

CHURCH OF WIFI
TIME TO PLAY

DEFCON

presents



Hacking Iraq

Michael Schearer ("theprez98")











CHURCH OF WIFI
TIME TO PLAY

DEFCON

Plan of Attack

- Introduction
- Disclaimers
- My Background
- Why is the Navy in Iraq?
- Iraqi Communications Infrastructure
- IEDs
  - Composition, Typology, Counter-IED Strategy
- The Future



CHURCH OF WIFI
TIME TO PLAY

DEFCON

Introduction

- Operational Security (OPSEC)
- Challenges and Limitations

Disclaimers

- This presentation is UNCLASSIFIED. On some issues I may be able to speak in generalities but not specifics.
- Nothing in this presentation is classified or "For Official Use Only," nor does it contain information regarding incidents under ongoing investigation or any information protected by the Privacy Act.

Disclaimers

- This presentation complies with DOD Directives 5230.9, 5400.7, and 5500.7.
- All images, videos and/or media within this presentation were obtained from open sources using unclassified search terms.
- I am not here as a representative of the U.S. government or U.S. Navy.
- I am not here to be "for" or "against" the war. Please leave your politics at the door!



CHURCH OF WIFI
TIME TO PLAY

DEFCON

My Background

- Active Duty, U.S. Navy Lieutenant (O-3)
- EA-6B Prowler Electronic Countermeasures Officer (Naval Flight Officer)
- Licensed Extra Class Amateur Radio Operator (N3WI)
- Church of WiFi Forums Administrator
- Remote-Exploit Forums Moderator
- “Regular” on DEFCON and NetStumbler forums


NK
NAVY
500






502


SKINNER









CHURCH OF WIFI
TIME TO PLAY

DEFCON

Why is the Navy in Iraq?

Threat from Improvised Explosive Devices

Improvised Explosive Devices

"The majority of insurgent attacks come in the form of IEDs targetting Iraqi and Coalition convoys and patrols. Most IEDs are made from leftover munitions and foreign explosive materials which are often hastily put together. Vehicle borne IEDs, VBIEDs, are devices that use a vehicle as the package or container of the device. These IEDs come in all shapes and sizes, from small sedans to large cargo trucks. There have even been instances of what appeared to be generators, donkey-drawn cards, and ambulances used to attempt attacks on Coalition forces and the new Iraqi government."[1]

[1]http://www.mnf-iraq.com/index.php?option=com_content&task=view&id=727&Itemid=44

Why is the Navy in Iraq?

Threat from Improvised Explosive Devices

+

Army asked for help

HEADQUARTERS
MULTI-NATIONAL CORPS-IRAQ
BAGHDAD, IRAQ
APO AE 09342

REPLY TO ATTENTION OF

April 26, 2006

Commanding General

Admiral Michael G. Mullen
Chief of Naval Operations
2000 Navy Pentagon
Washington, DC 20350-2000

Dear Admiral Mullen:

I would like to thank you for the much needed support you have provided to the Multi-National Corps-Iraq. The 291 Electronic Warfare Officers you sent, adds the missing dimension in our counter-improvised explosive device efforts. Your experts embedded at Battalion through Corps provide the technical expertise to adjust to the ever changing threat. Additionally, their training of our Soldiers and Marines is vital to our mission success and will instill the necessary level of confidence in our CREW Equipment.

Your team is highly motivated and I can assure you I am personally impressed with the enthusiasm and professionalism of your Sailors. The way they have integrated within the Multi-National Corps-Iraq to accomplish the mission is especially inspiring and you can be extremely proud of them. Be assured that I have the utmost confidence in their abilities.

Most important of all is your unselfish support will save the lives of Soldiers, Airmen, Marines and Sailors across the OIF Area of Operations. I can't thank you enough for your enthusiastic support of this most important counter IED initiative.

Sincerely,

Peter W. Chiarelli
Lieutenant General, US Army
Commanding

I HONESTLY BELIEVE THAT THIS SUPPORT WILL REDUCE CASUALTIES MORE THAN ANY OTHER SINGLE ACTION OF THE LONG WAR.

[2]http://www.militaryhomefront.dod.mil/campvictory/

Why is the Navy in Iraq?

Threat from Improvised Explosive Devices

+

Army asked for help

+

Indigenous Navy electronic warfare capability


NK
159907
USS JOHN C. STENNIS
NAVY
VAQ-139
500

Why is the Navy in Iraq?

Threat from Improvised Explosive Devices

+

Army asked for help

+

Indigenous Navy electronic warfare capability

=

JCCS-1

The Electronic Warfare Mission



"Suppress the RCIED threat to Coalition Forces and reduce casualties through enhanced electronic warfare coordination and JCREW operations, training and readiness."[3]

[3]https://www.militaryhomefront.dod.mil/campvictory3/



CHURCH OF WIFI
TIME TO PLAY

DEFCON

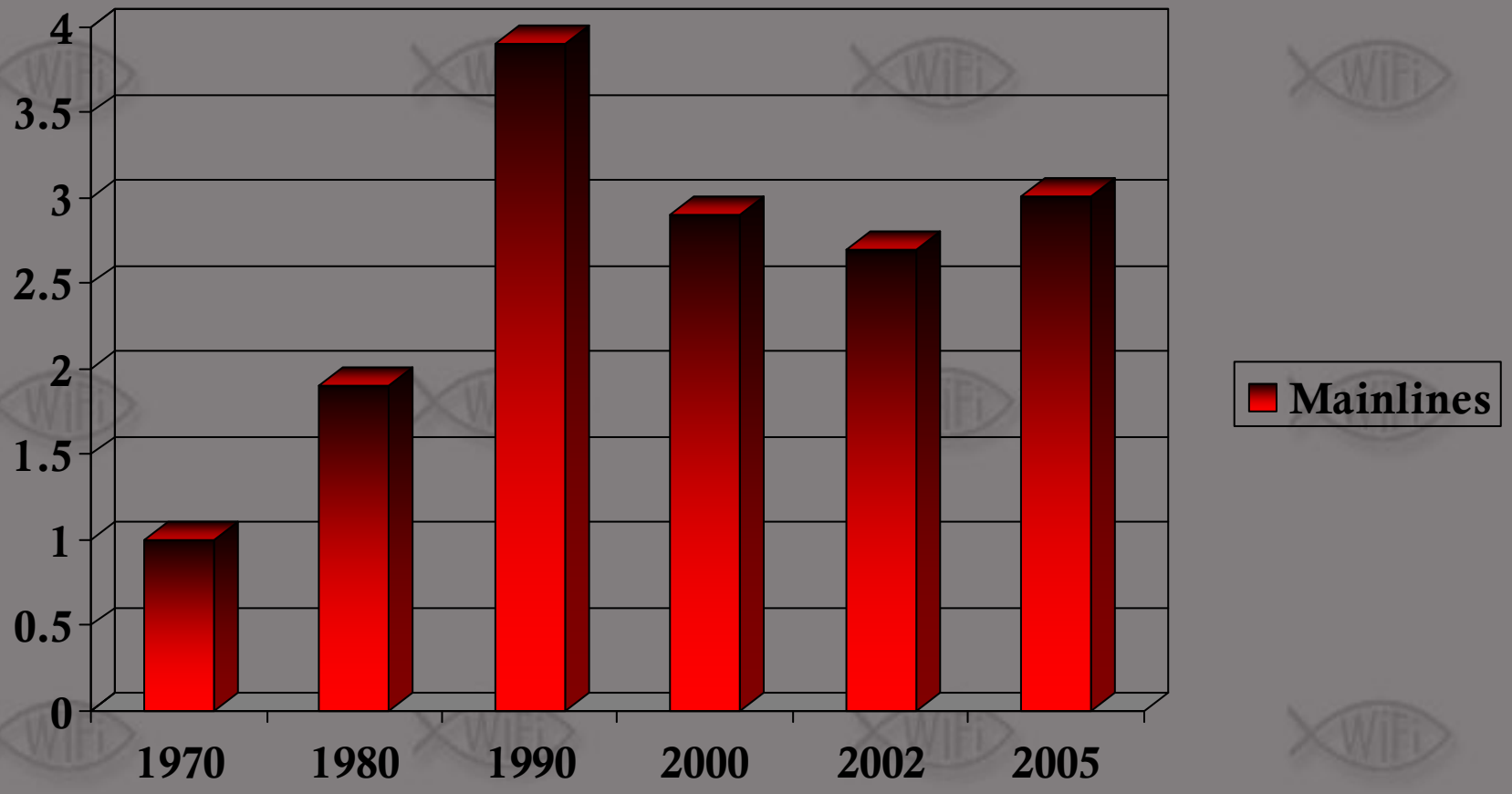
Iraqi Communications Infrastructure

- Landlines
- Cell networks
- Internet
  - History, dialup, satellite, wireless
- Satellite-based communications

Landline network

- Heavily damaged in Gulf War, Iraq War, and subsequent looting of stations
- ~833,000 lines in use (pop. ~26.7 mil)
  - Spotty service for those who do have dedicated lines
- Estimated $1 billion cost to rebuilt
  - Passed over in favor of cell networks

Telephone Mainlines per 100 people



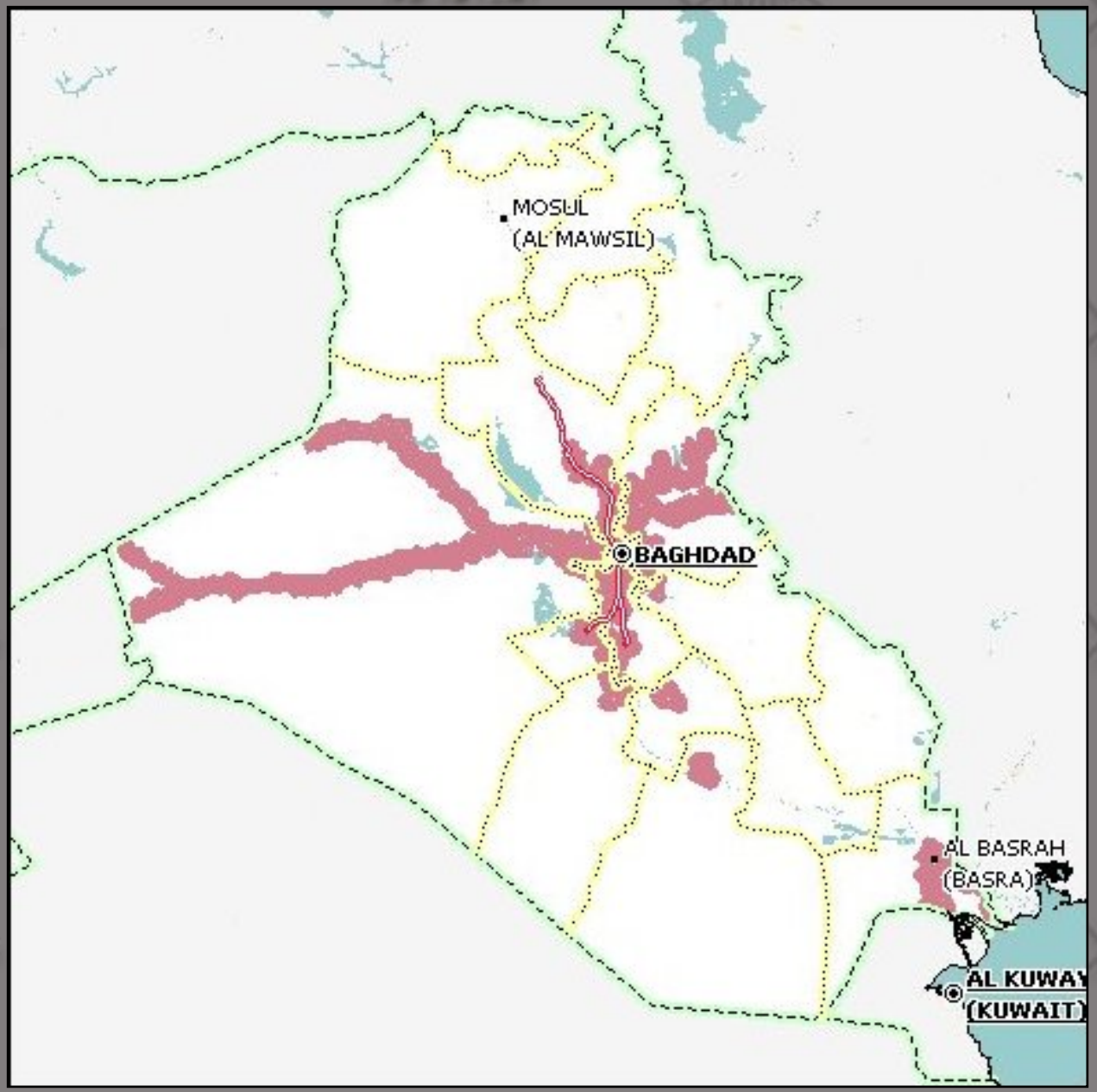
Cell networks

- Cell networks began installation 2003-04
- Iraqi cell phone providers (GSM 900)
  - **Iraqna**, **Asia Cell**, Atheer, Korek, SanaTel
  - 2004: 1.4 million subscribers
  - 2006: 7.1+ million subscribers

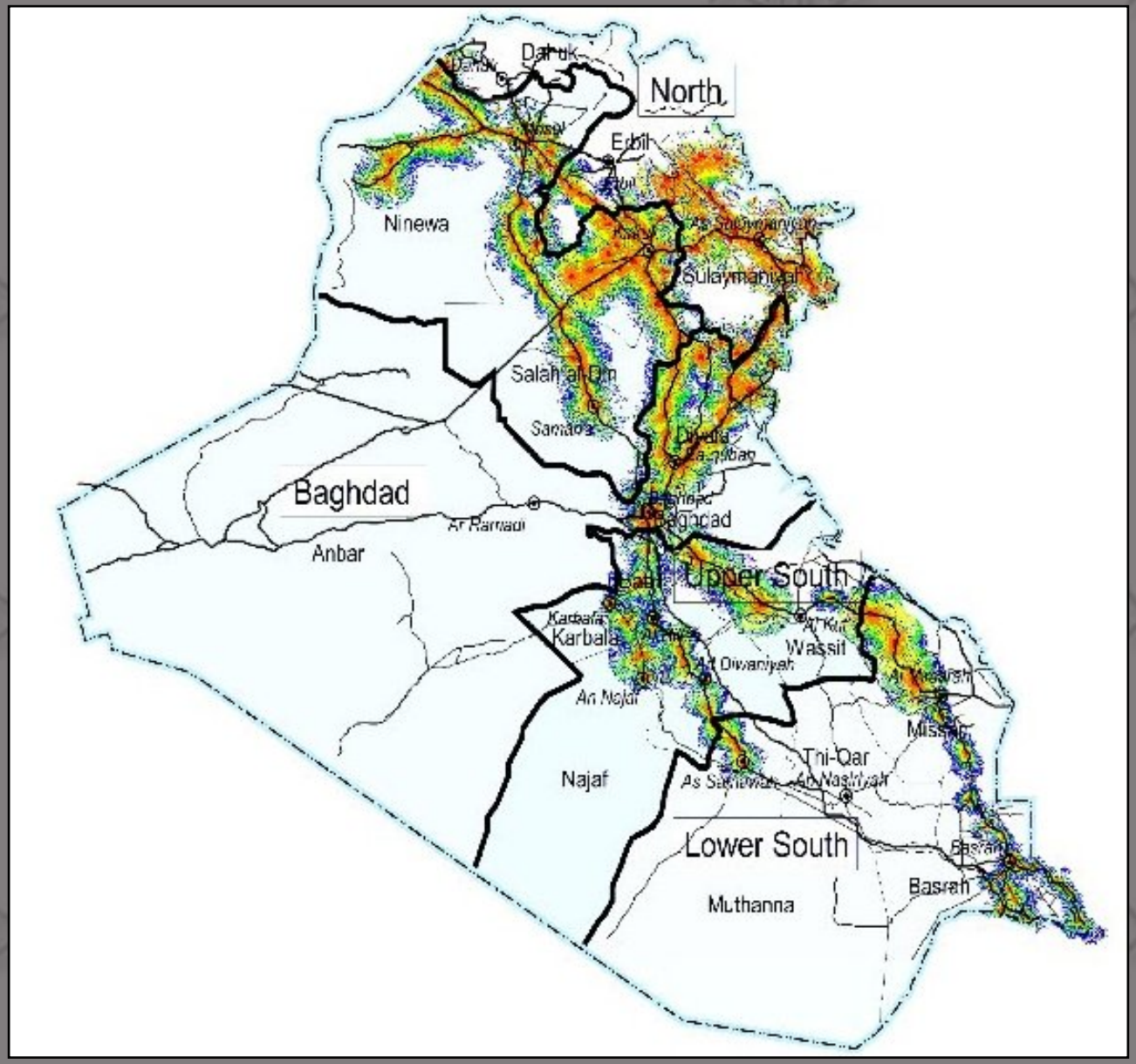




IRAQNA COVERAGE MAP

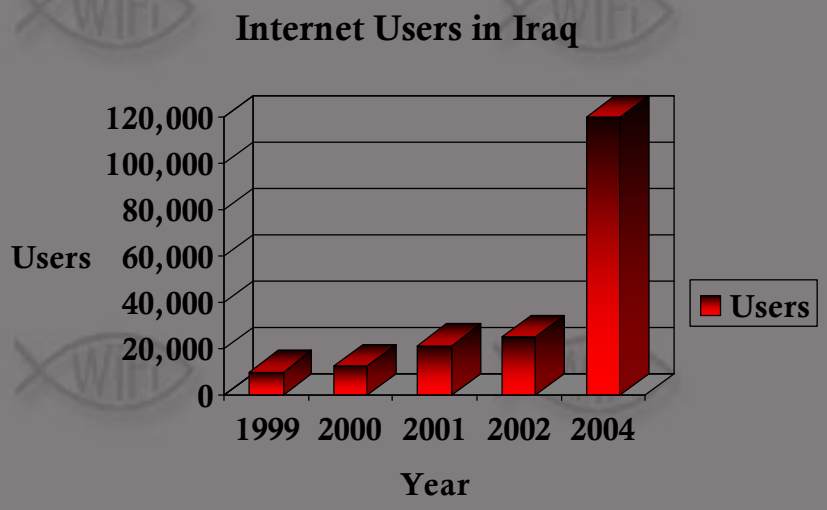


ASIA CELL COVERAGE MAP



Internet

- Pre-1999
  - ~10,000 users (mostly dialup)
    - Ba'athists, Loyalists, Wealthy
- 1999-2003
  - <25,000 users
  - ~75 Internet cafes
    - Censored satellite connection
- 2003-Present
  - 120,000 users and growing; Est. 500% increase in users over 5 years
  - Iraqi ISPs: Uruklink + others
  - Middle East/European VSAT



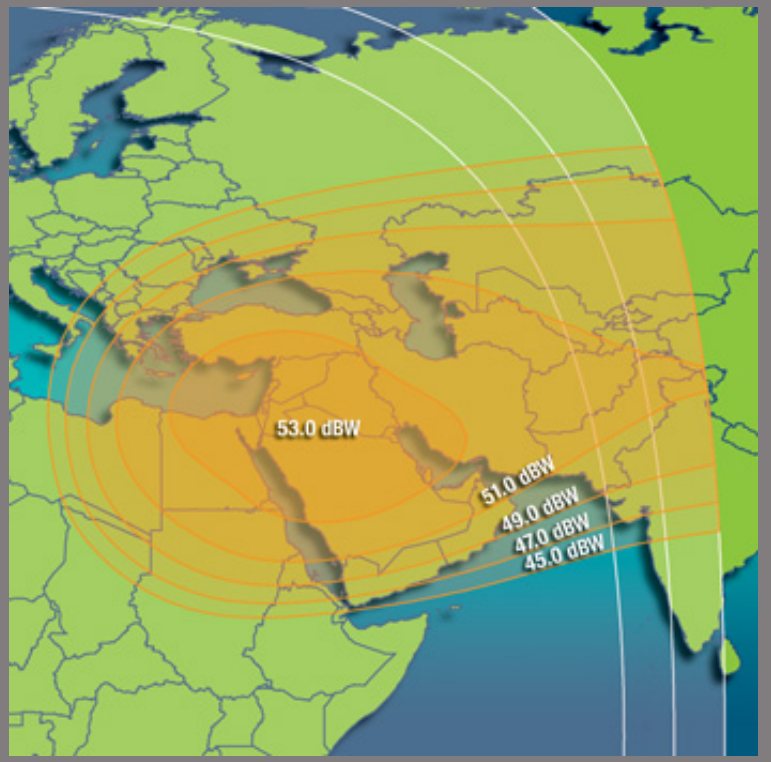
Internet

- .IQ domain originally owned by InfoCom
- Finally assigned to Iraq ~2005
- Many government sites still using .org, .net



Satellite-based communications

- A sample of other available satellite-based communications services:
  - Intelsat
  - Intersputnik
  - Thuraya (UAE)
  - Iridium



Improvised Explosive Devices

What makes up an IED?

Initiator

Detonator

Explosive charge





Initiators

- Command-wire (CWIED)
- Victim-operated (VOIED)
- Vehicle-borne (VBIED)
- Radio-controlled (RCIED)

[4]MNC-I Public Affairs Office; reprinted at http://www.arcent.army.mil/news/archive/2005_news/march/new_organization.asp; also http://www.defenselink.mil/news/BriefingSlide.aspx?BriefingSlideID=14

RC Initiators









Improvised Explosive Devices

What makes up an IED?

Initiator

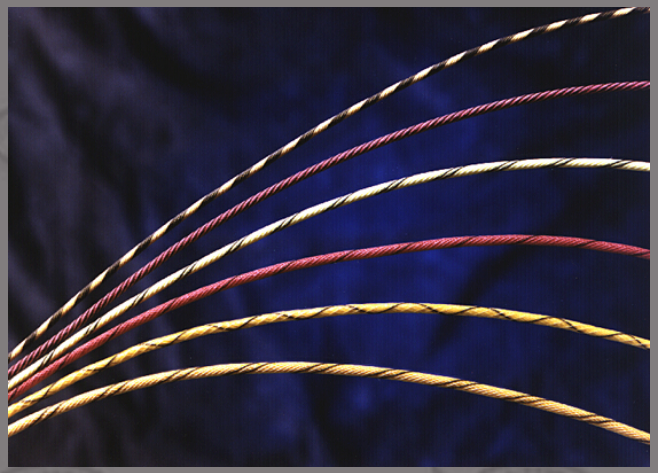
Detonator

Explosive charge





Detonators






EXPLOSIVE
DETONATOR-425-MS
DETONATOR-425-MS


AUSTIN POWDER COMPANY
A-CORD
FINE LINE

Improvised Explosive Devices

What makes up an IED?

Initiator

Detonator

Explosive charge





Explosive charges











Attacking the IED Problem



Eliminate source materials



Eliminate the IED network



Eliminate bomb emplacers



Prevent detonation



Protect against explosion

Eliminating Source Materials: Initiators

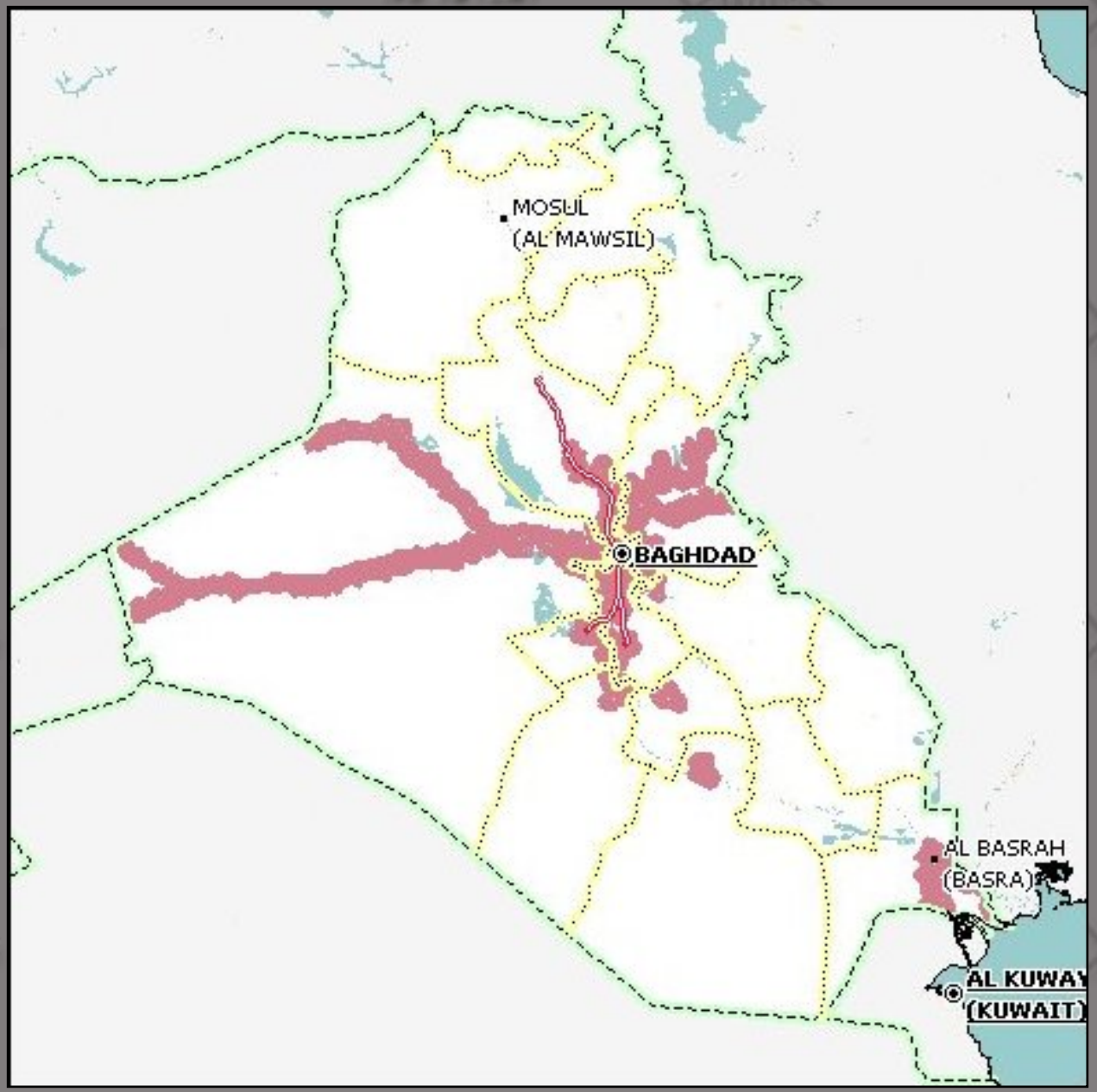
- Initiators have become dual-use technologies
  - Designed for non-military purposes
  - Exploited as initiation devices for IEDs
- Plentiful supply
- Virtually impossible to track
- Required for basic governmental functions

Eliminating Source Materials: Initiators

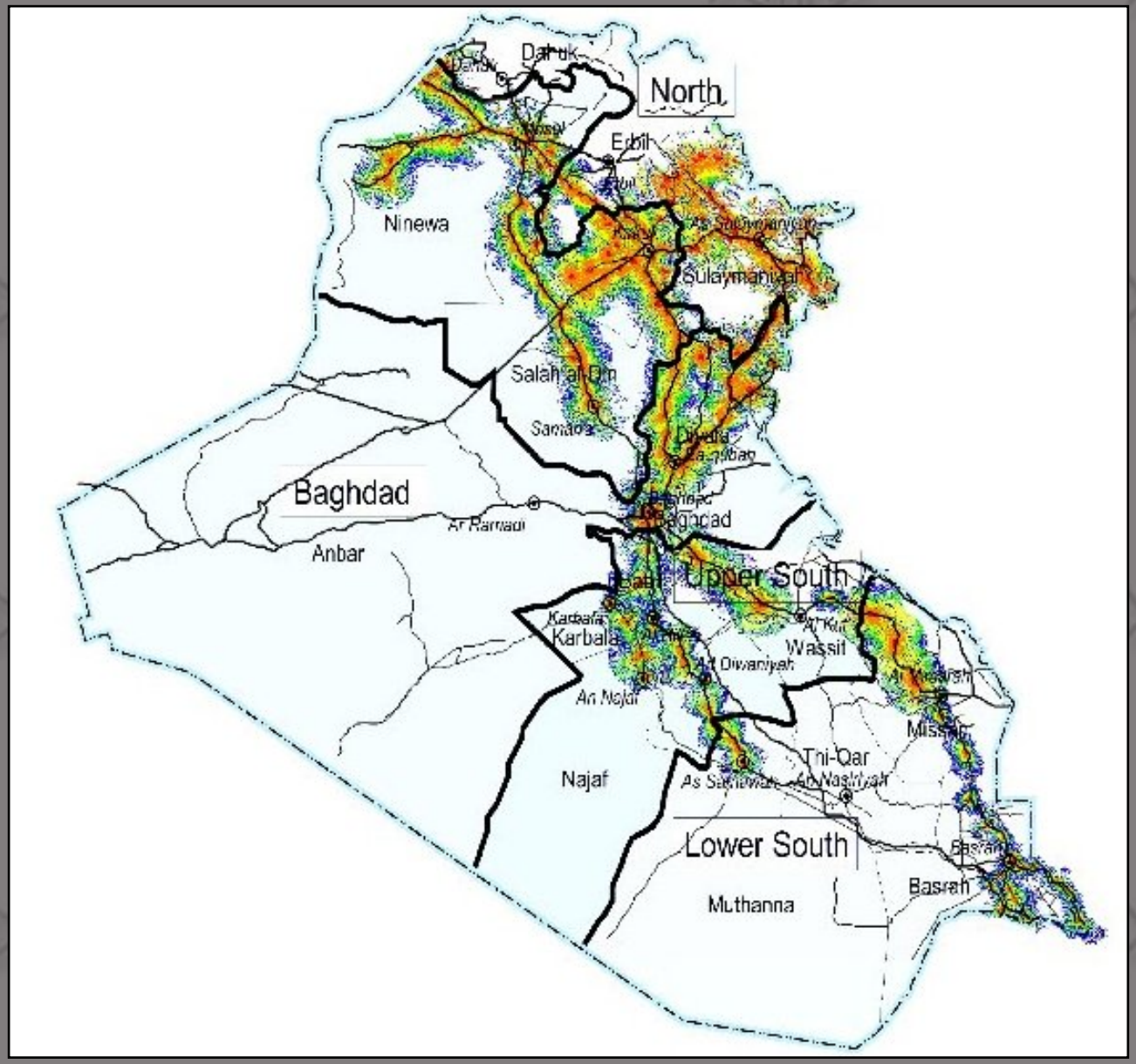
- Iraqi landline network virtually non-existent
- Extremely costly to rebuild ($1+ billion)
- Cell networks began installation 2003-04
- Iraqi cell phone providers (GSM 900)
  - **Iraqna**, **Asia Cell**, Atheer, Korek, SanaTel
  - 2004: 1.4 million subscribers
  - 2006: 7.1+ million subscribers



IRAQNA COVERAGE MAP

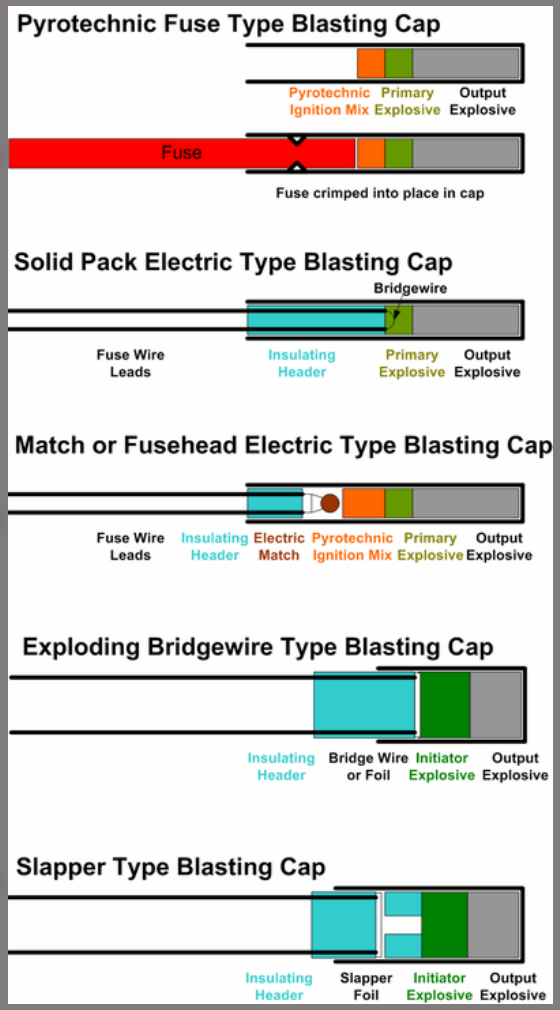


ASIA CELL COVERAGE MAP



Eliminating Source Materials: Detonators

- Detonators are also dual-use technologies
  - Legitimate uses particularly in construction (especially given the massive rebuilding effort)
  - Exploited as initiation devices for IEDs
- Plentiful supply
- Virtually impossible to track



Eliminating Source Materials: Explosive charges

- Huge caches of unused ordnance left over from the Iran-Iraq War (1980-88) and Gulf War (1991)
  - Artillery shells, mortar shells, unexploded ordnance
- Focus on WMD and major conventional weapons systems
- Plentiful supply
- Virtually impossible to track

Attacking the IED Problem



Eliminate source materials



Eliminate the IED network



Eliminate bomb emplacers



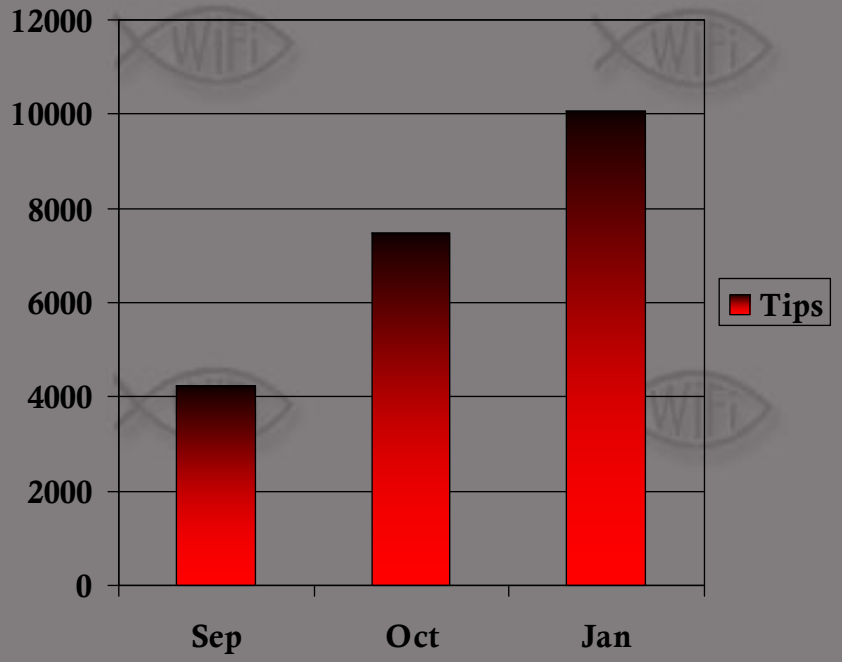
Prevent detonation



Protect against explosion

Eliminating the IED Network

- Locate and eliminate the financiers and support structure behind IED-making cells[5]
- JIEDDO Budget for "offensive operations" grown from 13% in FY06 to 31% in FY07[6]



[5]http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3901

[6]http://www.defenselink.mil/news/newsarticle.aspx?id=3275



Eliminating the IED Network: CEXC

Combined	Coalition
Explosives	IEDs
Exploitation	Forensic investigation and hardware hacking
Cell	Group

Eliminating the IED Network: CEXC

"CEXC provides **technical and operational analysis** of the improvised bombs the insurgents have used against coalition forces, and develops measures to counter the bombing campaign."[7]

[7]http://www.washtimes.com/national/20050316-110733-3348r.htm

Eliminating the IED Network: TEDAC

The U.S. Government explosives community, including the FBI, the Department of Defense, and the Bureau of Alcohol, Tobacco, and Firearms, collectively formed the Terrorist Explosive Device Analytical Center ("TEDAC"). Located at the FBI Laboratory in Quantico, Virginia, the TEDAC acts as a single inter-agency focal point to coordinate and manage the unified effort of law enforcement, intelligence and military assets as it relates to terrorist IEDs, and to **technically and forensically exploit** all IEDs …[8]

[8]http://www.usdoj.gov/opa/motion_dna.pdf; see also http://www.fbi.gov/page2/aug04/jordan081104.htm

Attacking the IED Problem



Eliminate source materials



Eliminate the IED network



Eliminate bomb emplacers



Prevent detonation



Protect against explosion

Eliminate Bomb Emplacers

- Emplaces IED at target location
- May or may not be part of the IED network
- May or may not arm/initiate the device
- May be involved in video-taping the incident
- Eliminating bomb emplacers:
  - Tips
  - Community pressure
  - $$$

Attacking the IED Problem



Eliminate source materials



Eliminate the IED network



Eliminate bomb emplacers



Prevent detonation



Protect against explosion

Prevent Detonation

- My primary job in Iraq
- "Suppress the RCIED threat to Coalition Forces and reduce casualties through enhanced electronic warfare coordination and JCREW operations, training and readiness."[9]
- Jammers
  - Airborne, Vehicle-mounted, Dismounted
  - Different models/manufacturers
  - Different capabilities
  - That's all I have to say about that…

[9]https://www.militaryhomefront.dod.mil/campvictory3/

Attacking the IED Problem



Eliminate source materials



Eliminate the IED network



Eliminate bomb emplacers



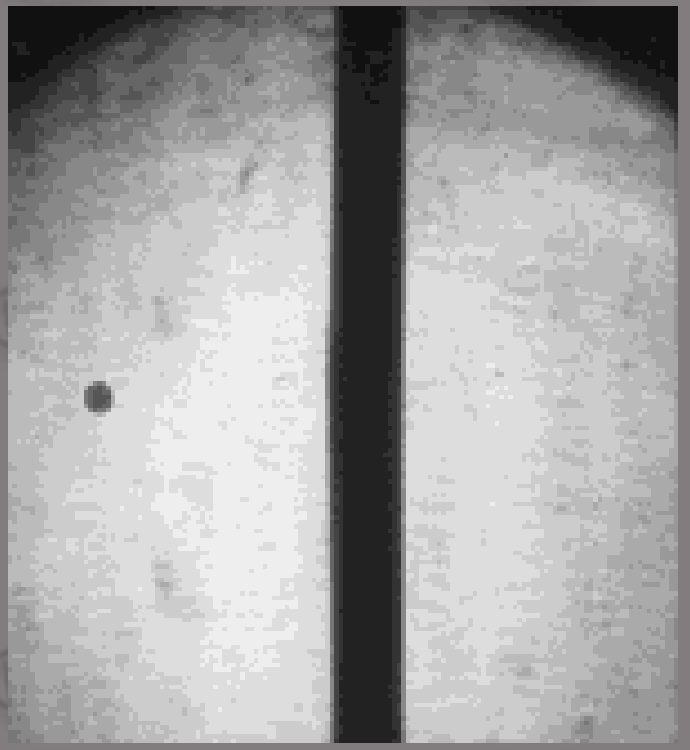
Prevent detonation



Protect against explosion

Protect Against Explosion

- Armor protection: It's not really just about "more"
  - HHS/brittle/spalling
  - RHA/spall protection



Protect Against Explosion

- More armor means more weight
  - Decreases maneuverability/speed
  - Increases rollover potential (higher COG)
  - Increases maintenance on engines and transmissions
- Underbody vs. sides
- V-shaped hulls

The Future

- Detection of IEDs using unintentional radiated emissions[10]
- Explosive resistant coating to add protection without adding significant weight[11]
- "Local Eyes" sensor network[12]

[10]http://web.umr.edu/~daryl/IEDs/

[11]http://www.ara.com/whatnew/lead/dragonshield/explosive%20resistant%20coating.htm

[12]http://www.nationaldefensemagazine.org/issues/2006/December/ResearchersTout.htm

The Future

- Hyperspectral sensors[13]
- Answers to the Explosively Formed Penetrator (EFP)



[13]http://www.nationaldefensemagazine.org/issues/2006/December/ResearchersTout.htm



CHURCH OF WIFI
TIME TO PLAY

DEFCON

Acknowledgements

- DEFCON Staff
- The Church of Wifi
- My Family

See Also

- Wireless Village @ Skybox 209
- Wireless Contests



CHURCH OF WIFI

TIME TO PLAY

DEFCON

Questions?

CHURCH OF WIFI
TIME TO PLAY

presents

DEFCON



A Hacker in Iraq

Michael Schearer ("theprez98")







