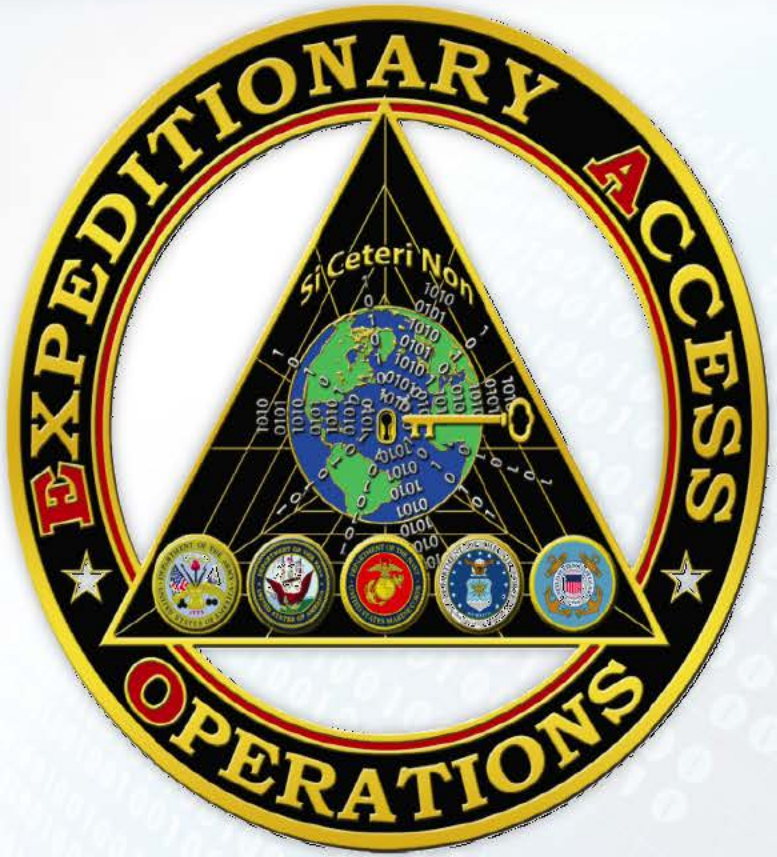


EXPEDITIONARY ACCESS OPERATIONS

NSA's Close Access Network Exploitation Program

Expeditionary Access Operations

(S//SI//REL) S3283 is the expeditionary arm of TAO which conducts worldwide Human Enabled Close Access Cyber Operations to satisfy National and Tactical SIGINT access requirements.

Technologies of Interest:

- Computers
- 802.11 (WiFi)

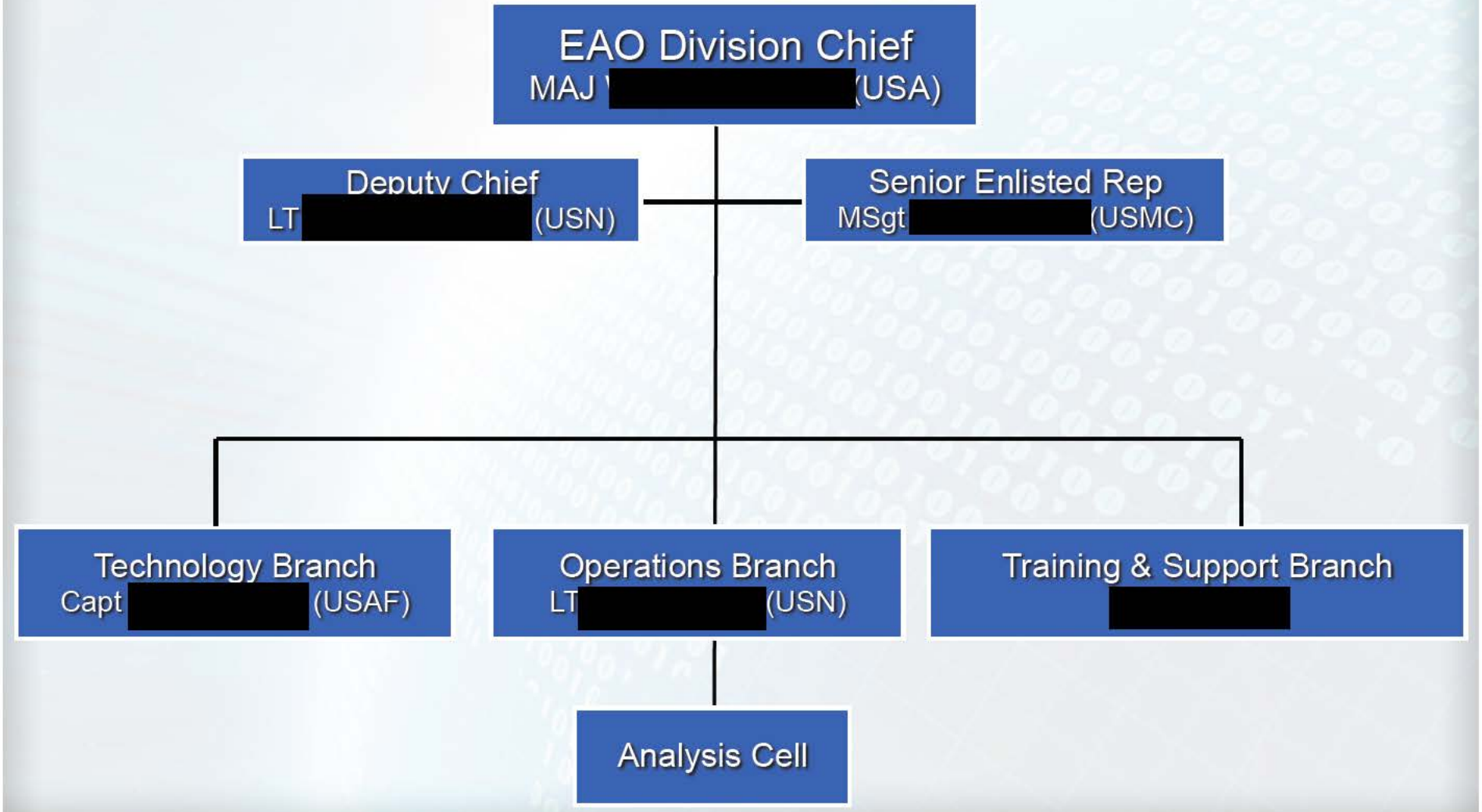
Customer Set:

- Various Task Forces
- COCOM Planners
- SOCOM Operations
- Service Cyber Elements
- 902nd MI Group
- DIA/CIA/FBI
- CSTs / CSGs
- NSA TOPIs
- Conventional SIGINT Elements
- 2nd Party Partners

Tasks

- Deploy certified operational teams to tactical environments to execute close access **Computer Network Exploitation (CNE)** in support of national and tactical requirements
- **Certify SIGINT personnel** to conduct human-enabled CNE missions
- **Develop, test, and field** solutions for future tactical CNE and endpoint geolocation systems and techniques

EAO Division



Human Enabled CNE Tools

Human Enabled CNE Level I

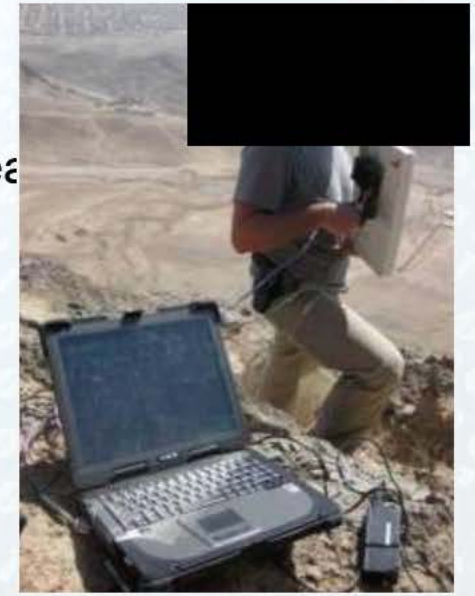
- Physical Access
- Software implants that act as the initial "hook" into target systems to enable remote operations (ROC)
  - Internet Cafes
  - Gifting
  - Detainee Computers

Human Enabled CNE Level II

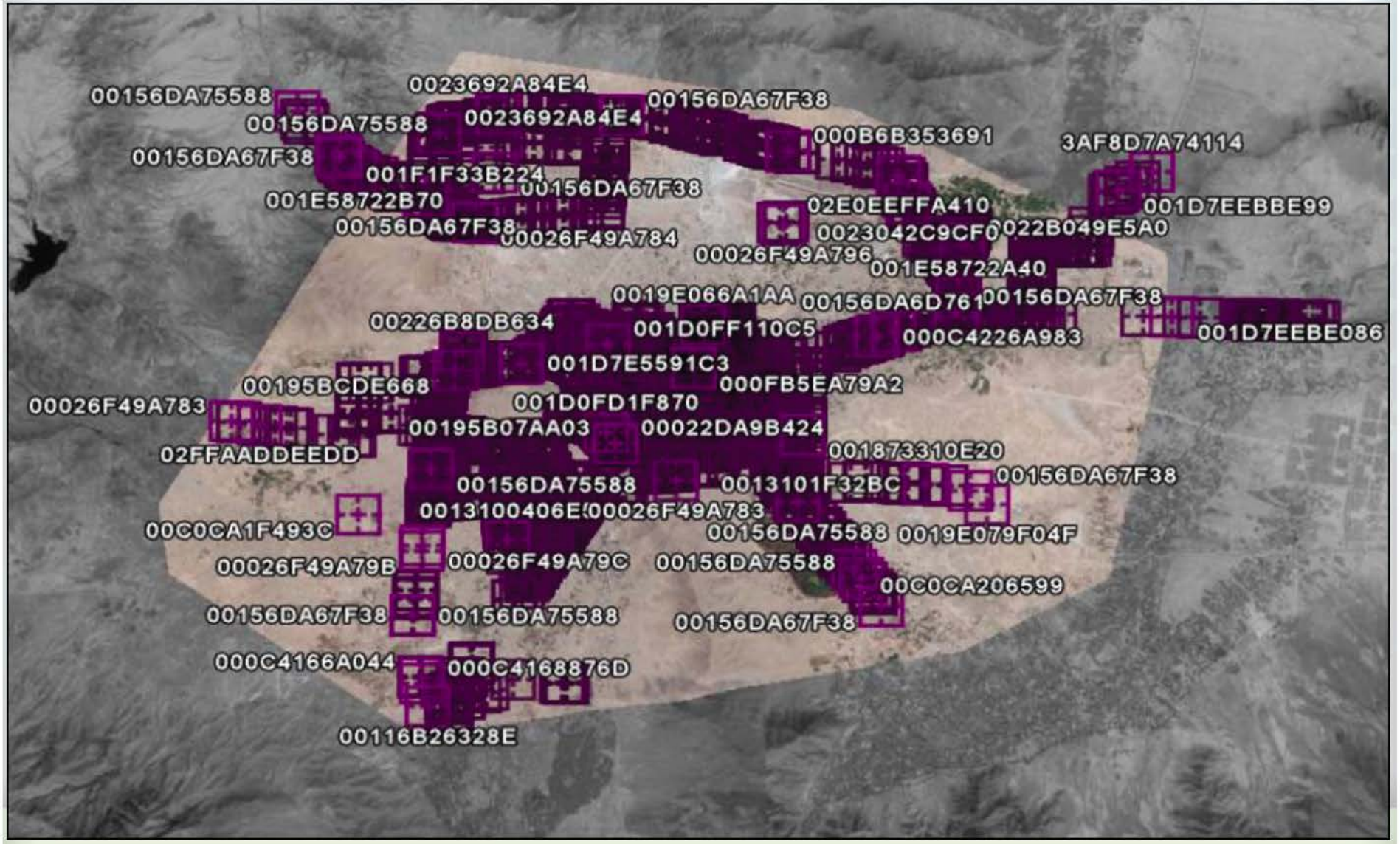
- **Wireless payload delivery/injection tool**
- **Monitors target's web traffic**
- **Injects special ROC tag**
- **Target unknowingly owned by the ROC**
  - **ISPs**
  - **Banks**
  - **Telecommunications**
  - **Consulates/Embassies**

BLINDDATE

- 802.11 a/b/g Survey/Exploitation Hardware
  - Handheld, laptop, deep install form factors
  - Plug-in architecture for custom functions: hea mapping, NITESTAND, HAPPY HOUR, BADDECISION, more
  - GUI used for active and passive CNE tools
  - Provides output data ingested by numerous databases (MASTERSHAKE, etc)



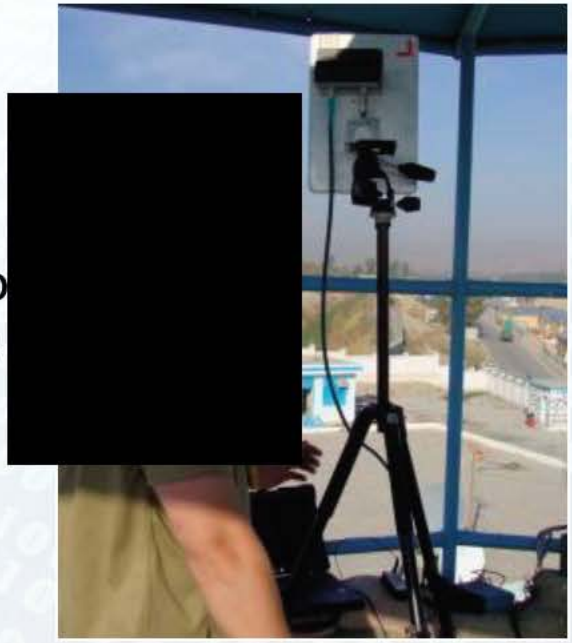
Kabul BD Survey Results



Heat Map Analysis

NITESTAND

- BLINDDATE Plug-in
- 802.11 a/b/g wireless injection tool
- Monitors target's web traffic
- Injects unique packet that forces client to access a monitored listening post on the internet for payload deployment
- Transparent to target



QKismet

Stop WiFi | Start Gps | Less <<

Networks | WiFi | GPS | Plugins | About

TASKED	TARGET	SSID	BSSID	BROWSER	GET	OK	SA IPADDR	TAG	AT
	00:15:6D:DC:24:4D	UTSwireless4	00:15:6D:DC:12:D9		✓	✓	202.95.79.204		25 c
	00:C0:CA:23:7E:D1	UTSwireless1	00:C0:CA:1F:48:F9			✓	202.95.79.204		0 of
	00:C0:CA:21:61:E9	UTSwireless3	00:C0:CA:1F:48:F6			✓	202.95.79.204		0 of
	00:C0:CA:1A:FD:54	UTSwireless3	00:C0:CA:1F:48:F6			✓	202.95.79.204		0 of
	00:C0:CA:1A:FD:01	UTSwireless3	00:C0:CA:1F:48:F6		✓		202.95.79.204		0 of
	00:1E:58:A0:89:70	UTSwireless4	00:15:6D:DC:12:D9		✓	✓	202.95.79.204		0 of

Current Operations

- EAO-W: Columbia Annex (CANX)
  - Supports Global CNE Operations in support of customers
  - Coordinates with R&T access priorities
  - Provides WiFi geo-location operator expertise to customers
- Afghanistan: OIC, Analyst, 7 x Operators - Bagram
  - Presence in Bagram, Kabul, and Kandahar
  - Requirements from TOPIs, TF 3-10, IOC, CJSOTF-A, tactical CST's
- Germany: 2 x operators- Stuttgart
  - Part of the ETC
  - Support EUCOM and AFRICOM requirements
- Southwest USA: 4 x operators- Texas
  - Supporting [redacted]
  - Requirements from NSA Texas

Operation IRONPERSISTENCE

ATO Support to DIA and TF 3-10 in Afghanistan

Ongoing

DIA approached EAO-AF about a source with access to some key Taliban targets in Afghanistan. These targets are two of TF 3-10's highest priority targets.

EAO-Washington coordinated with DIA as well as ATO's MX Team, Bridging and Exploitation Division, and Persistence Division to create the proper tool that addresses the target's sensitive OPSEC practices.

CNE enabled devices have since been forward deployed to Afghanistan to be used against this target. The devices will be delivered as soon as the source can schedule a meeting with the Task Force Target.

Expeditionary Access Operations-Iraq

Operation CLIMBINGSHIRT – EAO-I

OPPORTUNITY: EAO-Iraq was requested to conduct a CAT E implant on two laptops which were gifted to This is an opportunity to establish long term collect on and refine intelligence pertaining to Intelligence gain will identify the network communications of these individuals, and possibly serve to enhance the overall operational picture of the networks that these agents are operating on..

Result – SGT deployed tc and gifted two pre-implanted laptops to The items gifted included other items, such as under the auspices of The items were heartily accepted and EAO-I is awaiting results.

Operations in Development

- [redacted]
- Libya and Syria – EAO is prepared to support contingency operations regarding any requirements in hostile environments
- [redacted]

EAO Way Ahead

- Continue to use partnerships with DoD to meet National and Military access requirements

- Formalize Partnership with USCYBERCOM
  - Become their expeditionary capability
  - Respond to Cyber requirements in non-CENTCOM AORs
  - BPT conduct Title 10 operations
  - BPT respond to worldwide contingency Operations

- Expand the Close Access Network Operator training pipeline with respect to ADET's CANO work role

- Continue to work with sister offices, the Services, and commercial vendors for advancements in CANO capabilities and provide testing support when required

CONTACT INFORMATION

Division Chief	MAJ	[redacted]
Deputy Chief	LT	[redacted]
Operations Branch	LT	[redacted]
Analysis Cell	SFC	[redacted]
Training Branch		[redacted]
Tech Branch	CTN1	[redacted]

"Go EAO" *"Go EAO-A"*

[redacted]

General Inquires *Afghanistan*