

(b)(2)

~~TOP SECRET~~ [REDACTED] ~~ORCON, NOFORN//X1~~

September 1999  
DI-2410-49-99-SI

# DEFENSE INTELLIGENCE ASSESSMENT



## (U) Usama Bin Ladin/ Al-Qaida Information Operations

*DIADI 2410-49-99-SI*

Derived from: Multiple Sources  
~~Declassify on: X1, X2, X3, X6, X7, X8~~

The unauthorized disclosure of classified information may be prosecuted under Section 793 and Section 794, Title 18, USC, and is punishable by fine of not more than \$10,000, imprisonment of not more than 10 years, or both.

~~TOP SECRET~~ [REDACTED] ~~ORCON, NOFORN//X1~~

(b)(2)

(b)(2)

~~TOP SECRET// [REDACTED] //ORCON,NOFORN//X1~~

---

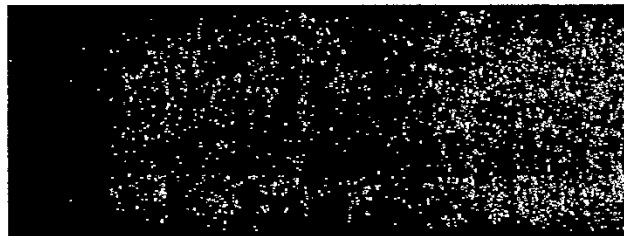
## Defense Intelligence Assessment

---

### (U) Usama Bin Ladin/Al-Qaida Information Operations

*Information Cutoff Date: 1 July 1999*

This document is published under the auspices of the Department of Defense Intelligence Production Program (DoDIPP). The Defense Intelligence Agency produced it as the designated DoDIPP producer for this subject.



(b)(3)

This product addresses the interests of the Secretary of Defense and J2.

*Derived from: Multiple Sources*

~~Declassify on: N1, N3, X5, X6, X7, X8~~

DI-2410-49-99-S1

~~TOP SECRET// [REDACTED] //ORCON,NOFORN//X1~~

(b)(2)

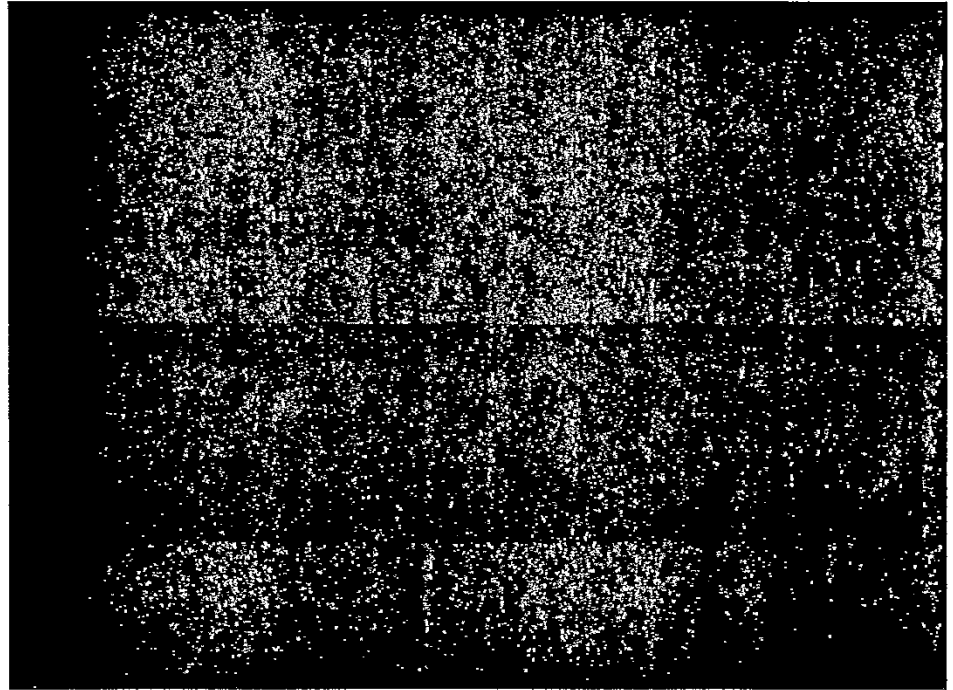
(b)(2)

~~TOP SECRET [REDACTED] ORCON,NOFORN//X1~~

**(U) Usama Bin Ladin/Al-Qaida Information Operations**

(b)(1)

Key Judgments



*Information Cutoff Date: 1 July 1999*

*Derived from: Multiple Sources*

~~Do not disseminate to: X1, X3, X5, X6, X7, X8~~

DI-2410-49-99-SI

(Reverse Blank)

(b)(2)

III

~~TOP SECRET [REDACTED] ORCON,NOFORN//X1~~

(b)(2)

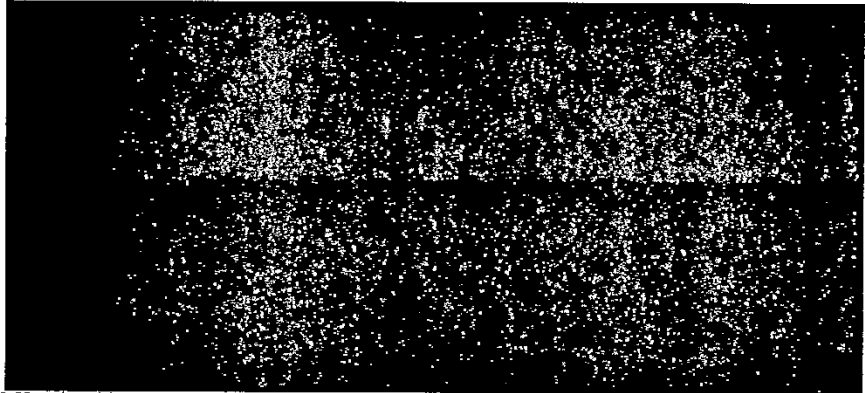
~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN//X1~~

---

## Contents

---

Foreword .....	vii
Summary .....	1
Defensive IO .....	1
Offensive IO .....	1
Defensive IO .....	2



(b)(2)

Offensive IO .....	9
--------------------	---



(b)(2)

Outlook .....	12
---------------	----

---

## Appendix

---

A. Al-Qaida .....	13
-------------------	----

---

## Figures

---

(b)(1)



2. INMARSAT-M Telephone .....	5
3. The Taliban's Homepage, <a href="http://www.ummah.net/taliban">www.ummah.net/taliban</a> .....	6
4. PGP Encryption Software Logo .....	7
5. Usama Bin Ladin During ABC Interview .....	9
6. Saudi Dissident Mohammed Al Massari .....	10

v

~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN//X1~~

(b)(2)

(b)(2)

~~TOP SECRET// [REDACTED] (ORCON,NOFORN//X)~~

**Contents (Continued)**

7. Islamic Gateway Web Site. . . . .	11
8. Muslim Hackers Club Web Page. . . . .	11
[REDACTED]	
11. Bin Ladin's London Press Representative, Khalid Al-Fawwaz. . . . .	15
12. Abu Hajar, aka Mamdouh Mahmud Salim . . . . .	15

(b)(2)

~~TOP SECRET// [REDACTED] (ORCON,NOFORN//X)~~

(b)(2)

(b)(2)

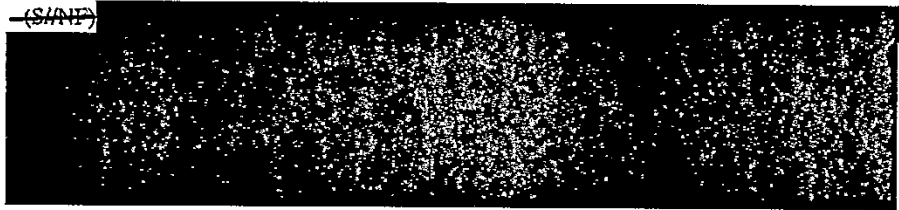
~~TOP SECRET// [REDACTED] ORCON,NOFORN//X1~~

## **(U) Usama Bin Ladin/Al-Qaida Information Operations**

Foreword

~~(S//NF)~~

(b)(1)



(U) Each classified title and heading has been marked properly; those unmarked are unclassified.

(U) COPYRIGHT WARNING: Further dissemination of the photographs in this publication is not authorized.

(U) Additional copies of this product may be obtained if it has not been placed on Intelink or Intelink-S or if your organization does not have access to Intelink or Intelink-S. To obtain additional copies, submit an online Form DD-1142 (accessible via DIA SAFE), a hardcopy Form DD-1142, an electronic message, or a letter according to these guidelines:

- OSD, JCS, and non-DoD national-level organizations: submit written requests to DIA (ATTN: SVD), Washington, DC 20340-5100; submit electronic message requests to DIA WASHINGTON DC//SVD.
- Other DoD organizations: submit all requests via your Dissemination Program Manager/ administrative chain of command.

To request a change in the distribution requirements for your organization, submit a request in writing or via electronic message to DIA (ATTN: SVD-2), Washington, DC 20340-5100 (or to DIA WASHINGTON DC//SVD-2//) according to the guidelines above.

(Reverse Blank)

vii

~~TOP SECRET// [REDACTED] ORCON,NOFORN//X1~~

(b)(2)

## (U) Usama Bin Ladin/Al-Qaida Information Operations

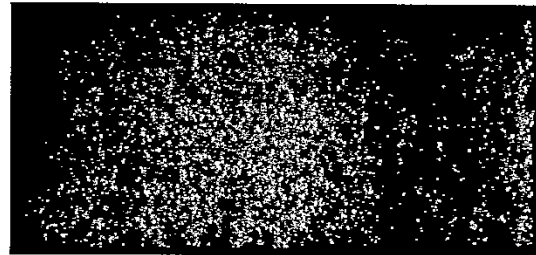
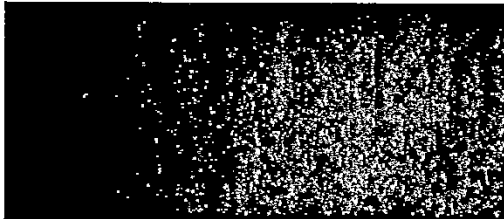
---

### Summary

---

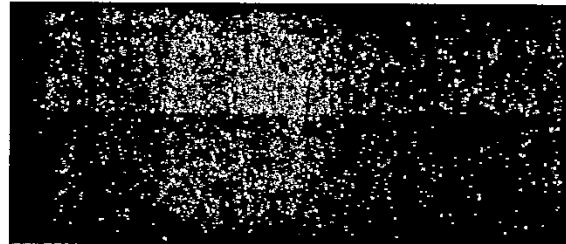
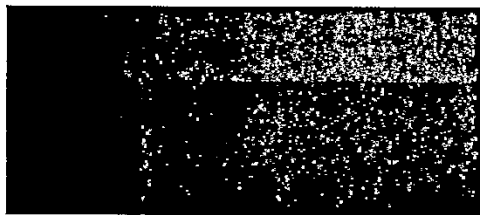
#### Defensive IO

(b)(1)



(b)(1)

#### Offensive IO



(b)(1)

---

### IO Definitions

(U) DoD defines IO as actions taken to affect adversary information and information systems while defending one's own information and information systems. Major capabilities to conduct IO include operational security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare (EW), and physical attack/destruction and could include CNA. IO-related activities include public affairs and civil affairs activities. The two major subdivisions within IO are offensive IO and defensive IO.

- **Offensive IO** involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers and achieve or promote specific objectives. Offensive IO capabilities and activities include OPSEC, military deception, PSYOP, EW, physical attack/destruction, and special information operations and could include CNA.
- **Defensive IO** integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted and assisted through information assurance, OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence, EW, and sensitive IO. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Offensive IO can support defensive IO.

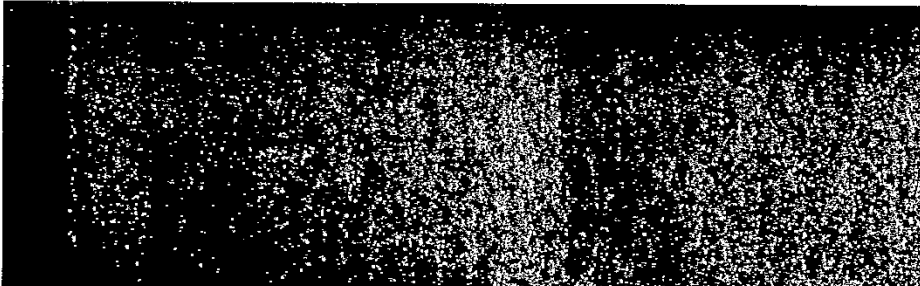
---

(b)(2)

(b)(2)

~~TOP SECRET~~ [REDACTED] /ORCON,NOFORN//SI

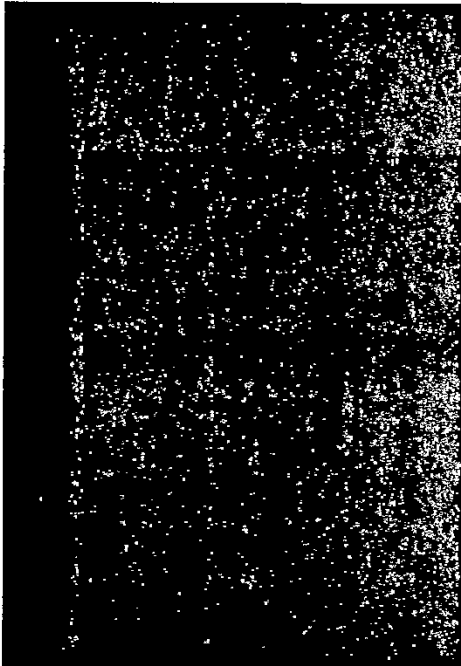
(b)(1)



Defensive IO

Al-Qaida Command and Control Overview

(b)(1)



(b)(1)

~~TOP SECRET~~ [REDACTED] /ORCON,NOFORN//SI

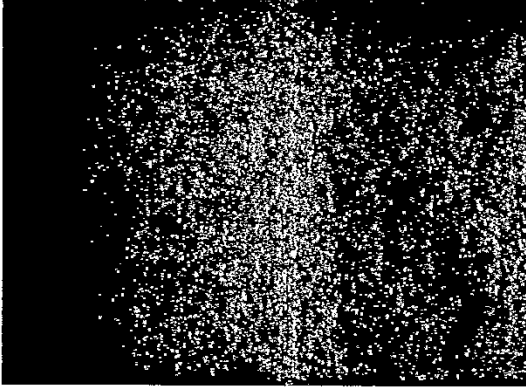
(b)(2)



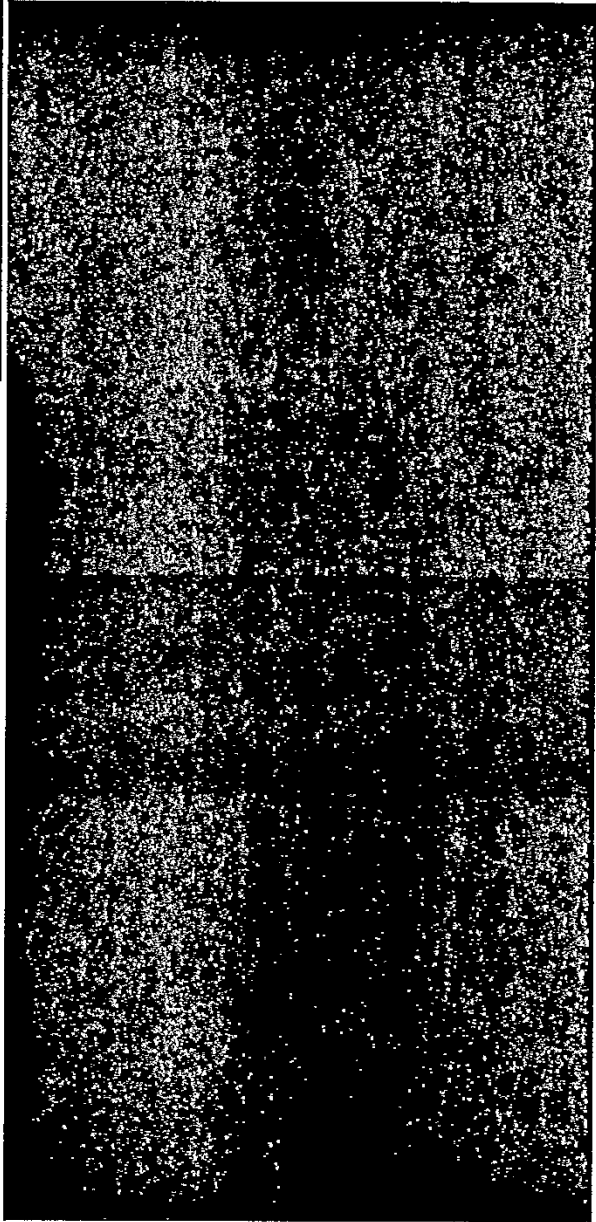
(b)(2)

~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN/X1~~

(b)(1)



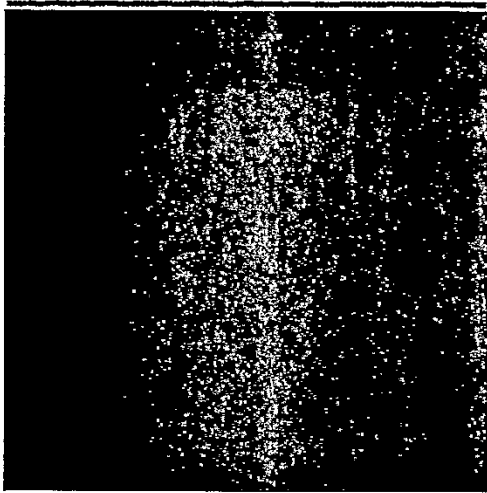
(b)(1)



**Callback Services**

(U) Callback services allow a person in a foreign country to dial a designated US number and hang up after several rings. A computer attached to the US telephone then calls the foreign number and presents a US dial tone. The caller in the foreign country then dials the number of the party to whom he wishes to speak and is charged the US long-distance rate, not the rate set by the country from which he is calling.

(b)(1)



(b)(1)

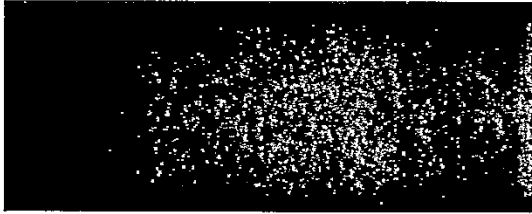
~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN/X1~~

(b)(2)

(b)(2)

TOP SECRET [REDACTED] /ORCON,NOFORN//X1

(b)(1)



UNCLASSIFIED

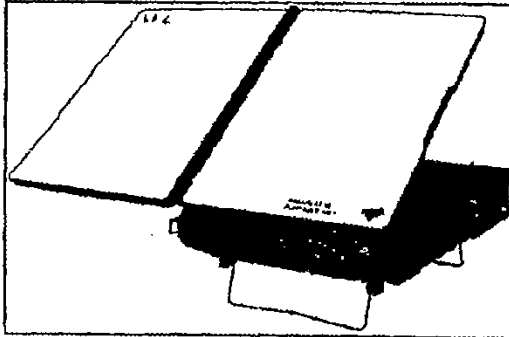
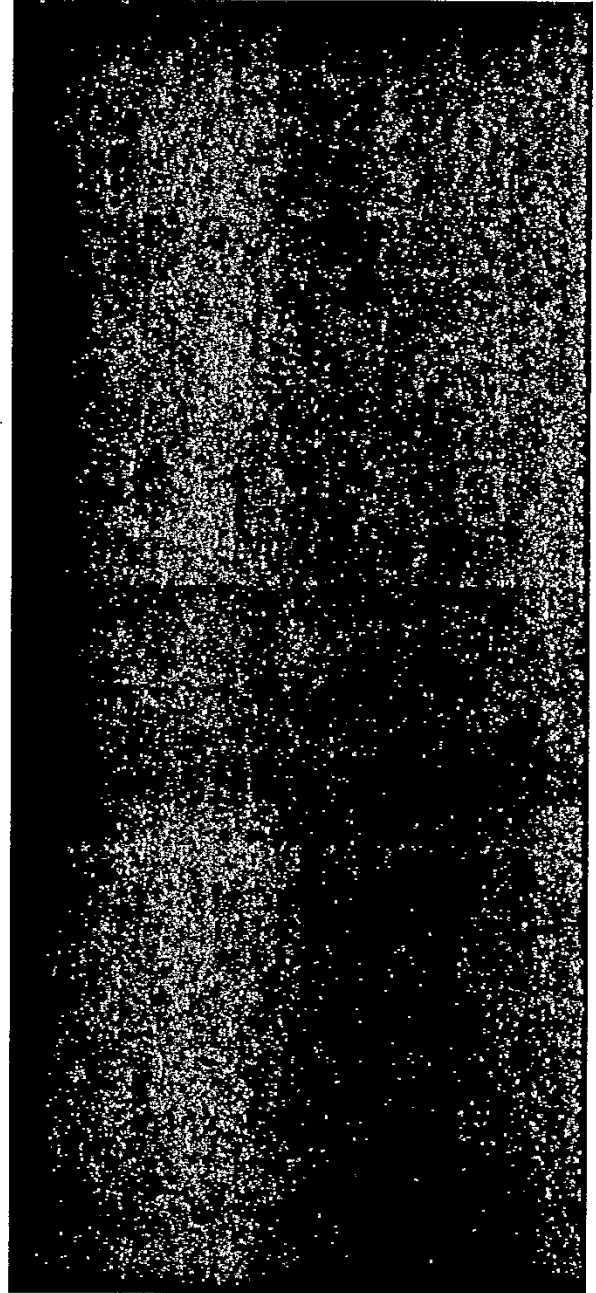
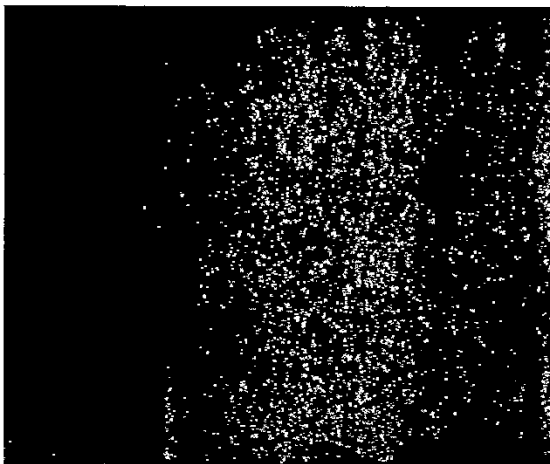


Figure 2. (U) INMARSAT-M Telephone. INMARSAT, which began operations in 1982, operates a system of satellites to provide mobile communications services. INMARSAT-M provides mobile telecommunication services through a small portable terminal. The system is intended primarily for land-mobile use, although several maritime versions are available. A typical briefcase terminal includes a flat patch array antenna, weighs 18-35 pounds, and can operate off an external power source or a built-in battery for up to an hour.

(b)(1)



(b)(1)

(b)(2)

(b)(2)

~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN//X1~~

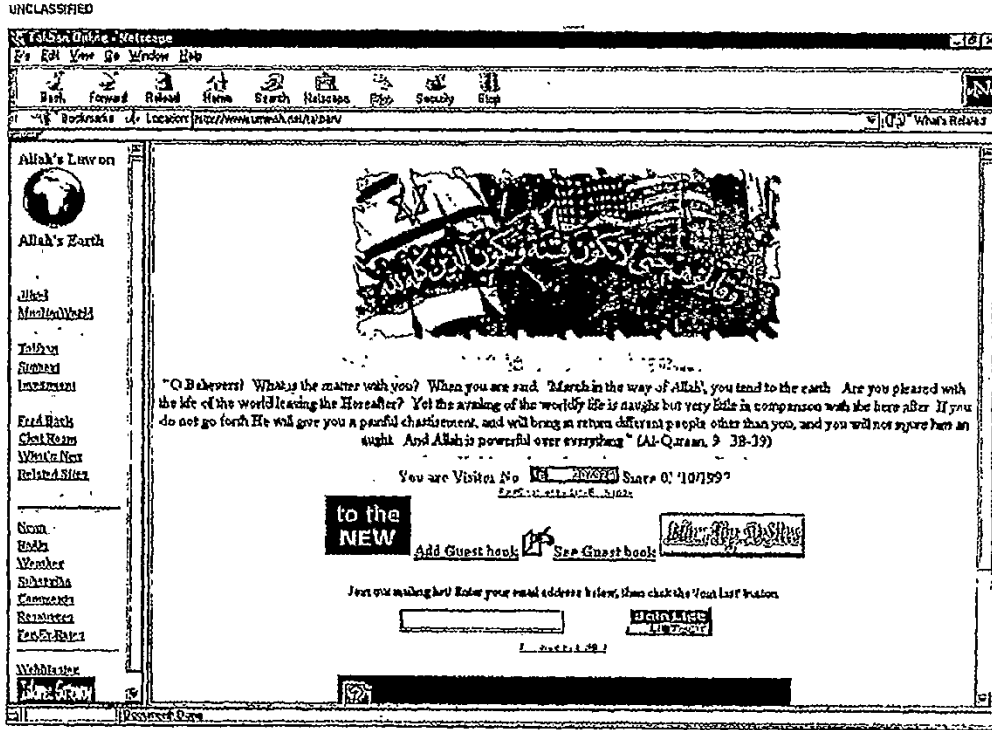
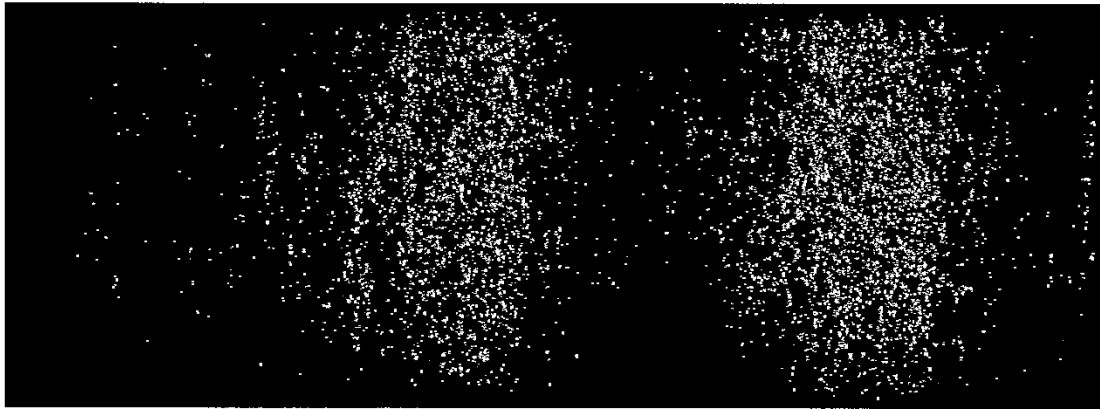


Figure 3. (U) The Taliban's Homepage, www.ummah.net/taliban.



(b)(1)

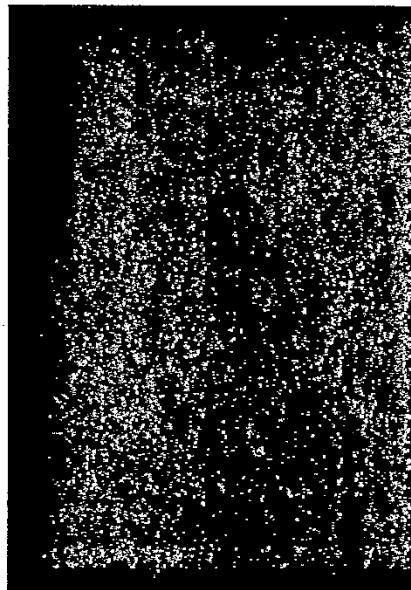
~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN//X1~~

(b)(2)

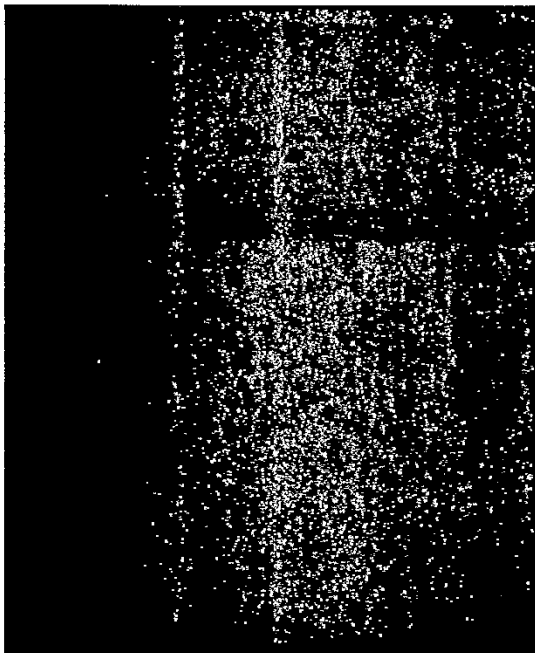
UNCLASSIFIED



Figure 5. (U) Usama Bin Laden During ABC Interview.

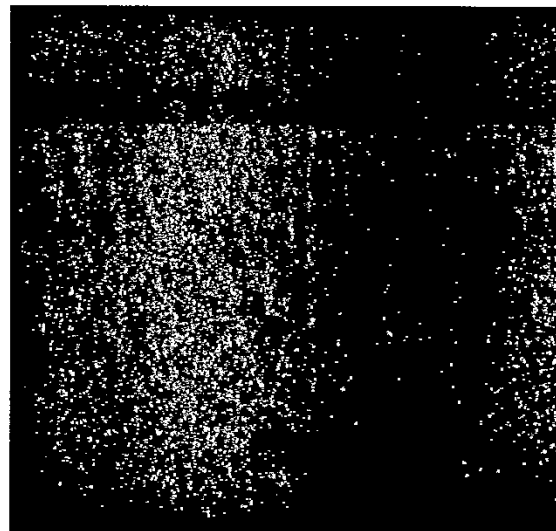


(b)(1)



(b)(1)

Offensive IO

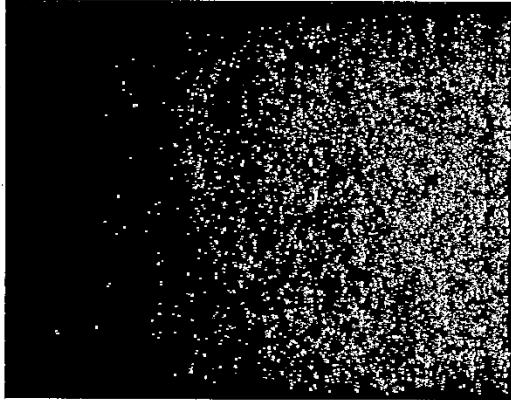


(b)(1)

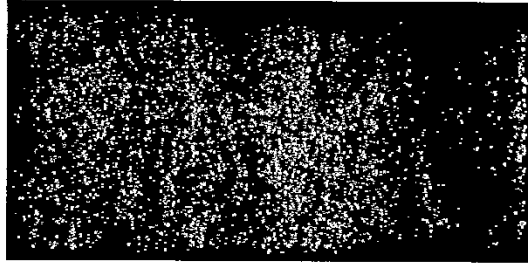
(b)(2)

~~TOP SECRET~~ [REDACTED] ORCON,NOFORN//X1

(b)(1)



tion and distribution of an English language version of the declaration.



(b)(1)

### Islamic Gateway

### Islamic Gateway and Hacker Groups

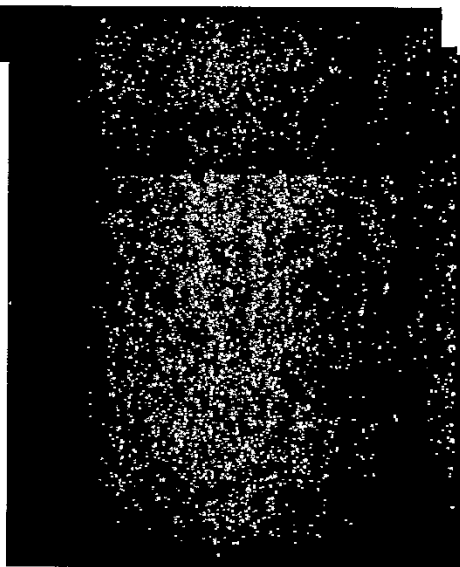
(U) Mohammed Al Masari, head of the now-bankrupt Committee for the Defense of Legitimate Rights and current patron of the Islamic Gateway, is known for his ties to Bin Ladin. In August 1996, for example, when Bin Ladin issued a "Declaration of War" urging all Muslims to boycott US goods and join in armed struggle against the US military presence in the Persian Gulf, Al Masari ordered dissemination of the Arabic-language document through the CDLR fax mailing list. Al Masari also personally supervised the transla-

(U) The Islamic Gateway is a web site dedicated to disseminating information on Islamic religious and political topics. The site is a professionally produced, extensive collection of Islamic information and news intended for a largely Western audience. Topics on the site include information on religious observance as well as Islamic militant movements and causes.

UNCLASSIFIED



Figure 6. (U) Saudi Dissident Mohammed Al Masari.



(b)(1)

(b)(2)

~~TOP SECRET~~ [REDACTED] ORCON,NOFORN//X1

(b)(2)

TOP SECRET [REDACTED] /ORCON,NOFORN//X1

UNCLASSIFIED

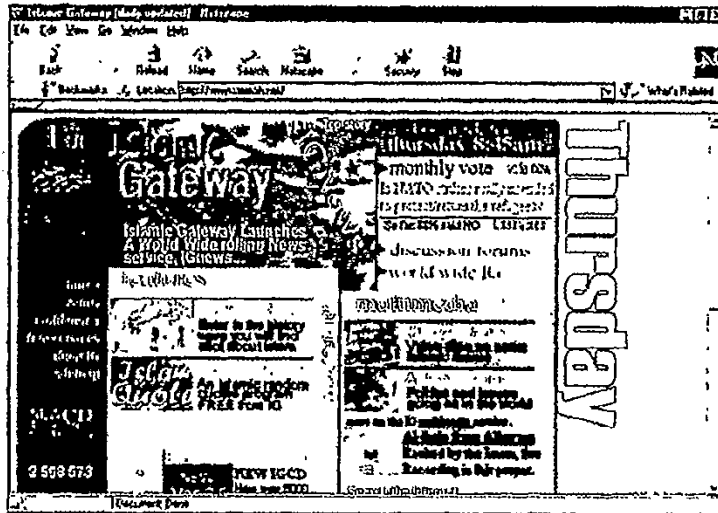


Figure 7. (U) Islamic Gateway Web Site.

UNCLASSIFIED

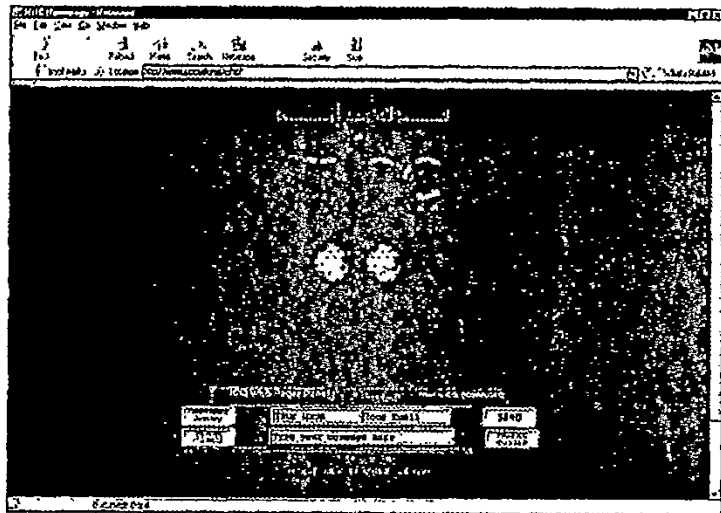


Figure 8. (U) Muslim Hackers Club Web Page.

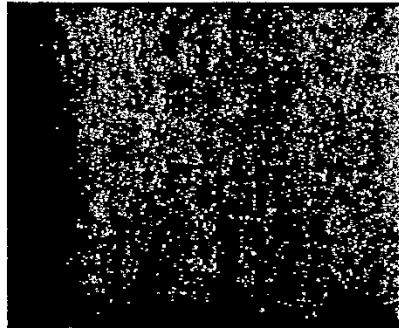
(b)(2)

~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN//X1~~

UNCLASSIFIED



Figure 11. (U) Bin Laden's London Press Representative, Khalid Al-Fawwaz.



UNCLASSIFIED

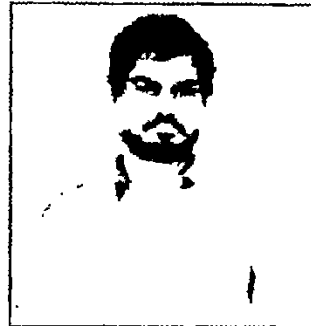


Figure 12. (U) Abu Hajar, aka Mamdouh Mahmud Salim. Hajar is Bin Laden's technology representative.

(b)(1)

UNCLASSIFIED

---

#### Chronology: Usama Bin Ladin

- 1957 — Born in Riyadh, Saudi Arabia.
  - 1979 — Attended King Abdul Aziz University.
  - December 1979 — Traveled to Afghanistan to fight against the Soviet invasion.
  - 1985 — Founded Al-Qaida.
  - February 1989 — Soviet forces withdrew from Afghanistan.
  - 1989 — Returned to Saudi Arabia.
  - 1991 — Left Saudi Arabia and relocated to Khartoum, Sudan; greatly increased interactions with and funding of Islamic groups.
  - 1994 — Stripped of Saudi citizenship because of anti-Saudi rhetoric and support of Islamic extremists.
  - 1996 — Expelled from Khartoum; traveled to Afghanistan.
  - February 1998 — Issued *fatwa* against United States.
  - August 1998 — Orchestrated bombing of US embassies in Kenya and Tanzania.
- 

(Reverse Blank)

15

~~TOP SECRET~~ [REDACTED] ~~ORCON,NOFORN//X1~~

(b)(2)