 | 358,598 | 2,469 |
| 11/22 | 46,378 | 15,557 | 453,056 | 2,436 |
| 11/23 | 19,360 | 5,857 | 189,006 | 924 |
| Total | 142,764 | 38,011 | 1,405,076 | 8,489 |

Activity Level by Day of Week

This section shows the activity for each day of the week for the report period (i.e. if there are two Mondays in the report period, the value presented is the sum of all hits for both Mondays.) Values in the table do not include errored hits.



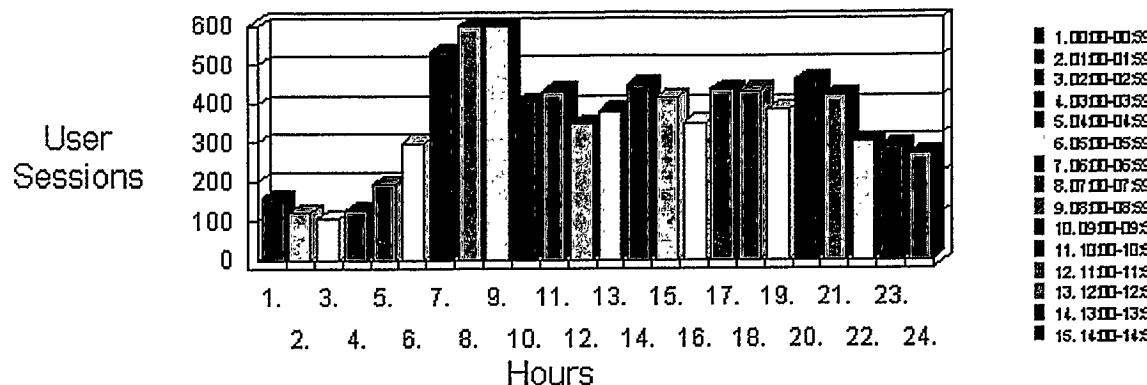
Activity Level by Day of the Week

| | Day | Hits | % of Total Hits | User Sessions |
|---|----------------|--------|-----------------|---------------|
| 1 | Sun | 46,378 | 32.48% | 2,436 |
| 2 | Mon | 19,360 | 13.56% | 924 |
| 3 | Tue | 0 | 0% | 0 |
| 4 | Wed | 0 | 0% | 0 |
| 5 | Thu | 0 | 0% | 0 |
| 6 | Fri | 41,866 | 29.32% | 2,660 |
| 7 | Sat | 35,160 | 24.62% | 2,469 |
| | Total Weekdays | 61,226 | 42.88% | 3,584 |
| | Total Weekend | 81,538 | 57.11% | 4,905 |

Activity Level by Hour of the Day

This section shows the most and the least active hour of the day for the report period. The second table breaks down activity for the given report period to show the average activity for each individual hour of the day (if there are several days in the report period, the value presented is the sum of all hits during that period of time for all days). All times are referenced to the location of the system running the analysis.

Activity Level By Hour of Day



Activity Level by Hour of the Day

| | |
|------------------------------|-------------|
| Most Active Hour of the Day | 08:00-08:59 |
| Least Active Hour of the Day | 01:00-01:59 |

Activity Level by Hours Details

| Hour | # of Hits | % Of Total Hits | # of User Sessions |
|-------------|-----------|-----------------|--------------------|
| 00:00-00:59 | 2,627 | 1.84% | 158 |
| 01:00-01:59 | 2,141 | 1.49% | 119 |
| 02:00-02:59 | 2,494 | 1.74% | 106 |
| 03:00-03:59 | 2,357 | 1.65% | 128 |
| 04:00-04:59 | 2,869 | 2% | 192 |
| 05:00-05:59 | 4,425 | 3.09% | 298 |
| 06:00-06:59 | 8,378 | 5.86% | 533 |
| 07:00-07:59 | 12,649 | 8.86% | 598 |
| 08:00-08:59 | 13,731 | 9.61% | 597 |
| 09:00-09:59 | 7,374 | 5.16% | 404 |
| 10:00-10:59 | 7,107 | 4.97% | 432 |
| 11:00-11:59 | 6,578 | 4.6% | 348 |
| 12:00-12:59 | 7,908 | 5.53% | 380 |
| 13:00-13:59 | 8,261 | 5.78% | 448 |
| 14:00-14:59 | 6,318 | 4.42% | 413 |
| 15:00-15:59 | 5,595 | 3.91% | 350 |
| 16:00-16:59 | 6,716 | 4.7% | 433 |
| 17:00-17:59 | 7,015 | 4.91% | 432 |
| 18:00-18:59 | 5,865 | 4.1% | 384 |
| 19:00-19:59 | 6,139 | 4.3% | 461 |
| 20:00-20:59 | 5,865 | 4.1% | 418 |
| 21:00-21:59 | 3,658 | 2.56% | 300 |
| 22:00-22:59 | 3,428 | 2.4% | 288 |
| 23:00-23:59 | 3,266 | 2.28% | 269 |

| | | | |
|--|--------|--------|-------|
| Total Users during Work Hours (8:00am-5:00pm) | 69,588 | 48.74% | 3,805 |
| Total Users during After Hours (5:01pm-7:59am) | 73,176 | 51.25% | 4,684 |

Technical Statistics and Analysis

This table shows the total number of hits for the site, how many were successful, how many failed, and calculates the percentage of hits that failed. It may help you in determining the reliability of the site.

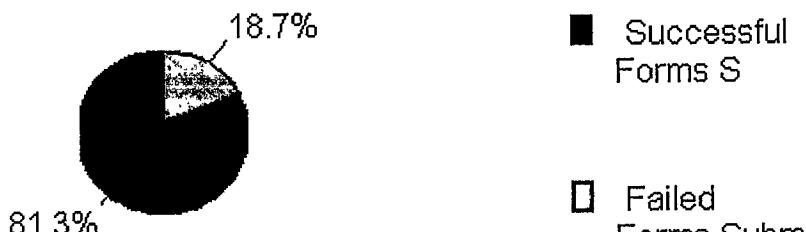
| Technical Statistics and Analysis | |
|-----------------------------------|---------|
| Total Hits | 157,076 |
| Successful Hits | 142,764 |
| Failed Hits | 14,312 |
| Failed Hits as Percent | 9.11% |
| Cached Hits | 17,789 |
| Cached Hits as Percent | 11.32% |

Forms Submitted By Users

This section shows the number of successful form submissions compared to the number that failed. WebTrends considers anything with Post command as a form.

Forms Submitted By Users

Percent
of Total
Hits

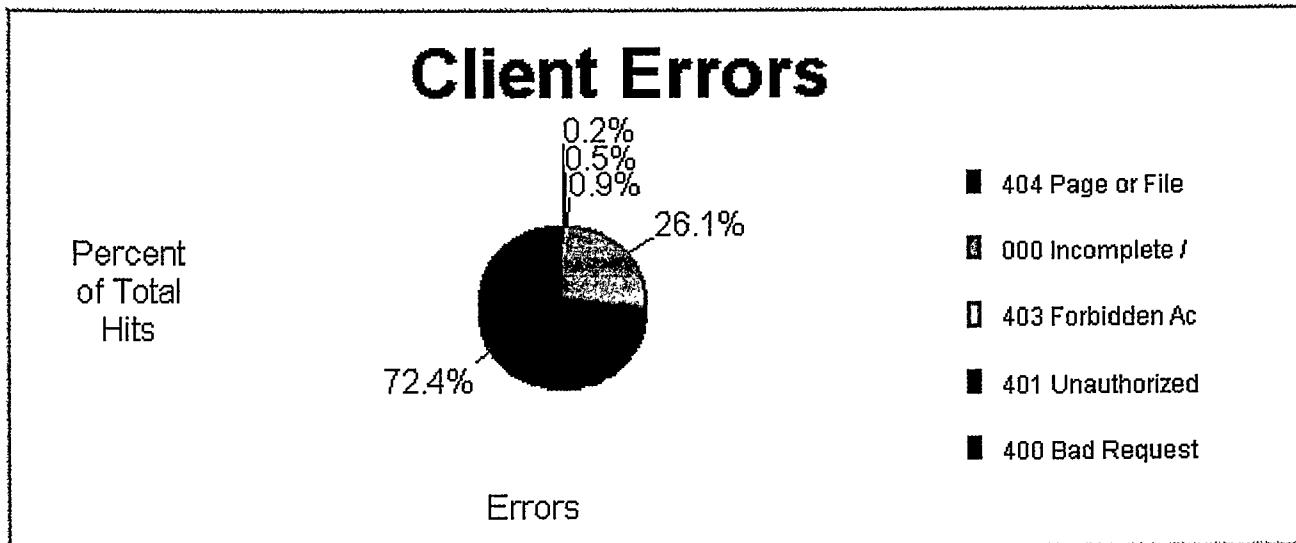


Forms

| Forms Submitted By Users | | |
|---------------------------------|--------------|-------------|
| Type | Hits | % of Total |
| Successful Forms Submitted | 3,082 | 81.31% |
| Failed Forms Submitted | 708 | 18.68% |
| Total | 3,790 | 100% |

Client Errors

This section identifies the type of errors which were returned by the Client accessing your server.



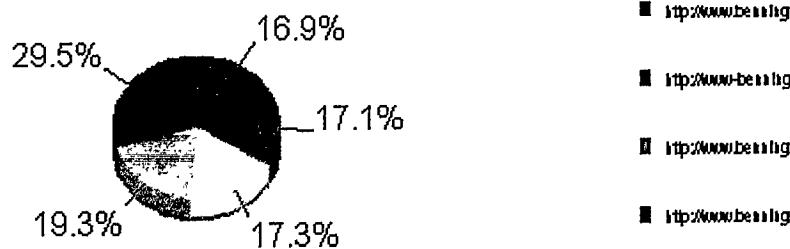
| Error | Hits | % of Total |
|----------------------------|---------------|-------------|
| 404 Page or File Not Found | 8,523 | 72.41% |
| 000 Incomplete / Undefined | 3,070 | 26.08% |
| 403 Forbidden Access | 102 | 0.86% |
| 401 Unauthorized Access | 56 | 0.47% |
| 400 Bad Request | 18 | 0.15% |
| Total | 11,769 | 100% |

Page Not Found (404) Errors

This section identifies "Page Not Found" (404) errors which occurred on the server.

Page Not Found (404) Errors

Percent
of Total
Hits



Page Not Found Errors

Page Not Found (404) Errors

Target URL and Referrer

<http://www.benning.army.mil/fbhome/Training/bkgMain.JPG>
(no referrer)

<http://www-benning.army.mil/fbhome/MAPS/images/limegreen.gif>
(no referrer)

http://www.benning.army.mil/What_about_the_accusations_that_the_School_teaches_torture_and_murder
(no referrer)

http://www.benning.army.mil/human_rights_training/_Additionally,_human_rights_are_continuously_discus
(no referrer)

http://www.benning.army.mil/Why_do_some_demonstrators_want_to_go_to_jail
(no referrer)

http://www.benning.army.mil/Does_the_School_really_have_a_Hall_of_Fame_or_Hall_of_Shame_as_cited
(no referrer)

<http://www-benning.army.mil/fbhome/11th/Airborne/3D Diamond.gif>
(no referrer)

http://www.benning.army.mil/other_words,_they_lost_the_war,_were_expelled_from_the_region,_and_now
(no referrer)

http://www.benning.army.mil/What_about_the_torture_manual_issue/is_this_true?_No/_There_were_seven
(no referrer)

http://www.benning.army.mil/they_believe_that_Latin_American_countries_do_not_have_the_inherent_right
(no referrer)

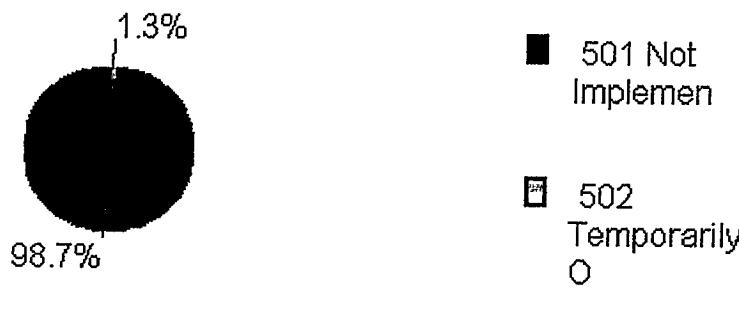
Total

Server Errors

This section identifies by type the errors which occurred on the server.

Server Errors

Percent
of Total
Hits



Errors

Server Errors

| Error | Hits | % of Total |
|----------------------------|-------|------------|
| 501 Not Implemented | 2,509 | 98.66% |
| 502 Temporarily Overloaded | 34 | 1.33% |
| Total | 2,543 | 100% |

WEBTRENDS

This report was generated by WebTrends.

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/09/1998

To: FBIHQ

Attn: IA [redacted]

From: New York

C-37

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] :11m

Case ID #: 288-NY-268557 (Pending) 30

b6
b7c

Title: ELECTRONIC DISTURBANCE THEATER;
[redacted]

CITA

OO:NY

Synopsis: Current status of ELECTRONIC DISTURBANCE THEATER (EDT) investigation.

Administrative: Re: telcal between SA [redacted] and IA [redacted] on 12/09/1998.

b6
b7c

Details: Information provided below is supplied pursuant to IA [redacted] request for information and status of investigation of EDT. This analysis is merely a summary of the facts and investigation at this time.

EDT is a group which claims on its Internet web site to protest various national and international policies through orchestrated attacks on computer systems. The attacks employ a program called "FloodNet" which causes a denial of service to targeted computers. EDT's Internet web site solicits visitors to participate in coordinated attacks of computer systems chosen by EDT. Participants simply click on the FloodNet icon on the EDT web site at a predetermined and published date and time.

Clicking on this icon initiates a Java applet. The initial version of the applet caused repeated reloading of files from the victim's computer system at an unusually high rate. Further versions of the applet have used the same repetitive reloading technique modified to optimize the impact on a targeted web site. This activity, when multiplied by many users, will cause service interruptions and possibly crash the server computer unless early detection is made and countermeasures are implemented. The visitors do not control the destination of the attack, rather it is programmed into the applet on the EDT's web site.

UPDATED

288-NY-268557-30

| | |
|----------------|---------|
| SEARCHED | INDEXED |
| SERIALIZED | FILED |
| DEC 10 1998 | |
| FBI - NEW YORK | |

by

WITH/TD [initials]
WITH/C [initials]
BY CM
DATE 12-21-98

fbihq.wpd

To: FBIHQ From: New York
Re: 288-NY-268557, 12/09/1998

EDT claims to have orchestrated at least five other attacks on targeted web sites. The NYO's investigation is focusing on two of EDT's most recent FloodNet attacks. The first of the attacks under investigation occurred on 09/09/1998. This attack targeted Mexican President Zedillo's web site, the Frankfurt Stock Exchange web site, and a Department of Defense web site: defenselink.com. The Department of Defense's initial analysis of the attack showed a fourfold increase in Internet traffic. This increase continued even after traffic was blocked from Austria, the origin of a significant portion of the traffic. The attack resulted in a severe increase in server latency which would have crashed the system without the active efforts of the defenseLINK system administrators. Analysis of this attack continues.

The second attack targeted the School of the Americas (SOA) web site, resident on the computer system of Ft. Benning, on 10/22/1998. Because of EDT's public announcement of this attack on its web site, SOA, with the assistance of the Defense Department computer emergency response team, was able to minimize the effect of the attack. Although prepared for the attack, Ft. Benning's computer systems suffered a slow down in computer response time similar to the DefenseLINK attack. Analysis of this attack continues.

Another attack is planned for 12/22/1998 in commemoration of the Acteal Massacre in Chiapas, Mexico. No target has been publicly announced nor identified.

Subject [redacted] has announced through his web site b6 b7C that EDT intends to release the FloodNet Java applet to the public on 01/01/1999. This release will allow non-EDT individuals to modify the applet and solicit attacks on targets of their choosing. The potential impact of the release of the Java applet is not significant due to the fact that a similar Java applet would not be difficult to author. However, the release would permit individuals without significant programming ability to use the FloodNet premise for their own designs.

The case has been presented to the Office of the United States Attorney for the Southern District of New York and has been assigned to an Assistant U.S. Attorney. Both the U.S. Attorney's Office and NYO is continually examining its investigative strategies paying close attention to potentially sensitive media topics involving freedom of speech and right to protest.

♦♦

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/08/1998

To: New York

From: New York

C-37

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]:11m

b6
b7C

[initials]
[signature]

✓ Case ID #: 288-NY-268557

Title: ELECTRONIC DISTURBANCE THEATER;
[redacted]

CITA;
OO:NY

Synopsis: [redacted]

Details: Subject Electronic Disturbance Theater (EDT) is a group claiming on its Internet web site to protest various national and international policies through orchestrated attacks on computer systems. The attacks employ a program called "FloodNet" which causes a denial of service to the target computer. To date, the EDT has orchestrated attacks on Federal Government computer systems as well as foreign government computer systems.

b6
b7C
b7E

SA [redacted] is in the process of [redacted] from Ft. Benning for all Internet traffic on 11/22/1998 during the EDT's FloodNet attack of their web site for the School of the Americas. DefenseLink, a Pentagon site, has also [redacted] from the 10/09/1998 FloodNet attack. [redacted]

C-37's [redacted]

[redacted]

[redacted]

288-NY-268557-31
cm cm

Costcost.wpd

UNCLASPED

WITH/TEST: ✓ _____
WITH CO: _____
BY: CM _____
DATE: 12-21-98

gd

288-NY-268557-
B2

| | |
|------------|---------|
| SEARCHED | INDEXED |
| SERIALIZED | FILED |
| CM | |

FEB 2 1 1998

REFERENCE: DEC mailing list / 12/18 Fugitive Action

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

CITAC

FYI.

Date: 12/17/98 15:08:45
From: [REDACTED]
Subject: I&W[EDT-Floodnet-White House website-tomorrow(Friday)]
To: See Below

Subject: INFOWAR: CALL FOR FLOODNET ACTION FOR PEACE IN THE MIDDLE EAST
Date: Thu, 17 Dec 1998 11:41:53 -0500
From: [REDACTED]
Reply-To: infowar@aec.at
To: "infowar@aec.at" <infowar-en@aec.at>

ARS ELECTRONICA FESTIVAL 98 INFOWAR. information.macht.krieg Linz,
Austria, september 07 ~ 12 http://www.aec.at/infowar

>From the Electronic Disturbance Theater

CALL FOR FLOODNET ACTION FOR PEACE IN THE MIDDLE EAST VIRTUAL SIT-IN ON
THE WHITE HOUSE WEB SITE

Friday, December 18, 1998 ← Tomorow

FROM 10:00 AM TO 4:00 PM (Washington D.C. TIME)

FROM 4:00 PM TO 10:00 PM (GMT- GREENWICH MEAN TIME)

<http://www.aurorablue.org/projects/rdom/zapsPublic/ddkfoyer.htm>

We oppose the U.S. military attack on Iraq and believe that the timing of this assault is designed to detract attention from President Clinton's impending impeachment hearing in Congress.

We do not accept the logic of the White House and the Pentagon that Iraq poses a national security threat. If any country is guilty of harboring weapons of mass destruction it is the United States.

We know that the U.S. government views the Middle East as a strategic area because, in part, it is an oil rich region. And we know the United States consistently uses the veil of "national security" as a means to pursue and justify its agenda of global economic domination.

We support the skeptical and angry views of the Russian, Chinese, and Iraqi ambassadors to the United Nations Security Council who strongly voiced their opposition to U.S. and U.K. aggression against Iraq.

We are saddened by the images on CNN of the innocent people who were injured in the first hours of the aerial bombardment. Moreover, we are aware that these victims are just a few of the hundreds of thousands of Iraqis who have either died or suffered greatly since the first Gulf War in 1991 and under U.S. backed sanctions that have existed since then.

We support the lifting of sanctions against Iraq. We support the efforts of international human rights organizations, groups like Friendship Across Frontiers, and other sectors of international civil society who have been working for years to help the Iraqi people.

We do not support Saddam Hussein but we believe it is not our right as Americans to go beyond merely having opinion. It is up to the Iraqi people, and others in the Arab world, to remove Saddam Hussein from office, if that is their desire and will.

We believe the age of imperialism should come to an end. It is quite telling that the imperial power of the 19th century, Great Britain, and the imperial power of the 20th century, the United States, have joined forces alone as we enter the 21st century.

In one instance, we agree with a characterization of the United States,

b6
b7C

DEC-21-1998 09:50

CITAC

202 324 0311 P.03/03

made by Iraqi leaders. The history of U.S. military and intelligence intervention, both covert and overt, in Latin America, Asia, Africa, the Middle East, and domestically within sovereign Native American territory, is enough evidence to support the classification of this country as an Evil Empire.

We support all efforts to denounce, oppose, protest, and resist the joint U.S.-U.K assault on Iraq, both domestically within the United States and England, in other European countries, in Middle Eastern countries, and throughout the world.

We recognize that resistance to the current bombardment of Iraq, and resistance to all future war, will take place in two spheres. One is on the ground, in the streets, in offices, in universities, in factories - in real spaces. The other is on the Net, in what the Pentagon now calls "battlespace." And we support the development and practice of joint virtual-real actions of resistance.

We do not believe that only nation-states have the legitimate authority to engage in war and aggression. And we see cyberspace as a means for non-state political actors to enter present and future arenas of conflict, and to do so across international borders.

We do not know how long the current U.S.-U.K. aerial assault on Iraq will last. Indications are that it will be short-lived. It may therefore not be an appropriate or strategic moment to attempt to inspire, coordinate, and sustain a campaign of virtual-real actions of resistance.

We do feel, however, compelled to take some action. And therefore we will use FloodNet, the same tool we have been using against web sites of the Mexican government, to now make a symbolic gesture of our opposition to the current assault on Iraq.

We therefore urge all people of good conscience who have the clarity of mind to oppose these aerial assaults to join us in a ongoing, nonviolent, virtual sit-in on the White House web site. We urge you to join us in a FloodNet Action for Peace in the Middle East.

Friday, December 18, 1998

FROM 10:00 AM TO 4:00 PM (Washington D.C. TIME)

FROM 4:00 PM TO 10:00 PM (GMT- GREENWICH MEAN TIME)

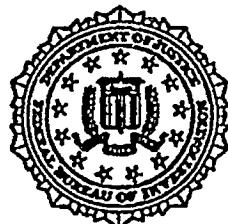
<http://www.aurorablue.org/projects/rdom/zapsPublic/ddkoyer.htm>

The Electronic Disturbance Theater

To:
To:
To:
To:
To:
To:
To:
To:

b6
b7C

TOTAL P.03



FBI FACSIMILE

COVER SHEET

b6
b7C

PRECEDENCE

- Immediate
- Priority
- Routine

CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- Unclassified

Time Transmitted:

Sender's Initials:

Number of Pages:

(including cover sheet)

To: KA

Name of Office

Date: 12/21/98

Facsimile Number:

Attn:

From: HQ/wrc

Name of Office

Subject: EDT

Special Handling Instructions:

Originator's Name:

Telephone:

Originator's Facsimile Number:

Approved:

Brief Description of Communication Faxed: Info Only

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18 USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

288-NY-268557-33

SEARCHED INDEXED
SERIALIZED FILED CM

MFC 21 1998

reference: SEC Inform Schedule

overview



| | | | | |
|--------------------|----------------|---|--|---|
| 7.9. mo/ mon | 21:00 | Ars Electronica Opening Event | ----- | Hauptplatz |
| | 23:30-open end | Super Collider - a sound accelerator | ----- | Stadtwerkstatt |
| 8.9. di/ tue | 10:00-13:00 | symposium INFOWAR - information.macht.krieg | ----- | Brucknerhaus |
| | 10.00-19:00 | openX - eine Versuchsanordnung | ----- | Brucknerhaus |
| | 15:00-18:00 | symposium INFOWAR - information.macht.krieg | ----- | Brucknerhaus |
| | 20:00-21:30 | Global Hockets | Supreme Particles/From Scarch | Brucknerhaus |
| | 22:30 | Cyberarts Nightline:Censoratorium | R. Huber, Gisburg, A. Clementi, B. Wackernagel, M. Daliot, I. Bordon, R. Dorfmeister | O.K Centrum für Gegenwartskunst |
| | 23:30-open end | Super Collider - a sound accelerator | ----- | Stadtwerkstatt |
| 9.9. mi/ wed | 10:00-13:00 | symposium INFOWAR - information.macht.krieg | ----- | Brucknerhaus |
| | 10.00-19:00 | openX - eine Versuchsanordnung | ----- | Brucknerhaus |
| | 15:00-18:00 | Symposium INFOWAR - information.macht.krieg | ----- | Brucknerhaus |
| | 15:00-21:00 | CAVE Presentations | M. Benayoun/J.-B. Barrière, H. Bizri/ M. Roussos, B. Lintermann | Ars Electronica Center |
| | 19:00 | Solar - A Wardenclyffe Project | M. Peljhan/ Projekt Atol | Brucknerhaus |
| | 21:00 | Electronic Theatre | ----- | O.K Centrum für Gegenwartskunst |
| | 21:00 | Prix Ars Electronica Gala | ----- | Landesstudio Oberösterreich |
| | 21:00 open end | Super Collider - a sound accelerator | ----- | Ars Electronica Quarter, Stadtwerkstatt |
| | 19:00 | openX - eine Versuchsanordnung | ----- | Brucknerhaus |

(X)
Fahr

| | | | | |
|--|-------------------|--|--|---|
| 10.9. do/ thu | 11:00-17:00 | Prix Ars Electronica Forum | Computeranimation/Visual Effects | Landestudio Oberösterreich |
| | 20:00-21:30 | Pole | Granular Synthesis | Posthof |
| | 21:00-open end | Super Collider - a sound accelerator | ----- | Ars Electronica Quarter, Stadtwerkstatt |
| 11.9. fr/ fri | 10:00-18:00 | Prix Ars Electronica Forum | Computer, Interactive Kunst, .net | Landestudio Oberösterreich |
| | 22:30 | Cyberarts Nightline: Nerve Theory: "Shades of Catatonia" | T. Sherman/B. Loibner | O.K Centrum für Gegenwartskunst |
| | 22:30 | Staalplaat Sound of Music | Negativland, People like Us, Barbed, Muzictoerist | Posthof |
| | 21:00-open end | Super Collider - a sound accelerator | ----- | Stadtwerkstatt |
| 12.9. sa/ sat tägl./ daily | 22:30 | Staalplaat Sound of Music | Negativland, People like Us, Barbed, Muzictoerist | Posthof |
| | 10:00-19:00 | Installations | ----- | Ars Electronica Center |
| | 10:00-24:00 | Cyberarts 98: Prix Ars Electronica Exhibition | ----- | O.K Centrum für Gegenwartskunst |
| | 10:00-24:00 | U19 Cybergeneration | ----- | O.K Centrum für Gegenwartskunst |

0007 MRI 00181/352

OO LON FBINY FBIWF

DE RUCNFB #0002 3520309

ZNY EEEEE

O 180214Z DEC 98

FM DIRECTOR FBI (288-NY-268557)

TO ZEN/WHITE HOUSE SITUATION ROOM WASHINGTON DC/IMMEDIATE/

ZEN/US SECRET SERVICE WASHINGTON DC/IMMEDIATE/

LEGAT LONDON/IMMEDIATE/

INFO ZEN/CIA WASHINGTON DC//DDO CTC/C/OAG/EC/CCB/CTC///IMMEDIATE/

ZEN/DIRACIC FT GEORGE G MEADE MD//IAMD-C-ACIC///IMMEDIATE/

ZEN/DISA WASHINGTON DC//D16/D312/D3332///IMMEDIATE/

ZEN/DEPT OF COMMERCE WASHINGTON DC//FOR OSY///IMMEDIATE/

ZEN/SECDEF WASHINGTON DC//C3I///IMMEDIATE/

ZEN/DEPT OF ENERGY WASHINGTON DC//OPS DIV/NN62/CIAC///IMMEDIATE/

ZEN/DEPT OF JUSTICE WASHINGTON DC/IMMEDIATE/

ZEN/DEPT OF JUSTICE COMMAND CENTER WASHINGTON DC/IMMEDIATE/

ZEN/DEPT OF STATE WASHINGTON DC//DS/ITA/INR/TNR///IMMEDIATE/

ZEN/DEPT OF TRANSPORTATION WASHINGTON DC//S-60/S-80///IMMEDIATE/

ZEN/DEPT OF TREASURY WASHINGTON DC//MSTR///IMMEDIATE/

ZEN/GSA OFFICE INFO SECURITY WASHINGTON DC//PSE/FPS///IMMEDIATE/



wcc

OPC, 12-17-98

2

C-37 STANDBY ADVISED
1040AM

CP Notified - CP notified

C-37

288-NY-268557-34

| | |
|----------------|---------|
| SEARCHED | INDEXED |
| SERIALIZED | FILED |
| DEC 17 1998 | |
| FBI - NEW YORK | |

b6
b7c

CP direct to [redacted]

PAGE TWO DE RUCNFB 0002 UNCLAS E F T O

ZEN/DIRNSA FT GEORGE G MEADE MD//NSOC/SIPO/IPA///IMMEDIATE/

ZEN/WHITE HOUSE NATIONAL SECURITY COUNCIL WASHINGTON DC/IMMEDIATE/

FBI NEW YORK/IMMEDIATE/

FBI WASHINGTON FIELD/IMMEDIATE/

BT

UNCLAS E F T O

CITE: //1332//

PASS: DIRNSA FOR ZKZK OO ZSL DE; WHITE HOUSE SITUATION ROOM

PLEASE PASS TO EOP SECURITY OFFICE.

SUBJECT: NIPC COMPUTER INTRUSION ALERT: ALLEGED PLANNED ACTS OF
ELECTRONIC DISRUPTION TO TARGET WHITE HOUSE WEB SITE ON DECEMBER 18.

REFERENCE: DIRECTOR FBI WASHINGTON DC 090305Z SEP 98 (NOTAL),
CAPTIONED QUOTE ALLEGED ACTS OF ELECTRONIC DISRUPTION TO TARGET
CERTAIN U.S., MEXICAN, AND GERMAN INTERNET-BASED SITES AND
SERVICES, SEPTEMBER 9 THROUGH NOVEMBER 22, 1998, IN SYMPATHY WITH
ZAPATISTA MOVEMENT UNQUOTE.

WARNING NOTICE: ALTHOUGH UNCLASSIFIED, THIS COMMUNICATION SHOULD NOT
BE FURNISHED TO THE MEDIA OR OTHER AGENCIES OUTSIDE THE LAW
ENFORCEMENT/U.S. GOVERNMENT COMMUNITY WITHOUT THE PERMISSION OF
THE FBI/NIPC. UNAUTHORIZED DISCLOSURE OF FBI COMMUNICATIONS COULD

JEOPARDIZE ONGOING FBI INVESTIGATIONS.

1. AN ENTITY KNOWN AS THE QUOTE ELECTRONIC DISTURBANCE THEATER UNQUOTE (EDT), HAS CALLED FOR A QUOTE VIRTUAL SIT-IN ON THE WHITE HOUSE WEB SITE FROM 10:00 AM TO 4:00 PM (WASHINGTON, D.C. TIME) UNQUOTE ON DECEMBER 18. THIS IS THE LATEST ROUND OF ACTIONS CARRIED ON THE EDT'S PUBLICLY-ACCESSIBLE WEB SITE ([HTTP://WWW.THING.NET/\(TILDE\)RDOM/ECD/ECD.HTML](http://WWW.THING.NET/(TILDE)RDOM/ECD/ECD.HTML)). IN A RECENT MASS E-MAILING, THE EDT CLAIMS ITS ACTIONS HAVE BEEN PROMPTED BY THE RECENT COMBINED U.S. AND UK COMBINED MILITARY ACTION AGAINST IRAQ. THE EDT IS A GROUP CONSISTING OF ACTIVISTS WHO HAVE, IN THE PAST, PRIMARILY TARGETED U.S. AND MEXICAN GOVERNMENT SITES IN SUPPORT OF MEXICO'S ZAPATISTA NATIONAL LIBERATION ARMY (EZLN).

2. THE EDT HAS A HISTORY OF CARRYING OUT ITS THREATS UTILIZING FLOODNET, A DENIAL-OF-SERVICE SOFTWARE TOOL, DESIGNED TO DISRUPT ACCESS TO TARGETED WEB SITES BY FLOODING THE HOST SERVER WITH REPEATED REQUESTS FOR THAT WEB PAGE. TO ACCOMPLISH THIS, FLOODNET USERS SIMPLY LEAVE THEIR BROWSERS OPEN, WHICH ALLOWS THE FLOODNET APPLET TO AUTOMATICALLY RELOAD A TARGET WEB PAGE EVERY FEW SECONDS. THIS TOOL ALSO ALLOWS THE USER TO POST HIS OWN MESSAGES ON THE TARGET WEB PAGE.

PAGE FOUR DE RUCNFB 0002 UNCLAS E F T O

3. ON SEPTEMBER 9, 1998 THE EDT MOUNTED AN UNSUCCESSFUL ATTACK ON A DOD WEB SITE USING FLOODNET. ON OCTOBER 5, 1998, THE GROUP SPONSORED A DEMONSTRATION OUTSIDE THE FEDERAL COMMUNICATIONS COMMISSION (FCC) HEADQUARTERS BUILDING IN WASHINGTON D.C. THE GROUP STATED THAT IT WAS QUOTE PROTESTING THE FCC'S ROLE IN SUPPRESSING FREE SPEECH ON THE AIRWAVES UNQUOTE. ON NOVEMBER 22, THE GROUP TARGETED THE U.S. ARMY'S SCHOOL OF THE AMERICAS WEB SITE FOR A FLOODNET ACTION.

4. NATIONAL INFRASTRUCTURE PROTECTION CENTER (NIPC) COMMENT: THE EDT'S PAST ELECTRONIC CIVIL DISOBEDIENCE ACTIONS HAVE SHOWN IT IS DETERMINED TO PURSUE ITS ANNOUNCED AGENDA. HOWEVER, BASED ON ITS PAST ACTIONS, THE EDT DOES NOT APPEAR TO POSSESS THE SOPHISTICATION AND ORGANIZATION TO POSE A SERIOUS, WELL-COORDINATED CYBER THREAT AT PRESENT. AT THE SAME TIME, ITS POLITICAL AGENDA HAS BEEN SOMEWHAT SUCCESSFUL DUE TO THE MEDIA COVERAGE IT HAS RECEIVED.

5. CONTACT POINT IS THE [REDACTED] AT [REDACTED] b7E

6. LEGAT LONDON: PLEASE NOTIFY APPROPRIATE BRITISH GOVT. REPRESENTATIVES FOR THEIR INFORMATION.

BT

#0002

NNNN

288-NY-268-557-35

SEARCHED INDEXED
SERIALIZED FILED CM

DEC 21 1998

12/21/98

REFERENCE: ECD USEAGE

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

electronic civil disobedience



Next Virtual Sit-in on
December 22
Anniversary of the Acteal massacre
in Chiapas



Two recent News segments on
The Electronic Disturbance Theater
First one is a quicktime mov. from
New Media News.

Also

*How To Make Trouble
and Influence People*

by Ian Walker

An hour long RealAudio on
Culture Jammers around the world.
Featuring interviews with
RT@Mark, Adbusters,
The Electronic Disturbance Theater,
and many more.



Mid-way into the Sit-In
at School of the Americas
on November 22
Fort Benning countered
by IP Blocking Address

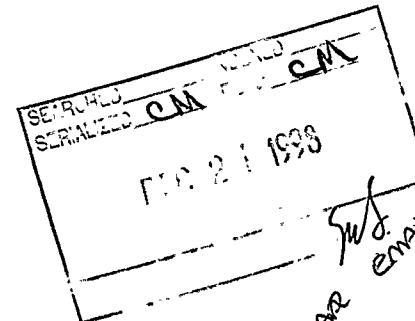
We will post updates as more
information flows in!

Recent Action Against
The Thing's
Support of FloodNet
VIOLATION OF THE VERIO
ACCEPTABLE USE POLICY
Read About It On Thing.news. In
Threads.

SWARM Chronology

(X)
JW

288-NY-268557 -36



Reference: AEC INFRASTRUCTURE
SAC email: matusz@ust

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG



You have three choices on this page: you can

1. subscribe to the English mailing list;
2. to the German mailing list;
3. or to both mailing lists.

As mentioned in the instructions, this is an experiment; the main focus of the discussion will take place on the web page, but we don't want anyone to feel left out, so here we offer you the choice to subscribe to the mailing list in the language of your choice. In order to get the whole discussion, you will obviously have to subscribe to both lists (or read it on the web site); but for those of you who prefer only one language, the mailing list would be the safest bet.

This form allows you to subscribe to the Info War English-language mailing list, which directs messages to be delivered to your Internet e-mail address. You will receive e-mail confirmation of your subscription. You can also use this form to change the name associated with your subscription. Just enter the same address under which you are subscribed with Majordomo and enter a new name.

Your Full Name:

Your Email Address:

Sie haben drei Möglichkeiten auf dieser Seite können

1. die englische mailing list abonnieren;
2. die deutsche mailing list abonnieren;
3. oder beide mailing lists erhalten.

Diese Seiten stellen ein Experiment dar, wie der Anleitung erwähnt; das Augenmerk der wird auf der Webseite liegen, aber wir wollen ausschließen, so daß wir hier die Möglichkeit eine mailing list in der Sprache Ihrer Wahl zu abonnieren. Um alle Beiträge verfolgen zu können müssen Sie natürlich beide Listen abonnieren (Webseiten lesen); doch für diejenigen, die lieber einer Sprache lesen wollen, ist die mailing list Wahl.

Diese Form erlaubt es Ihnen, die deutsche mailing list zu abonnieren, die Nachrichten an Ihre Internet e-mail Adresse liefert. Sie bekommen eine e-mail eine Bestätigung Ihres Abonnements können diese Form auch verwenden, um die e-mail Adresse assoziierten Namen zu ändern müssen nur die gleiche e-mail Adresse angeben der Majordomo Sie kennt, und Ihren neuen Namen eingeben.

Ihr Name:

Ihre Email-Adresse:

b6
b7c

DISCUSSION DEUTSCH - ENGLISH | MATERIAL | INSTRUCTIONS | LINKS



288-NY-268557-37

| | |
|----------------|----------|
| SEARCHED | INDEXED |
| SERIALIZED CM | FILED CM |
| DEC 21 1998 | |
| FBI - NEW YORK | |

REFERENCE: FORBES ARTICLES A
1998

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

Forbes

By Adam L. Penenberg

When art meets cyberwar



Forum



Email



Archives

Adam Penenberg is a senior editor at Forbes magazine and a regular contributor to the Forbes Digital Tool.

PERHAPS THE FIRST electronic attack against a target on American soil was the result of an art project.

It all started in January of this year in chat rooms and newsgroups, when political activists, protesting the Mexican Government's suppression of Chiapas, organized "virtual sit-ins" on Mexico City financial institutions. For such a cutting-edge idea, the organizers had a decidedly low-tech strategy: Protestors were instructed to surf to one of the offending pages and keep hitting "reload," the theory being that if enough people did this, the site would be effectively blocked.

Realizing they were on to something, two activists, Ricardo Dominguez, a classically-trained actor, and Stefan Wray, a graduate student at New York University, decided to make an art project out of organizing political protests over the Internet. Brett Stalbaum, a Java programmer and graduate art student at San Jose State University in California, told them he could automate the process. Together, they formed the Electronic Disturbance Theater.

Stalbaum coded a Java applet he called FloodNet, which would, when accessed, launch a denial of service attack. As a Java reload function, it would request search engines on targeted sites to look up words like "justice," "egalitarianism" and "human rights" every seven seconds. The sheer number of



Franklin Templeton

MUTUAL FUNDS PENSION EQUITY

For nearly half a century, Mutual Series has used a value-driven philosophy that has consistently guided investors through the inevitable highs and lows in the securities market. For more info on these value-driven funds

[INVESTOR CENTER](#)

TELEFONICA ASIAN INVESTMENT EQUITY

Many in the world view Asian markets with apprehension. Templeton understands this concern, but we also see unprecedented opportunities. To find out how to invest in these opportunities

[INVESTOR CENTER](#)

Franklin TAX-FREE MUNICIPALS

Taxes impact all of us. Franklin was one of the first pioneers of the tax-free "mutual fund" concept. For more info of tax-free investing

[INVESTOR CENTER](#)



Enter Franklin Templeton
Online

requests for information would slow down site traffic to a crawl-- as if protestors had actually showed up and barricaded themselves inside the site.

On Apr. 10, eight thousand protestors visited the The Electronic Disturbance Theater site over a four-hour period, clicked on the FloodNet button and intermittently blocked Mexican President Zedillo's site. (Ironically, Zedillo's search engine replied that words like "justice," "egalitarianism" and "human rights" were not to be found anywhere on the site.) The group organized two more similar electronic events in May and June. In the second one, Mexican programmers had gotten wise and deployed a Java applet of their own, which successfully parried FloodNet.

By then, the Electronic Disturbance Theater was a rising star in lefty activist circles, and in September, Dominguez and Wray were invited to speak at Ars Electronica, an art and technology conference held in Austria. While there, they planned their biggest event: A simultaneous attack on Zedillo's web site (again), the Pentagon and the Frankfurt Stock Exchange.

But this time, the protestors were attacked in their own right. Stalbaum suspects that Pentagon programmers detoured FloodNet traffic into a hostile applet of its own, which caused browsers to crash. "They even called their applet 'hostile applet,'" says Stalbaum, who dissected it.

Dominguez loves the intrigue. "As a person of the theater, I couldn't have created a better script--the drama, the conflict."

This net-based counterattack, although minor in scope, raises important national security issues. Since the American military is not supposed to act within the nation's borders unless specifically directed, does the Pentagon have the right to counter any of the hundreds of hack attacks it receives every day with cyberattacks of its own? If so, will it be allowed to target sites in the U.S., as well as abroad? What limitations should be placed on our military when it comes to identifying and

acting on targets in cyberspace? Will we as a nation have to redefine the role of the military in the coming digital years?

As fascinating as I find these issues, Dominguez and Wray are more interested in retrofitting political activism for the millennium. Both of them come from activist backgrounds. Dominguez got his start working with nuclear fallout victims in southern Utah, then with Act Up (the AIDS activist group) in the '80s. Wray was a rabid anti-Gulf War protestor. Together they formed the genesis of The Electronic Disturbance Theater.

"Electronic civil disobedience began with Act Up, with phone trees and jamming opponents' fax machines," Dominguez says. "But after awhile we found that spectacular actions weren't getting the response from the media that they did before."

The Electronic Disturbance Theater's next event will be held on Dec. 22. The group's season-ending finale is scheduled for Jan. 1, 1999, when users will be encouraged to actually download a copy of the FloodNet software (complete with instructions) and distribute it to the masses. Part of the art project, it seems, is finding out what the activist community will end up doing with FloodNet.

Whether you agree or disagree with the group's politics is irrelevant. What is important is to acknowledge that The Electronic Disturbance Theater has come up with a cutting-edge way to use the Internet for mass political protest.

Look for the group's methods to spread to other factions, on the left and the right, as the Internet continues to transform the political landscape.

What do you think about this issue? You can contact me through the Forum, which can be accessed from this page.

External link:

The Electronic Disturbance Theater
(<http://www.thing.net/~rdom/ecd/archives.html>)

[Subscribe to Forbes](#) · [Letters to the Editor](#)

[Forbes Front Page](#) · [Forbes Magazine](#) · [The Toolbox](#)

[Sitemaps](#) · [Help](#) · [Search](#) · [Webmaster](#)

© 1998 Forbes Inc. [Terms, Conditions and Notices](#)

Date 12/18/98

Birth Credit Criminal Death INS Marriage* Motor Vehicle Other

D TEC

| | |
|------------------------|---|
| To <u>SA's</u> | Buded |
| Return to <u>SA</u> | File number Ex-3-385 288-NY- <u>268557</u> |

Name and aliases of subject, applicant, or employee, and spouse

| | |
|-----------|--------------------------|
| Addresses | <input type="checkbox"/> |
| Residence | <input type="checkbox"/> |
| Business | <input type="checkbox"/> |

X
dm

| | |
|--------|--------------------------|
| Former | <input type="checkbox"/> |
| | <input type="checkbox"/> |
| | <input type="checkbox"/> |

*Date and place of marriage
(if applicable)

b6
b7C
b7E

| | | | | | | |
|------|--|-----|--------|--------|------|------|
| Race | Sex <input checked="" type="checkbox"/> Male <input type="checkbox"/> Female | Age | Height | Weight | Hair | Eyes |
|------|--|-----|--------|--------|------|------|

| | |
|------------------------------|------------|
| Birth date <u>9/26/49</u> | Birthplace |
|------------------------------|------------|

| | | |
|---------------|----------------------------|--------------------|
| Arrest Number | Fingerprint classification | Criminal specialty |
|---------------|----------------------------|--------------------|

| | |
|------------------------|---|
| Social Security Number | Drivers License Number |
| | <input type="checkbox"/> D/L Photo <input type="checkbox"/> Other |

Specific information desired

Results of check

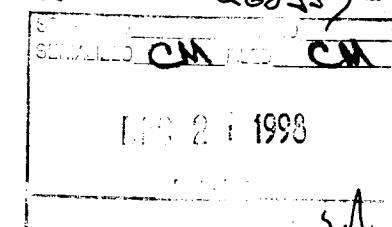
need an address.

288-NY-26855-38
SEARCHED CM INDEXED CM

DEC 21 1998

SA

12/18/98



Record Request
FD-125 (Rev. 4-1-93)

PLEASE
CALL WHEN
READY

Date 12/17/98

Birth Credit Criminal Death INS Marriage Motor Vehicle Other

*o

OPC

Buded

Return to

SA

File number

288-NY-268557

Name and all aliases or subject, applicant, or employee, and spouse

[Redacted]

NON pub /CA.

Addressess

Residence

Business

Former

*Date and place of marriage
(if applicable)

b6
b7C
b7E

| | | | | | | |
|------|---|-----|--------|--------|------|------|
| Race | Sex <input type="checkbox"/> Male <input type="checkbox"/> Female | Age | Height | Weight | Hair | Eyes |
|------|---|-----|--------|--------|------|------|

Birth date Birthplace

| | | |
|---------------|----------------------------|--------------------|
| Arrest Number | Fingerprint classification | Criminal specialty |
|---------------|----------------------------|--------------------|

| | |
|------------------------|------------------------|
| Social Security Number | Drivers License Number |
|------------------------|------------------------|

D/L Photo Other

Specific information desired

Results of check

[Redacted]

288-NY-268557-39

SLT-AZ-22 CM CM

12/17/98

12/17/98

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

SEARCHED INDEXED CM
SERIALIZED FILED CM
DEC 21 1998
FD-302

RECORDED: INTERNAL



[Home](#) [Contact Us](#) **Registration Services**
[RESOURCES](#) [HOW TO...](#) [FORMS](#) [FAQ](#) [SITE MAP](#) [SEARCH](#)

Whois Query Results

Registrant:

aurora.blue AURORABLUE-DOM
15710 Minnetonka Boulevard
Minnetonka, MN 55345

Domain Name: AURORABLUE.ORG

Administrative Contact, Technical Contact, Zone Contact:

Golightly, Sky SG687 sky@GOLIGHTLY.ORG
(408) 812-0613

Billing Contact:

Golightly, Sky SG687 sky@GOLIGHTLY.ORG
(408) 812-0613

Record last updated on 14-Aug-98.

Record created on 06-Feb-98.

Database last updated on 15-Dec-98 03:16:33 EST.

Domain servers in listed order:

| | |
|---------------|---------------------|
| ZONE.AREA.COM | <u>165.90.20.20</u> |
| NS.AREA.COM | <u>165.90.22.22</u> |



[Home](#) [Contact Us](#) **Registration Services**
[RESOURCES](#) [HOW TO...](#) [FORMS](#) [FAQ](#) [SITE MAP](#) [SEARCH](#)

Whois Query Results

Registrant:

Golightly GOLIGHTLY2-DOM
7055 Oak Ridge Rd.
Aptos, CA 95003

Domain Name: GOLIGHTLY.ORG

Administrative Contact, Technical Contact, Zone Contact:

Golightly, Sky SG687 sky@GOLIGHTLY.ORG
(408) 812-0613

Billing Contact:

Golightly, Sky SG687 sky@GOLIGHTLY.ORG
(408) 812-0613

Record last updated on 25-Sep-98.

Record created on 09-Dec-96.

Database last updated on 15-Dec-98 03:16:33 EST.

Domain servers in listed order:

| | |
|---------------|---------------------|
| ZONE.AREA.COM | <u>165.90.20.20</u> |
| NS.AREA.COM | <u>165.90.22.22</u> |



[Home](#) [Contact Us](#) [Registration Services](#)
[RESOURCES](#) [HOW TO...](#) [FORMS](#) [FAQ](#) [SITE MAP](#) [SEARCH](#)

Whois Query Results

Registrant:

Golightly GOLIGHTLY2-DOM
7055 Oak Ridge Rd.
Aptos, CA 95003

Domain Name: GOLIGHTLY.ORG

Administrative Contact, Technical Contact, Zone Contact:

Golightly, Sky SG687 sky@GOLIGHTLY.ORG
(408) 812-0613

Billing Contact:

Golightly, Sky SG687 sky@GOLIGHTLY.ORG
(408) 812-0613

Record last updated on 25-Sep-98.

Record created on 09-Dec-96.

Database last updated on 15-Dec-98 03:16:33 EST.

Domain servers in listed order:

| | |
|---------------|---------------------|
| ZONE.AREA.COM | <u>165.90.20.20</u> |
| NS.AREA.COM | <u>165.90.22.22</u> |

288-NY-268557 - 41

| | |
|---------------|----------|
| SEARCHED | INDEXED |
| SERIALIZED CM | FILED CM |
| DEC 23 1998 | |
| | |
| | |

East/PW

REFERENCE:

12/22/98 Action Against Mexican Stock Exchange

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

b6
b7C

Date: 12/19/98 11:41:23
From: [REDACTED]
Subject: FWD: (g2i) ECD: Floodnet targets mexican stockexchange - decembre
To: See Below

[REDACTED]
Principal Engineer

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

I&W for FloodNet.

Date: 12/18/98 5:19 PM
From: [REDACTED]

Subject: THE ZAPATISTA FLOODNET TARGETS THE MEXICAN STOCKEXCHANGE - December 22, 1998

THE ZAPATISTA FLOODNET TARGETS THE MEXICAN STOCKEXCHANGE IN MEMORY OF THE ACTEAL DEAD
DECEMBER 22, 1998

FROM 10:00 AM TO 4:00 PM (MEXICO CITY TIME)

FROM 4:00 PM TO 10:00 PM (GMT- GREENWICH MEAN TIME)

<<http://www.thing.net/~rdom>>

Dear sisters and brothers,

This time the Winds blow South. This Zapatista FloodNet sit-in is directed against the Mexican Stock Exchange, which has played a key role in enforcing the continued "low-intensity conflict" in the State of Chiapas.

Under the direction of the Mexican Government and with the support of the United States, the weapons and training for The Drug Wars are being used in Chiapas. Counterinsurgency orders were established by the Department of National Defense's *Chiapas Campaign Plan 1994* which makes explicit that the key objective is: "The breaking of the support relationship which exists between the population and the transgressors of the law." They have been building the intensity level ever since by using groups which make up the Mixed Operations Bases (BOM), which include paramilitary units, the Federal Army, the State Public Security agencies, the State and Federal Judicial Police, in addition to the immigration police, specifically in those areas where there are Zapatista Army of National Liberation (EZLN) sympathizers living.

On December 22, 1997, in Acteal 45 people were killed brutally by paramilitary groups, a community under the protection of the militarization. The Mexican government propaganda framed the massacre as the outcome of "intra and inter-community conflicts." The PRI party instead of pursuing the guilty and holding them responsible, it exploited it in order to reinforce the military presence in the entire state.

The killing was a State crime. The attack was planned and executed according to military counterinsurgency manuals. The purpose for the genocide was to combat the rebellious communities. There is evidence and testimonies in judicial records that point to official responsibility. The freedom enjoyed by the assassins in order to carry out their crime was incredible. More than 60 people--90 according to the Fray Bartolome Center--armed with AK-47 guns, 22 rifles and UZI machine guns fired their guns for seven hours against these people who had been praying at a hermitage.

The outcome: 45 dead, 22 wounded... and a people hurt forever. There are proofs that "40 members of the police were 200 meters away from the place where the crime took place and didn't do anything while the indigenous people were being massacred".

Alonso Vazquez Gmez Lorenzo Gmez Pirez, Marma Luna Mindez, Versnica Pirez Oyalti, Rosa Vazquez Luna, Sebastian Gmez Pirez, Versnica Vazquez Luna, Daniel Gmez Pirez, Micaela Vazquez Luna, Pablina Hernandez Vazquez, Juana Vazquez Luna, Roselia Gmez Hernandez, Juana Luna Vazquez, Graciela Gmez Hernandez, Marma Jiminez Luna, Guadalupe Gmez Hernandez, Susana Jiminez Luna, Marma Ruiz Oyalti, Miguel Jiminez Pirez, Catalina Vazquez Pirez, Marcela Luna Ruiz Catalina Luna Ruiz, Alejandro Luna Ruiz, Manuela Paciencia Moreno, Jaime Luna Ruiz, Margarito Gmez Paciencia, Regina Luna Pirez, Rosa Gmez Pirez Roselia Luna Pirez Doida Ruiz Gmez Ignacio Pukuj Luna,

b6
b7C

Agustmn Ruiz Gsmez Micaela Pakuj Luna, Rosa Pirez Pirez Victorio Vazquez Gsmez, Manuel Vazquez Pirez Agustmn Gsmez Ruiz Juana Vazquez Pirez Juana Pirez Josefa Vazquez Pirez Juan Carlos Luna Pirez Marcela Capote Vazquez Marcela Vazquez Vazquez, Marcela Capote Ruiz, Antonia Vazquez Vazquez,

***** Tuesday, December 15, 1998.

***** AMBUSH IN LOS PLATANOS *****

ZAPATISTAS DENY BEING RESPONSIBLE FOR AMBUSH IN LOS PLATANOS.

La Jornada.

In a communique signed by Comandantes David, Moises and Daniel, the EZLN denied any responsibility for the ambush of a group of PRI indigenous yesterday in the community of Los Platanos, municipality of El Bosque, and they said that, just a few days prior to the first anniversary of the Acteal massacre, the government is trying to distract public opinion and put the victims in the dock. Condemning the attack, in which one child was killed and 7 persons were wounded, the zapatistas held the federal government responsible and called on civil society to not be deceived, since the EZLN does not attack civilians, and the government does. They explained the ambush was due to an internal struggle between groups who are fighting for control of Los Platanos and for the money and equipment which the government is giving to paramilitary groups. The zapatista leadership added that, for a year now, Los Platanos has been under the control of paramilitary groups, Public Security police and federal soldiers, who permit or deny access to people there. The EZLN said that there is also evidence that Public Security collaborated in the attack, since, an hour after the ambush, 11 police officers arrived in a community near Los Platanos, asking for help in escaping. Some 370 PRI families live in Los Platanos, who expelled 34 zapatista families in late April, who were in refuge in nearby locales. So far this year, five PRI indigenous persons have died, and more than 24 have been wounded as a consequence of eight armed attacks.

This information was provided as a service of Zapatistas Online.

The Electronic Disturbance Theater Invites the World Wide Community To Celebrate The Fifth Anniversary of The Zapatista Manifestation on January 1, 1999.

At one minute after midnight, we will release the Public Version of the Zapatista FloodNet. Which individuals and groups will be able to download and use for Virtual Sit-Ins the day after and In the days to come.

The URL to the Public Version of the Zaptatista FloodNet will be found at one minute after midnight at:

<<http://www.fakeshop.com>>

Please join us. The Electronic Disturbance Theater

THE ZAPATISTA FLOODNET TARGETS THE MEXICAN STOCKEXCHANGE IN MEMORY OF THE ACTEAL DEAD

DECEMBER 22, 1998

FROM 10:00 AM TO 4:00 PM (MEXICO CITY TIME)

FROM 4:00 PM TO 10:00 PM (GMT- GREENWICH MEAN TIME)

<<http://www.thing.net/~rdom>>

RFC822 header

Received: from mbunix.mitre.org (mbunix [129.83.20.100])
by mail91.mitre.org (8.8.8+Sun/8.8.8) with ESMTP id RAA26925

TOTAL P.03



**FBI FACSIMILE
COVER SHEET**

b6
b7c

PRECEDENCE

- Immediate
 - Priority
 - Routine

CLASSIFICATION

- Top Secret
 Secret
 Confidential
 Sensitive
 Unclassified

Time Transmitted:

Sender's Initials:

Number of Pages

(including cover sheet)

To: _____ Name of Office

Date: 12/31/98

Faxsimile Number:

Attn: _____ Name _____ Room _____

From: 11/9/0078 Name of Office

Subject:

Special Handling Instructions:

Originator's Name:

Telephone:

Originator's Facsimile Number:

Approved:

Brief Description of Communication Faxed:

WARNING

WARNING
Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18 USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

12/18/98

On December 18, 1998, SA [redacted] printed out the web pages located at the Uniform Resource Locator (URL) of <http://www.wellengaged.com/engaged/wrap.cgi/formes.cgi?c=forbes&f0&t=2>, titled [redacted] Forum." The forum was linked to the Forbes newsarticle titled "When art meets cyberwar" by [redacted]. This article found at the URL of <http://www.forbes.com/penenberg/index.htm>.

b6
b7c

(X)
JRW

42

288-NY-268557-
SEARCHED SERIALIZED CM CM
DEC 21 1998
SAC

UPLOADED

WITH/TEXT ✓
WITH/OUT TEXT _____
BY CM
DATE 12-24-98

Investigation on 12/18/1998 at New York

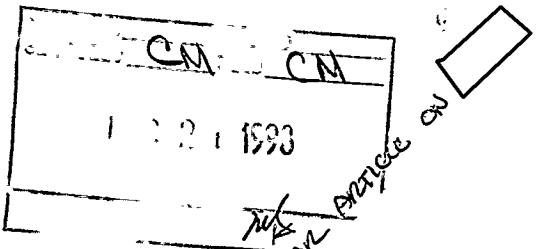
File # 288-NY-268557 Date dictated 12/18/1998

by SA [redacted] b6

b7C

Forbes.wpd

288-NY-268557-44



RELEASER: AEC INFOWAR
DATE: 12-28-2015 BY C32W33B91 NSICG

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG

THEMEN - INFOWAR

Eric Kluitenberg
InfoWar Reflection #1

This should be the first of a small series of informal notes from the Ars Electronica Festival 1998, which devotes itself to the theme InfoWar (you all know that). And there is a regular infowar going on, it seems, in the lobby of the Bruecknerhaus, where experimental soundscapes continuously bombard our senses, deregulating and disinforming them, dissociating understanding from perception, competing for wetware input channels, in the face of adverse machinic output channels that crowd the environment in abundance.



Yesterday there was a relative calm (before the storm? - no desert this time though!). We were enjoying the calm view on the River Danube, flowing softly along the banks of the city Linz. The paysan scene was hardly reminiscent of the electronic disorder that was impeding upon us, within a matter of a few hours. Yesterday we muttered words in the net, and the air even, as we watched the sun set over the river and some distant hills, while we interviewed some of the distinguished guests of the festival and the InfoWar symposium.

Meanwhile, today (Tuesday) the symposium has started off, in a tightly structured academic proceeding, completely remote from the info-pandemonium that awaits the 'innocent' visitor outside of the quiet lecture hall.

The talks opened a predictable path of discourse. The grand war machines of the post-industrial era as the production sites for the contemporary formats of the InfoWar products. Much implied secrecy, non-disclosures and semi-disclosures, partly by the people we are lead to believe operate in the very belly of the beast on a daily basis. This is the institutionalised version of InfoWar, the official intelligence complots and exploits, a world of wonder and danger, maybe adventure..? But always a war machine, waging its effort against a perceived enemy, clear or abstract. The strategic arena of information and dis-information tactics, of perceptual de-stabilisation, of informatic security and transgression.

This institutionalised version of InfoWar is countered by it's logical and necessary counter-part, the InfoTerror, individualist and small-scale autonomous action against the corporate, state and global players. The destructive gestures of the aggressive mega-hacker. No longer a game, but a serious attempt to destabilise whatever order apparently needs to become the object of the attack.

Yesterday I talked with Stefan Wray of the Electronic Disturbance Theater about his concept of bottom-up information warfare and more importantly electronic civic disobedience. Wray's approach to info-action (perhaps

more than *war*) in effect seems to point towards a third way, out of the dichotomy of InfoWar and InfoTerror. With their real blockades of targeted web sites via "virtual sit-ins", the floodnet system, enabling any visitor to trigger an auto-reload sequence which when operated with the right critical mass of active floodnet visitors blocks the site, they propose a model for collective civil info-action. It emphasises the social dimension of the Net, where only through collective action a real effect is achieved, and can be achieved by engaging the critical mass of individuals into a collective civil disobedience action.

Collective info-action is a new tool to dismantle the neo-liberal mythologies of the cyber-sphere, and re-locate the net discourse in the very heart of society and all its inherent social, political and cultural debates, contradictions, and shared and contested beliefs, where it belongs.

09/08/1998

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/18/98

On December 18, 1998, SA [REDACTED] printed out the new web pages located at the Uniform Resource Locator of <http://www.thing.net/~rdom/ecd/ecd.html>, titled ELECTRONIC CIVIL DISOBEDIENCE. There was an announcement for EDT FloodNet action on the White House web site from 10:00 a.m. to 4:00 p.m.

On December 18, 1998, at approximately 10:00am and at various other times until 5:00pm, SA [REDACTED]

[REDACTED]

SA

[REDACTED]

[REDACTED]

SA

[REDACTED]

[REDACTED]

b6
b7C
b7E

UPLOADED

WITHOUT
BY DATE
12-29-98

288-NY-268557-45

| | |
|-------------|---------|
| SEARCHED | INDEXED |
| SERIALIZED | FILED |
| DEC 21 1998 | |

35

Investigation on 12/18/1998 at New York

File # 288-NY-268557 Date dictated 12/18/1998

by SA [REDACTED] b6
b7C

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/23/1998

To: CID/NSD
NIPC/CIOS/STAU/Rm 11728

Attn: [redacted]

From: New York

C-37

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]:11m

b6
b7C

Case ID #: 288-NY-268557

Title: ELECTRONIC DISTURBANCE THEATER;
[redacted]

CITA;
OO:NY

Synopsis: [redacted]

Details: Subject Electronic Disturbance Theater (EDT) is a group claiming on its Internet web site to protest various national and international policies through orchestrated attacks on computer systems. The attacks employ a program called "FloodNet" which causes a denial of service to the target computer. To date, the EDT has orchestrated attacks on Federal Government computer systems as well as foreign government computer systems.

SA [redacted] is in the process of [redacted] from Ft. Benning for all Internet traffic on 11/22/1998 during the EDT's FloodNet attack of their web site for the School of the Americas. DefenseLink, a Pentagon site, has also [redacted] from the 10/09/1998 FloodNet attack. On 12/18/1998, the White House web page was also the victim of a FloodNet attack, [redacted]
[redacted]
[redacted] C-37's [redacted]

b6
b7C
b7E

[redacted] The EDT is continuing to target various Federal and foreign governmental systems, as a result, more victims will be identified [redacted]
[redacted]

288-NY-268557-46

UP

WITH/TELE: _____
WITH/DT/DT: _____
BY: CN
DATE: 12-29-98

PPR 2001

CM

Snape.C

b6
b7C

To: CID/NSD From: New York
Re: 288-NY-268557, 12/23/1998



b7E

♦♦

REPLY FORM - INVESTIGATIVE INFORMATION SERVICES

To help us better serve your investigative needs, please complete and return to:

FBI, Butte Information Technology Center
400 Main Street, Room #115
Butte, Montana 59701

b6
b7c

BUTTE ITC RECORD #: UCFN: 288-NY-268557

ANALYST: _____ SUBJECT: _____
Was the information provided helpful to your investigation? YES NO
If NO, please let us know how we could be more helpful to your investigation:

ACCOMPLISHMENT(S) resulting from information:

PERSON(S): (Enter total number applicable to each of the following)

- ____ FBI Fugitive(s) Arrested: FBI Local Date _____
(Forward photo of Fugitive arrested with this Reply form)
____ Local Fugitive(s) Arrested: FBI Local Date _____
(Forward photo of Fugitive arrested with this Reply form)
____ Subject(s) Arrested Located Identified
(Forward photo of Subject arrested with this Reply form)
____ Witness(es) Located Identified
____ New Witness(es) Located Identified

BUSINESS(ES): (Enter total number applicable to each of the following)

- ____ New Business(es) Identified
____ New Business Associates/Associations Identified
____ Financial Audit Trail(s) Enhanced

ASSET(S): (Enter total number applicable to each of the following)

(TYPES: C = CASH R = REAL PROPERTY P = PERSONAL PROPERTY)

- ____ Asset(s) Located Identified [VALUE: _____] TYPE: _____
____ Asset(s) Subject to Seizure/Forfeiture [VALUE: _____] TYPE: _____
____ Potential Economic Loss Prevented [VALUE: _____] TYPE: _____

OTHER: (Enter total number applicable to each of the following)

- ____ New Case(s) Initiated 2 New Lead(s) Generated

COMMENTS: _____

288-NY-268557-47

CM CM

- 1 Case File (288-NY-268557)
1 BITC

PLEASE RETURN TO: BUTTE ITC

12

11

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/28/98

The following investigation was conducted in connection with the Electronic Disturbance Theater (EDT). On December 10, 1998, SA [redacted] used an E-mail account [redacted]
[redacted]
[redacted]

b6
b7C
b7E

(X)
dms

From December 10, 1998 through December 28, 1998, SA [redacted] received twenty five E-mails from [redacted]
[redacted] These messages have been printed out and attached in a 1A envelope.

UPLOADED

WITH/TEXT _____
WITH/CL, TEXT _____
BY CM
DATE 1-4-99

288-NY-268557-148

| | |
|---------------|----------|
| SEARCHED | INDEXED |
| SERIALIZED CM | FILED CM |
| DEC 30 1998 | |

12/28/98

Investigation on 12/10/1998 at New York

File # 288-NY-268557 Date dictated 12/28/1998

by SA [redacted] b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

12-10-28.wpd

200-NM-268557.- 49

CIA CIA

REFERENCE: CART EVALUATION OF APAC70 11/17/74

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-28-2015 BY C32W33B91 NSICG



INVESTIGATIVE INFORMATION REQUEST FORM

FBI, Butte Information Technology Center
400 North Main Street, Room #115
Butte, Montana 59701

► Commercial Telephone [redacted]
► FTS: [redacted] FAX: [redacted]
► Secure FAX & STU III: [redacted]

| | | |
|------------------------|----------------|--|
| ITC Use Only: | BITC Record #: | [redacted] |
| Date/Time In: | Dec 10 10:30 | am <input type="checkbox"/> pm <input checked="" type="checkbox"/> |
| Date/Time Out: | 12/21 8:03 | am <input checked="" type="checkbox"/> pm <input type="checkbox"/> |
| Database(s) Used: | | |
| 1. <u>TW</u> | 5. <u>LN</u> | 9. _____ |
| 2. <u>EF</u> | 6. _____ | 10. _____ |
| 3. <u>MN</u> | 7. _____ | 11. _____ |
| 4. _____ | 8. _____ | 12. _____ |
| Handled By: [redacted] | | |

TO: FBI, BUTTE INFORMATION TECHNOLOGY CENTER

Date: 12/19/98

Forfeiture/Seizure Related: Type of Request: FAX Telcal Mail

Response: Telcal Mail

Requestor: SA [redacted] (Requestor Name is Requestor) Phone #: [redacted] FAX #: [redacted] UCFN: 288-NY-268557

(UCFN (File #) is Required)

Office/RA: NEW YORK

Precedence: ROUTINE IMMEDIATE
(Emergency/Crisis Situation)

SEARCH CRITERIA (Attach additional sheets if necessary)

Name - Last: GOLIGHTLY First: SKY Middle: 12

Alias: _____ Sex: _____ DOB1: / / DOB2: / /

SSAN1: _____ SSAN2: _____ Spouse: _____

Fugitive: Yes No Driver's License #: _____ State: _____

RESIDENCE

Street Address: _____ City/State: _____ Zip: _____ Phone: _____

BUSINESS

Business Name: AURORA BLUE Street Address: 15710 MINNETONKA BLVD

City/State: MINNETONKA Zip: MN Phone: 408 8120613 Business ID#: _____

CHECK DESIRED SEARCH PARAMETERS (Please check only those that are needed)

1. Specific Information Desired _____
2. Determine All Individuals Associated with Social Security Number(s)
3. Report Validity of Social Security Number
4. Determine Who is Associated with Telephone Number(s)
5. Determine Address of Business/Person (U.S. _____, _____, _____ State(s))
6. Determine Property Owned by Individual (U.S. _____, _____, _____ State(s))
7. Determine Who Owns Property Listed Above
8. Determine Who Resides at Address Listed Above
9. Determine Financial Background Info, i.e., Bankruptcy, Judgments, Liens, UCC filings, or Lawsuits
10. Determine Corporate Business Info, i.e., Officer, Director, Registered Agent _____ (Person/Business)
11. Customs Border Crossings / Subject query / I-94 info (circle one)
12. Federal Prison Inmate Information
13. Telemarketing Complaints

b6

b7C

b7E

Reply From: FBI, Butte Information Technology Center (BITC)

Return Reply To:
SAC, _____

Attention: _____

Based on search criteria, marked records are attached:

- Possible Identifiable Records
 Other Peripheral Information

Brief Synopsis of Information Found: 288-NY-268557-50
 No Information Found: CM

110-1000

7-50

MAIL-IT REQUESTED: DECEMBER 22, 1998

103T3F

CLIENT:

LIBRARY: ASSETS

FILE: MNOWN

YOUR SEARCH REQUEST AT THE TIME THIS MAIL-IT WAS REQUESTED:
15710 W/2 MINNETONKA

NUMBER OF RECORDS FOUND WITH YOUR REQUEST THROUGH:

LEVEL 1... 1

LEVEL 1 PRINTED

DISPLAY FORMAT: FULL

SEND TO: BUTTE, 8
FBI
400 N MAIN ST RM 115
BUTTE MONTANA 59701-8866

*****05630*****

2