#PRISM : let's have a look at the big picture

By Kitetoa, June 24th 2013

http://reflets.info/prism-lets-have-a-look-at-the-big-picture/

A long time ago in a galaxy far, far away, Daisy had a knowledge database stored on a Netscape Web server. Its aim was to secure the US military networks (and more). However, this Web server was secured like shit…

Please, meet my friend Daisy :

> *The Defense Information Systems Agency (DISA), is a United States Department of Defense (DoD) combat support agency composed of military, federal civilians, and contractors. DISA provides information technology (IT) and communications support to the president, vice president, secretary of defense, the military services, the combatant commands, and any individual or system contributing to the defense of the United States.*

Almost all the IT projects, all of the Army's and the Government's communication problems, everything was there. A unique view on how the US Government and Army reacted to the 9/11 events, a way to understand what was in the mind of the USA behind its war on terror.

What can be learned from these documents ?

- The neocons had shitty ideas.
- Wikileaks couldn't have happen without these projects.
- The US wanted to know everything about their citizens.
- Networks have diplomatic consequences.
- US military networks are as rotten as their private counterpart.
- The military networks were undersized when the "global war on terror" started.
- 9/11 was a momentum. NeoCons had an agenda. It helped.

Soon after 9/11, NeoCons promoted a huge Net Centric plan for the Army and the Government. Its ambition was for the "Warfighters" to get all the needed information to take the right decision at the right time.

But guess what: a secret, is a secret. A shared secret isn't a secret anymore…

If you're looking for accountability, look no further than the Bush administration and – specifically -Paul Wolfowitz, deputy defense secretary in the Bush administration, as he was one of the key guys for the Net Centric plan.

C4n I Haz a PhoN3 L1n3 pleAz ?

Please meet the Global Information Grid, the Net Centric concept…

The GIG provides the foundation for NCW, information superiority, decision superiority, and, ultimately, full-spectrum dominance, as depicted in the following figure.

Source: Capstone Requirements Document for the GIG

Foundation for Achieving Full-Spectrum Dominance

The concept of the GIG evolved from concerns about the interoperability and end-to-end integration of automated information systems. Issues such as streamlined management and improved information infrastructure also heightened the interest in a GIG. However, the real demand for a GIG originates from the requirement for information and decision superiority to achieve full-spectrum dominance, as expressed in Joint Vision 2020. The ability to achieve shared situational awareness and knowledge among all elements of a joint force, including allied and coalition partners, is increasingly viewed as a cornerstone to transform warfighting capabilities.

Network Centric Warfare. The GIG Capstone Requirements Document states that NCW allows a warfighting force to achieve improved information positions in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power.

Information Superiority. Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority is achieved in a noncombat situation, or one in which there are no clearly defined adversaries, when friendly forces have the information necessary to achieve

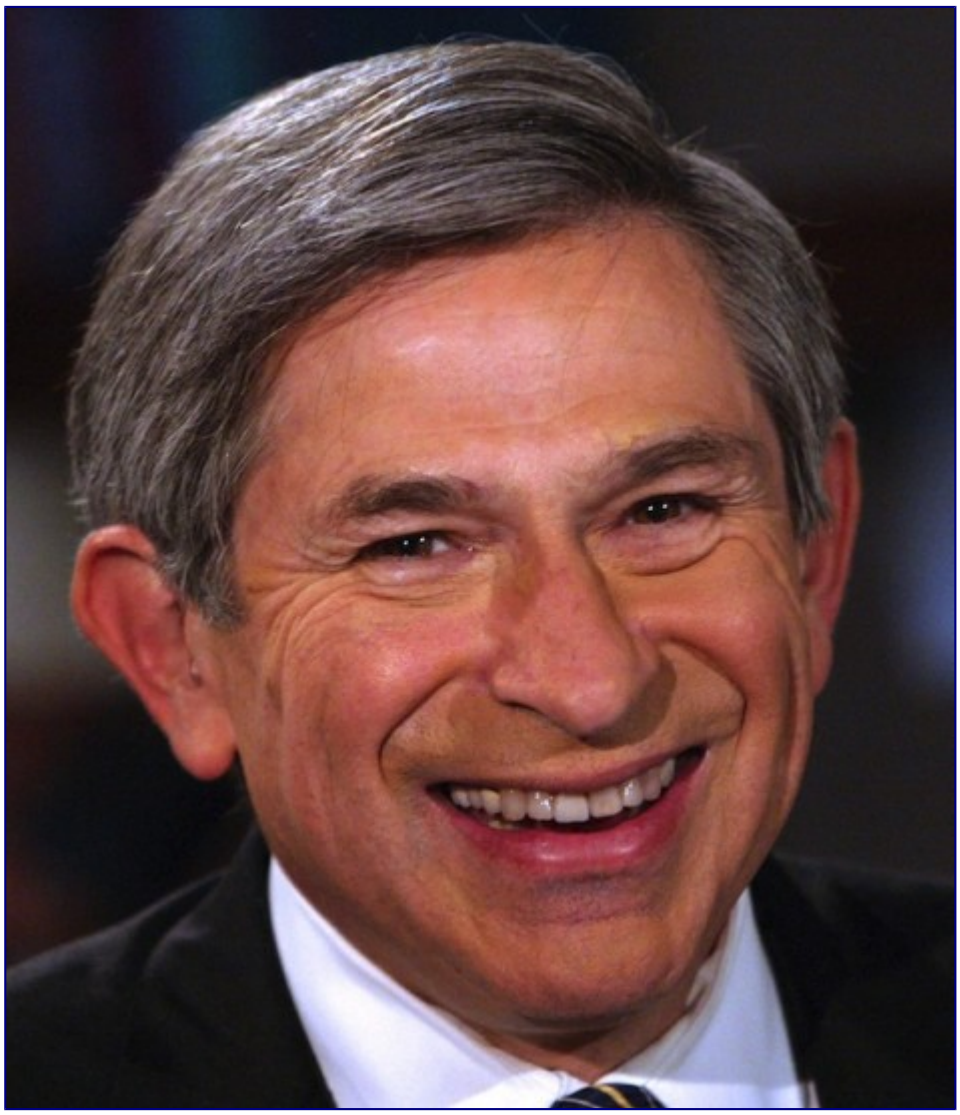
The GIG is defined as a global interconnected end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.
The GIG comprises many systems that interoperate to provide the right info to the right places when needed. (...) allow vast amounts of information to be readily accessed by anyone, anywhere, anytime

GIG, connecting people...

The GIG had to be connected to every useful information source, like the Department of Homeland Security (see the MOU here), or NATO... (see the MOU here).

Before reading any further, answer this question honestly: where you really surprised by the PRISM leaks ? Well, PRISM is just a small part of the GIG.

For our part, we were in no way surprised by anything PRISM revealed so far.



On May 2003, Paul Wolfowitz created Talon.

Years after Kitetoa.com and Wired published articles about Talon, a document about this project appeared on Wikileaks.

This database codenamed Talon was designed to collect the following pieces of information :

- non-specific threats to DoD interests;
- Suspected surveillance of DoD facilities and personnel;
- elicitation attempts, suspicious questioning, or other suspected intelligence collection activities focused on DoD interests;
- tests of security;
- **unusual repetitive activity**;
- bomb threats;

- and any other suspicious activity and incidents reasonably believed to be related to terrorist activity directed against DoD personnel, property, and activities within the United States.

Talon would include :

> *« Non validated » information on strange behavior of American citizens and raw information reported by concerned citizens and military members regarding suspicious incidents. Information in TALON reports is non-validated, may or may not be related to an actual threat, and by its very nature may be fragmented and incomplete. The purpose of the TALON report is to document and immediately disseminate potential threat information to DoD personnel, facilities, and resources…*

To say this differently, it has been public knowledge for years now that the American Government wanted to know everything about its citizens. Even *non validated* information. Even information that is *not related to an actual threat*.

How does that sound ?

Talon was probably to be inserted into the GCCS-J.

What's that? You might ask.

> *"GCCS-J is widely used by all the combatant commands, all Service GCCS programs, USCG, DIA, NSA"*
>
> *The Global Command & Control System – Joint (GCCS-J) service offers vital connectivity to systems used to plan, execute and manage military operations for both joint and multinational operations. GCCS-J fuses select C2 capabilities into a comprehensive, interoperable system by exchanging imagery, intelligence, status of forces, and planning information. GCCS-J is focused on meeting emerging operational needs through sustainment and synchronization support to operational baselines (Global, COP I3 and JOPES) and subject matter experts to assist with critical operation and the GCCS-J Family of Systems (FoS).*
>
> *GCCS-J is a Command, Control, Communications, Computer, and Intelligence (C4I) system for achieving full spectrum dominance, consisting of hardware, software, procedures, standards, and interfaces that provide a robust, seamless C2 capability to the Commander-in-Chief (CINC), Secretary of Defense (SECDEF), National Military Command Center (NMCC), Combatant Commanders (CDRs), Joint Force Commanders, and Service Component Commanders. It is a suite of mission applications fusing select C2 capabilities into a comprehensive, interoperable system by exchanging imagery, intelligence, status of forces, and planning information. GCCS-J is the principal foundation for dominant battlespace awareness, providing an integrated, near real-time picture of the battlespace necessary to conduct joint and multinational operations. It offers vital connectivity to the systems the joint warfighter uses to plan, execute, and manage military operations.*
>
> *The GCCS-J modernization vision is focused on continuing to decompose applicable existing applications into services, limiting local deployment, and continuing to expose data and scale services to support an enterprise implementation; reducing overall sustainment cost through use of more cost effective and appropriate COTS and HW products; and increasing the use of*

agile development practices.

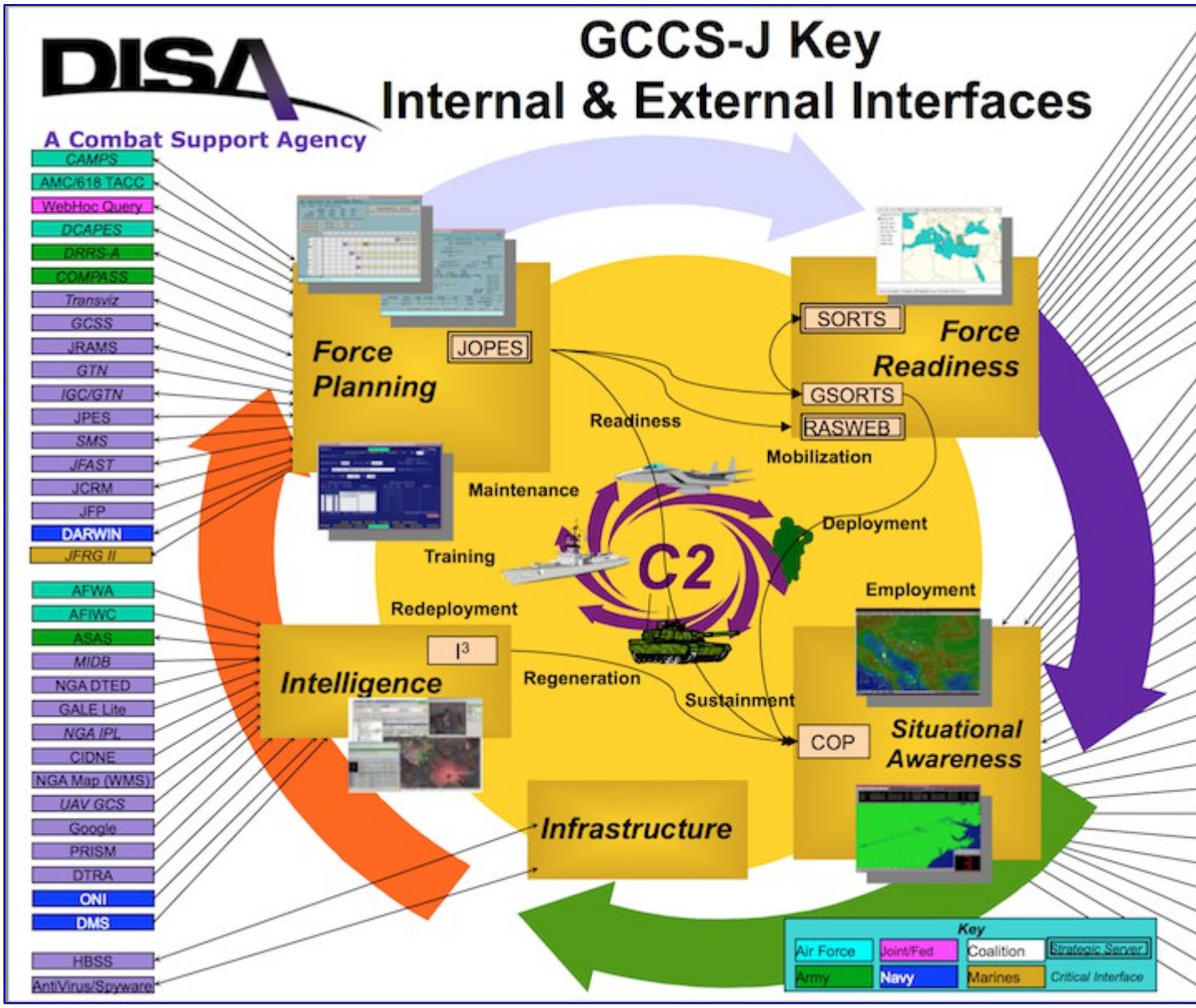
The GCCS-J is, in fact, the real effective GIG. It is used by the US Army and other agencies so that the « warfighter » can make the good move, at any time, based on good intelligence.

GCCS is the tool for C2 (C2 : « *the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission*«)

Ok… But PRISM ? Well… When suicide bombers lolcats wants to blow the USA, the Empire needs something useful to defeat them. Why not PRISM ?

PRISM is a part of the GCCS-J.

Looking for Waldo PRISM



 There are a lot of acronyms in this slide. Here is a little help from our friends at the Disa :

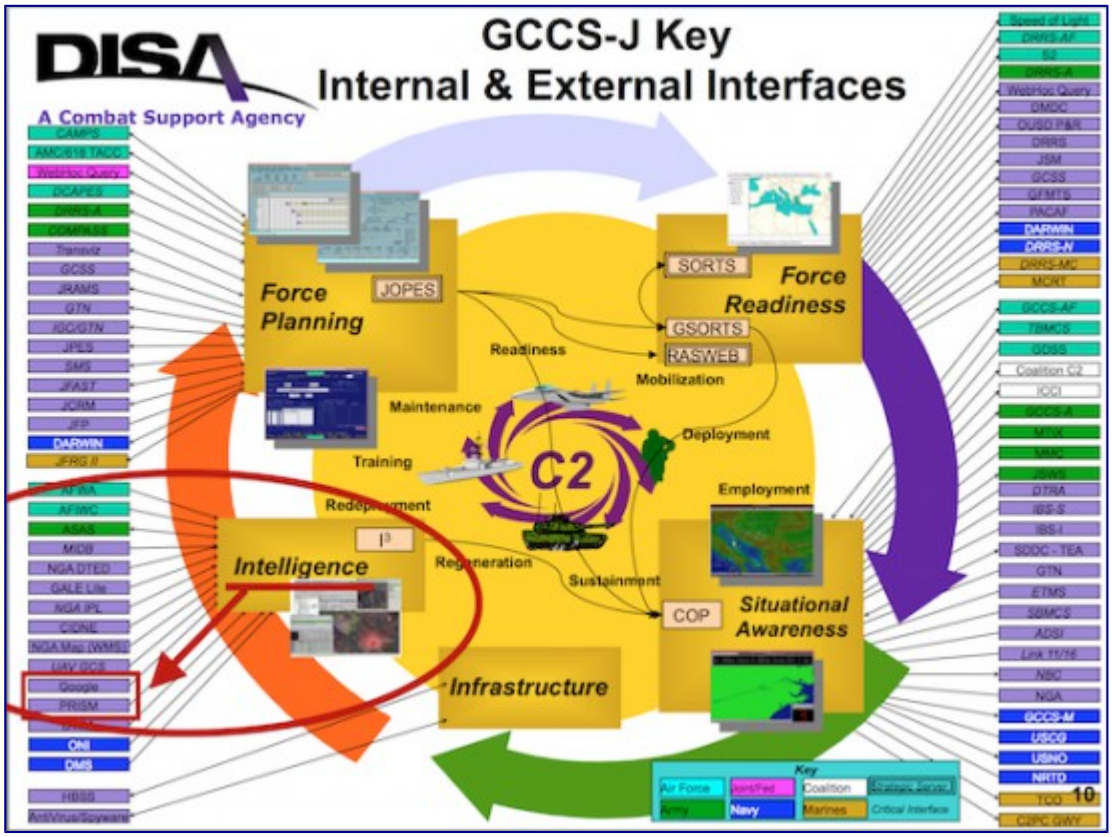
- DVT – Deployment Visualization Tool
- JOPES – Joint Operation Planning and Execution System
- ACOA – Adaptive Courses of Action
- JFRG II – Joint Force Requirements Generator
- SORTS – Status of Resources and Training System
- GSORTS – GCCS Status of Resources and Training System
- COP – Common Operational Picture
- CAMPS Consolidated Air Mobility Planning System
- LOGCAT/ BCAT Logistician's Contingency Assessment Tools/ Beddown Capability Assessment Tool
- WHQ WebHoc Query
- DCAPES Deliberate Crisis Action Planning and Execution System
- AF Weather AF Weather Agency
- TBMCS Theatre Battle Management Core Systems
- AFIWC Air Force Information Warfare Center
- AFSORT DET Air Force SORTS Data Entry Tool
- JADE Joint Assistant for Deployment & Execution
- AFSATCOM/ TIBS Air Force Satellite Communications – Tactical Information Broadcast System
- GDSS Global Decision Support System
- ALOG Army Logistics
- GCCS-A Global Command and Control System – Army
- TAG TPFDD Access Gateway
- COMPASS Computerized Movement Planning And Status System
- FOCUS Force Operation Characteristics Unified System
- ASAS All Source Analysis Remote Workstation
- ASORTS Army SORTS
- SDDC-TEA Surface Deployment and Distribution Command – Transportation Engineering Agency
- JSTARS Joint Surveillance Target Attack Radar System

- MAGTF II Marine Air Ground Task Force II
- GOMERS Global Online Marine Editing and Reporting System
- IAS Intelligence Analysis System
- FSR – Force Status Readiness (USSTRATCOM)
- JSC – Joint Spectrum Center
- DARWIN Dynamic Analytical Reporting Web-based Interactive Navigator
- USN Observatory Time Source US Naval Observatory Time Sync Interface
- TRMS Type Commander Readiness System
- GCCS-M Global Command and Control System – Maritime
- NNSOC Naval Network and Space Operations Command
- FNMOC Fleet Numerical Meteorological and Oceanographic
- NRTD Near Real Time Data
- AMP Analysis of Mobility Platform (USTRANSCOM)
- MAT Medical Analysis Tool
- SMS Single Mobility System
- ICIS Integrated Consumable Item Support
- JFAST Joint Flow And Analysis System For Transportation
- TCAIMS II Transportation Coordinators Automated Information For Movement System II
- MIDB Modernized Integrated Database
- NGA 5D Demand Driven Direct Digital Dissemination
- WinJMEM Windows – Joint Munitions Effects Manual
- NGA IPL Integrated Products Library
- UAV GCS Unmanned Aerial Vehicle Ground Control Station
- GPS Global Positioning System Time Source
- DMS/AMHS Defense Message System/Automated Message Handling System
- Raindrop Raindrop Point Mensuration
- DMDC Defense Manpower Data Center
- CFAST Collaborative Force-Building Analysis Sustainment and Transportation
- DRRS Defense Readiness Reporting System
- FEDB Failure Experience Data Bank
- FEDMTC Federal Multi-TADIL Capability
- JRAMS Joint Readiness Automated Management System
- TDDS Tactical Data Dissemination System
- TRIXS Tactical Reconnaissance Intelligence Exchange Service
- GALE Lite Generic Area Limitation Environment
- GTN Global Transportation Network
- ETMS Enhanced Traffic Management System
- SBMCS Space Battle Management Core System
- ADSI Air Defense System Integrator
- EPLRS Enhanced Position Location Reportying System
- QTRACS Qualcomm Tracks
- ADAMS Allied Deployment and Movement System
- NATO ICC NATO Integrated Command and Control
- NATO JOIIS Joint Operations Intelligence Information System

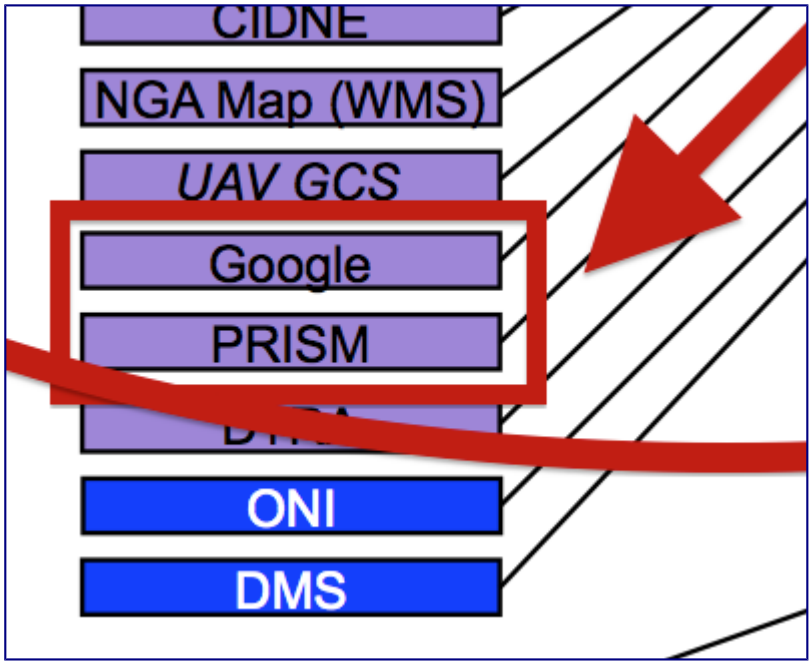
Note that PRISM is not in the list.

Did you find Waldo PRISM ?

Let's focus on the left side of the image :



Let's zoom in…



Now, the big question… What PRISM are we talking about?

There are a few « PRISM » in the Army…

- PRISM Portable Resource for the Investigation of Suspected MANPADS [MANPADS denotes Man-Portable Air-Defense Systems]
- Planning Research and Intelligence Scalable Modeling (PRISM)
- PRISM Input Tool (© Mitre Corporation)
- There is a PRISM in Israel : Global Research in International Affairs (GLORIA)

Center THE PROJECT FOR THE RESEARCH OF ISLAMIST MOVEMENTS (PRISM)

The PRISM everybody is talking about theses days is probably this one:

> ***Planning Tool for Resource, Integration, Synchronization, and Management (PRISM)****, a subsystem of collection management mission application. A Web-based management and synchronization tool used to maximize the efficiency and effectiveness of theater operations. PRISM creates a collaborative environment for resource managers, collection managers, exploitation managers, and customers.*

Fortunately, you can find some definitions of PRISM in the Army's publications.

> *Where applicable, requests for SIGINT support should be entered into approved systems such as PRISM, for approval by the designated signals intelligence operational tasking authority (SOTA).*
> *Collection Management Mission Application (CMMA). CMMA is accessed through JWICS and SIPRNET and comprises a tailorable suite of interoperable automated tools designed to enhance the collection planning, execution, and ISR battle management capability of CCMDs, subordinate joint forces, and components. CMMA includes PRISM, which is used in collection planning, operations, and managing of intelligence collection assets that are deployed to all CCMDs and USFK.*
>
> Source : Joint and National Intelligence Support to Military Operations - 05 January 2012

The Rand Corporation also gives some clues: in 2007, the Rand published a paper entitled « *A Strategies-to-Tasks Framework for Planning and Executing Intelligence, Surveillance, and Reconnaissance (ISR) Operations*« . This report suggest improving ISR collection planning and execution through the implementation of a strategies-to-task framework for collection planning.

The report states that PRISM is « *Currently used to integrate collection requests from the JFC and various components and, with other tools, generate the daily collection deck*« .

It looks like PRISM is a tool you can use to integrate demands for intelligence and collect MANY kind of data. Not only the one from Google, Facebook, etc.

Remember GCCS-J : there are many networks, many sources. Not only PRISM.

Let's go back to the Army's definition :

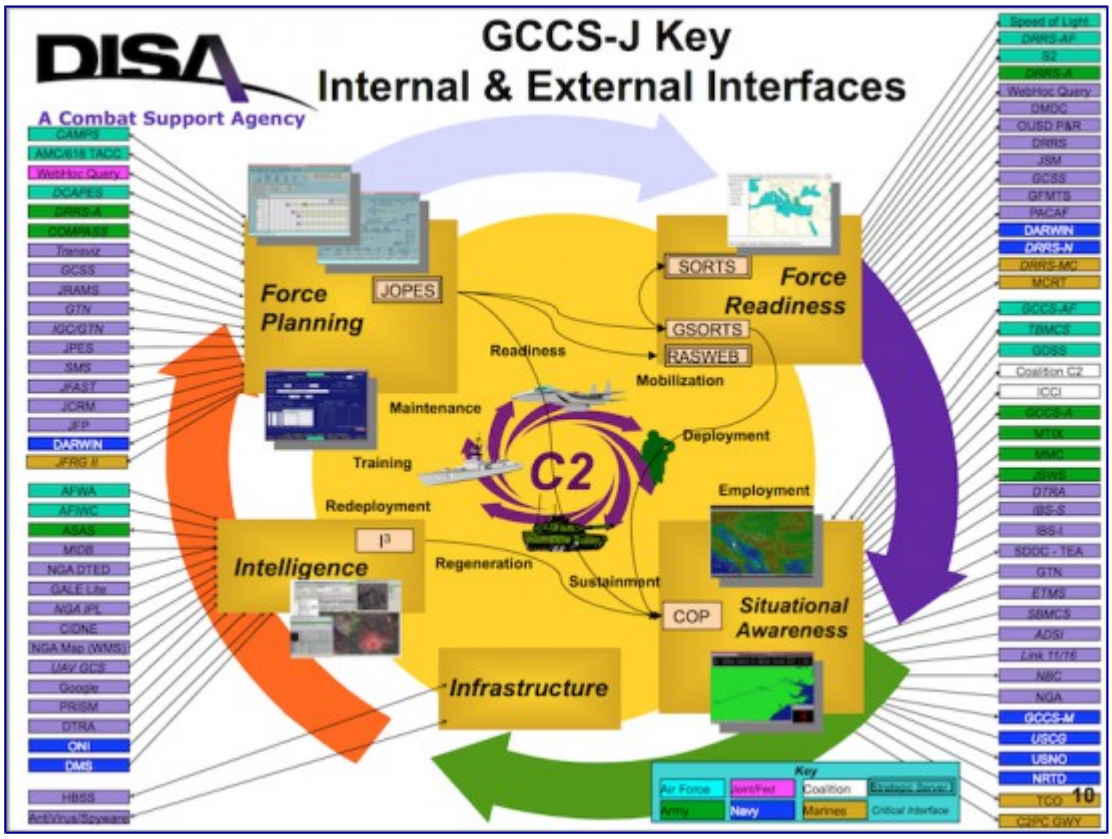
> *JOINT ISR PLANNING SYSTEMS*
> *Two joint ISR planning systems—the collection management mission application and* ***the Planning Tool for Resource, Integration, Synchronization, and Management (PRISM)—help facilitate access to joint resources. PRISM, a subsystem of collection management mission application, is a Web-based management and synchronization tool used to maximize the efficiency and effectiveness of theater operations.*** *PRISM creates a collaborative environment for resource managers, collection managers, exploitation managers, and customers. In joint collection management operations, the collection manager coordinates with the operations directorate to forward collection requirements to the component commander exercising tactical control over the theater reconnaissance and surveillance assets. A mission*

> *tasking order goes to the unit responsible for the collection operations. At the selected unit, the mission manager makes the final choice of platforms, equipment, and personnel required for the collection operations based on operational considerations such as maintenance, schedules, training, and experience. The Air Force uses the collection management mission application.* ***This application is a Web-centric information systems architecture that incorporates existing programs sponsored by several commands, Services, and agencies. It also provides tools for recording, gathering, organizing, and tracking intelligence collection requirements for all disciplines.***
>
> Source

Let's recap…

The PRISM you've read about in the media seems to be a small part of a bigger PRISM which in turn, is a small part of a huge system used by the Army, the Government and the Intelligence community : the GCCS-J.

Let's have a look at the big picture once again :



Echelon: so 20th century…

PRISM may look as something huge, but this is the XXIth century, guys…

We don't want to tap fax machines: let's head for the backbones!

> "*We hack network backbones – like huge internet routers, basically – that give us access to the communications of hundreds of thousands of computers without having to hack every single one*".

Edward Snowden

Hacking the backbones (the backbones routers) isn't about getting some information from Google of Facebook, it's about tapping all the internet's information flows. This, is huge.

So, how's PRISM working?

So far, we don't know.

The journalists who have THE PowerPoint presentation only released 5 slides out of 41.

Too bad. Journalism has it's limits… People probably don't need to know everything, right?

Still, we can guess how PRISM is working. One thing's for sure: they have access to private US companies' data, but they could do without it. Big routers and backbones are easier to tap.

Don't forget the NSA has Narus and… so many backbones to tap.

Even if the US government decided to drop the PRISM program (the one your read about in the Press), they would still have all the tools needed to see what's in your email.

Flower Pilgrim: like a virgin

How about France? What is doing our government? Do we also tap the backbones?

Fleur Pellerin, french state secretary for digital economy, said she was awaiting « *explanations* » from the US Gov. concerning this « *alarming* » PRISM news.

But Wait… There's more. She also said on Jan 1, 2013 :

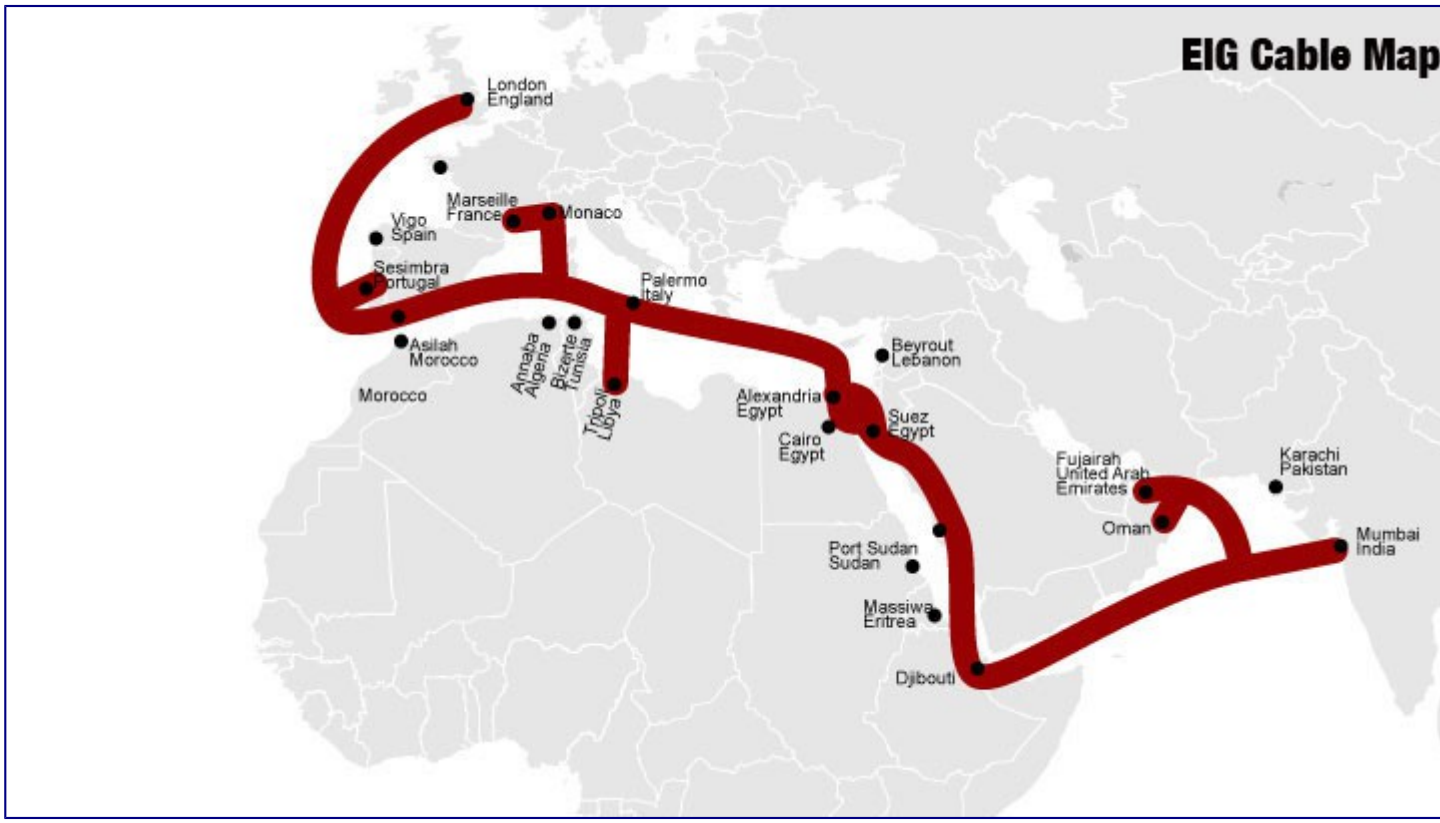
> « ***The Alcatel Submarine Networks (ASN) expertise is indeed unique*** *and covers the production, installation and maintenance of submarine cables. This is a strategic activity to connect overseas territories and the African continent with broadband.* ***There is also an issue related to cyber surveillance and homeland security****. We support a solution that maintains the integrity of ASN and its national roots.* ***Let me remind you that any equity takeover would in any case be subject to a review of the Treasury under the decree on foreign investment in France***.«

Surprisingly, a few days after the PRISM leaks were published, *Le Monde*, on June 11 (2013) published a paper entitled « *In France, the* [secret services] *DGSE at the core of an internet monitoring program*« .

Note this interesting quote:

> « *The French authorities argue that the* [DGSE Internet spying] *sites are, for the most part, based abroad, which exonerated the DGSE to respond to French law.*«

Can I h4Z a #PrismBurger ?



Surprisingly (or not), every time you can locate an internet surveillance Amesys Eagle installation, there is an Alcatel cable next to it:

- Alcatel was leader of the consortium who built EIG.
- Alcatel owns the routers
- The EIG cable lands in Tripoli, Libya (a happy Eagle owner)
- The EIG cable lands in Jeddah, Saudi Arabia (a suspected happy Eagle owner)
- The EIG cable lands in Fujairah, United Arab Emirates (a suspected happy Eagle owner)
- Another cable (FLAG Alcatel-Lucent Optical Network) lands in Qatar (a happy Eagle owner)
- Another cable (Atlas Offshore) lands in Morocco (a happy Eagle owner)
- The ACE (African Coast to Europe) cable installed by Alcatel lands in Gabon (a happy Eagle owner)
- Jan, 2011 : Alcatel-Lucent announced that it has completed the deployment of the first gigabit passive optical network (GPON) in Astana, the capital city of Kazakhstan (a suspected Eagle owner)

Networks have diplomatic consequences…

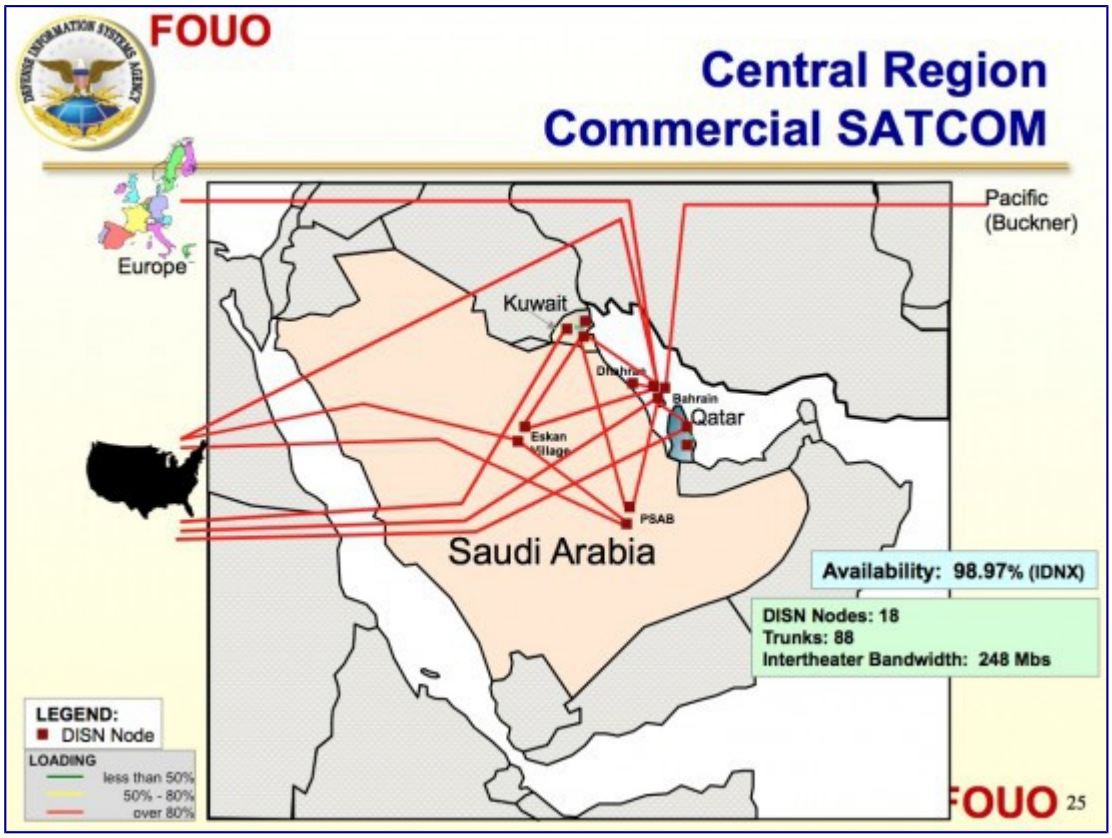
Tell me where is your network going through, I'll tell you who's your friend or foe.

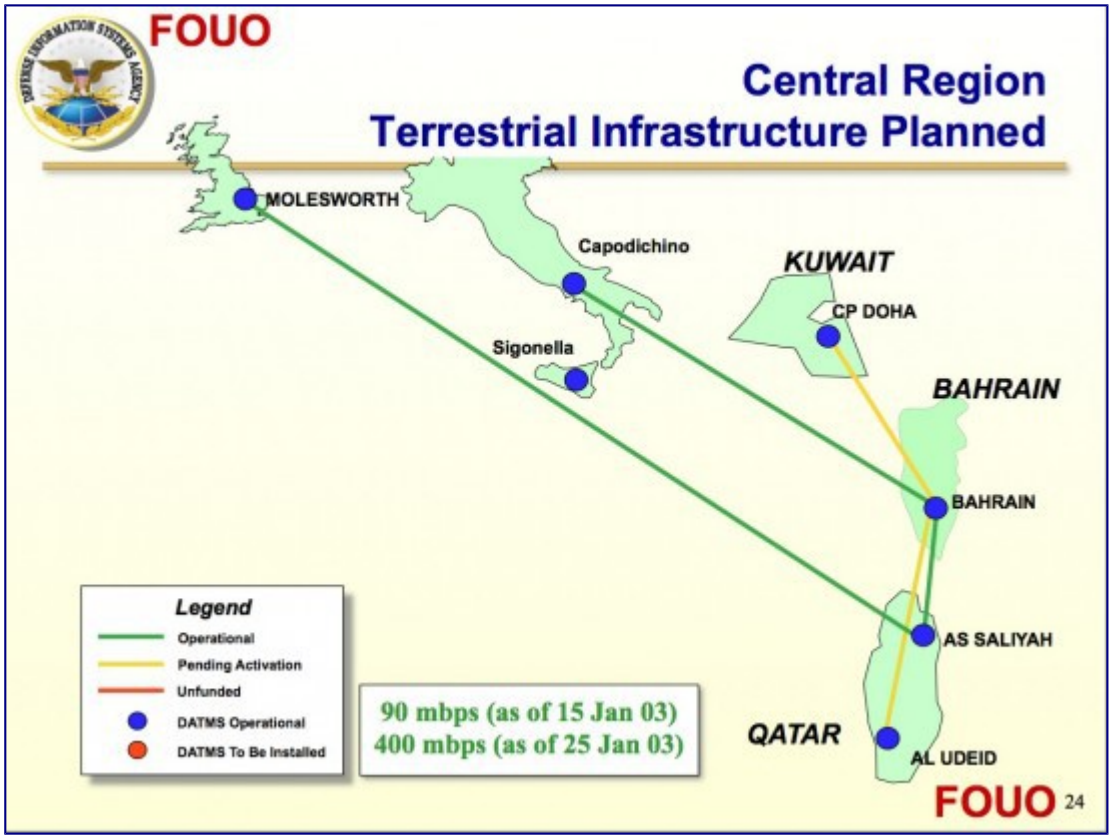
As an example, let's look at Bahrain and its neighboring cables.

Did you notice nobody's talking about Bahrain and its popular protests, no more that it's bloody repression? Do you wonder why? Part of the answer might come from the fact that the U.S. military has a very important military base in this small country. The Defense Information System Network (DISN) South West Asia and DISN-Pacific is managed from Bahrain: « *Network management is performed by the Bahrain RNOSC on a 7 x 16 basis and transfers to the Europe RNOSC after hours and anytime the Bahrain RNOSC needs*

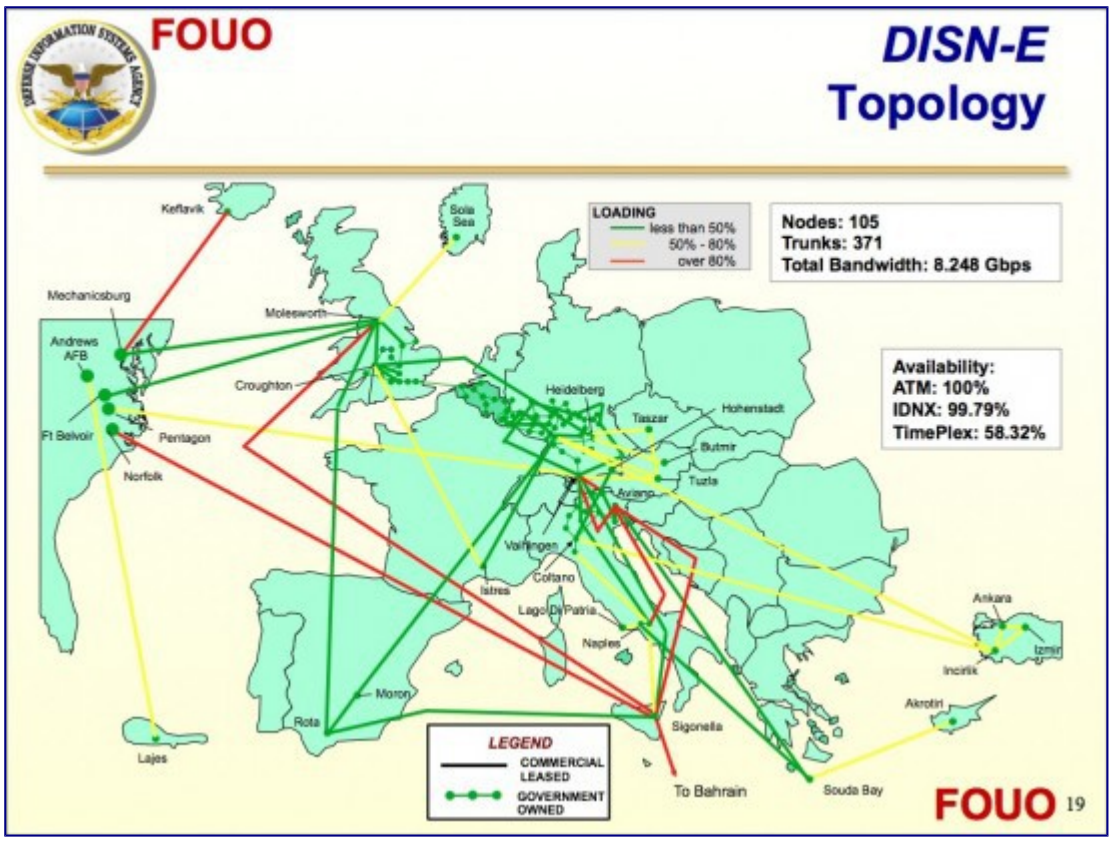
assistance« .

But there is more.





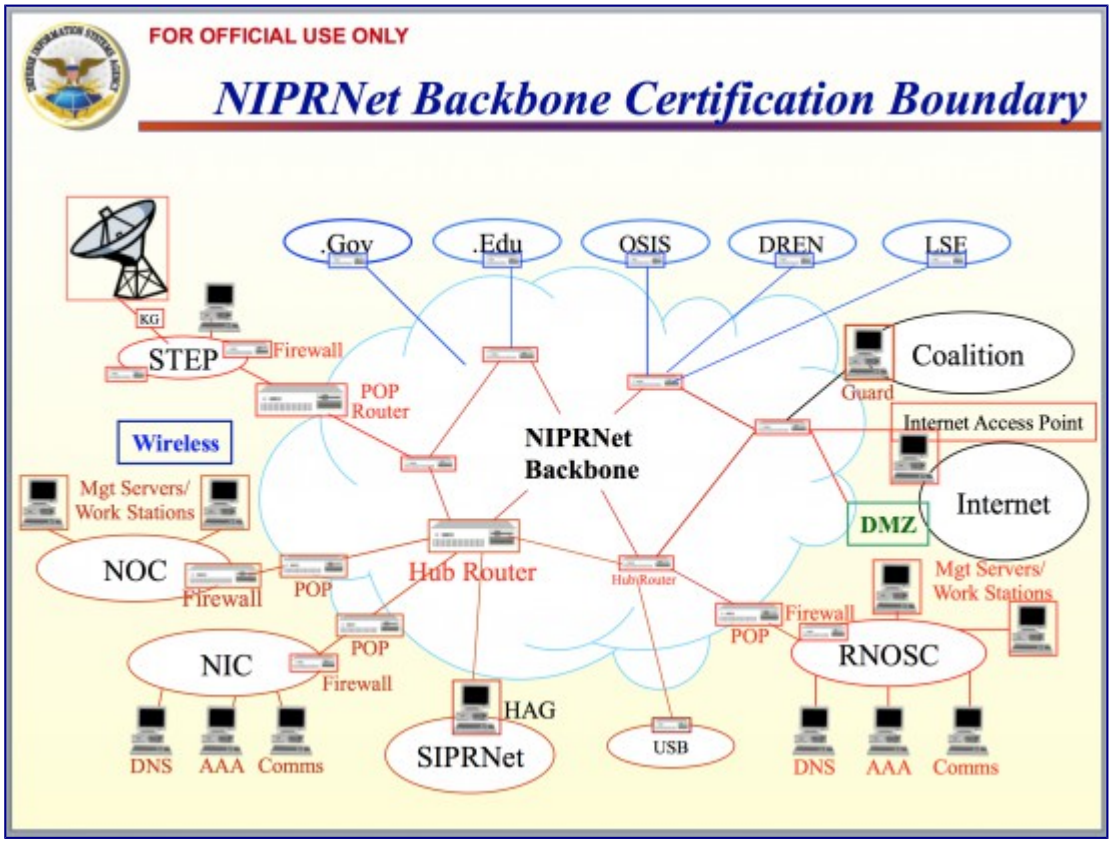
Oh-Oh… Wait… France (Istres) is here too :



Now, I guess *Reflets.info* would qualify as an unlawful combatant, don't you think ?

Are we helping Osama Bin Laden by publishing those maps? Oh Wait… He's dead. Must be OK then.

Let's look further into those documents then, while we keep asking ourselves: how secure are those US military networks, like the NIPRNet?



When presenting the "*Unclassified But Sensitive Internet Protocol Router Network (NIPRNet) Backbone*" at a "*Certification Decision Briefing*" in 2003, there were a few bugs left pending.

Let's have a look!

FOR OFFICIAL USE ONLY

Purpose

- Decision Brief to the Principal Director for Operations and Designated Approval Authority (DAA) for the Department of Defense Information Systems Network (DISN) that are Defense Information Systems Agency (DISA) developed and maintained
- The Goal is to obtain a 180 day extension to the Interim Authority to Operate (IATO) for the NIPRNet Backbone based upon:
  - Certification Authority's recommendation and recent Security Testing and Evaluation results
  - NIPRNet Backbone Compliance with DISA security policies and procedures
  - Acceptable risk mitigation of all remaining findings

3

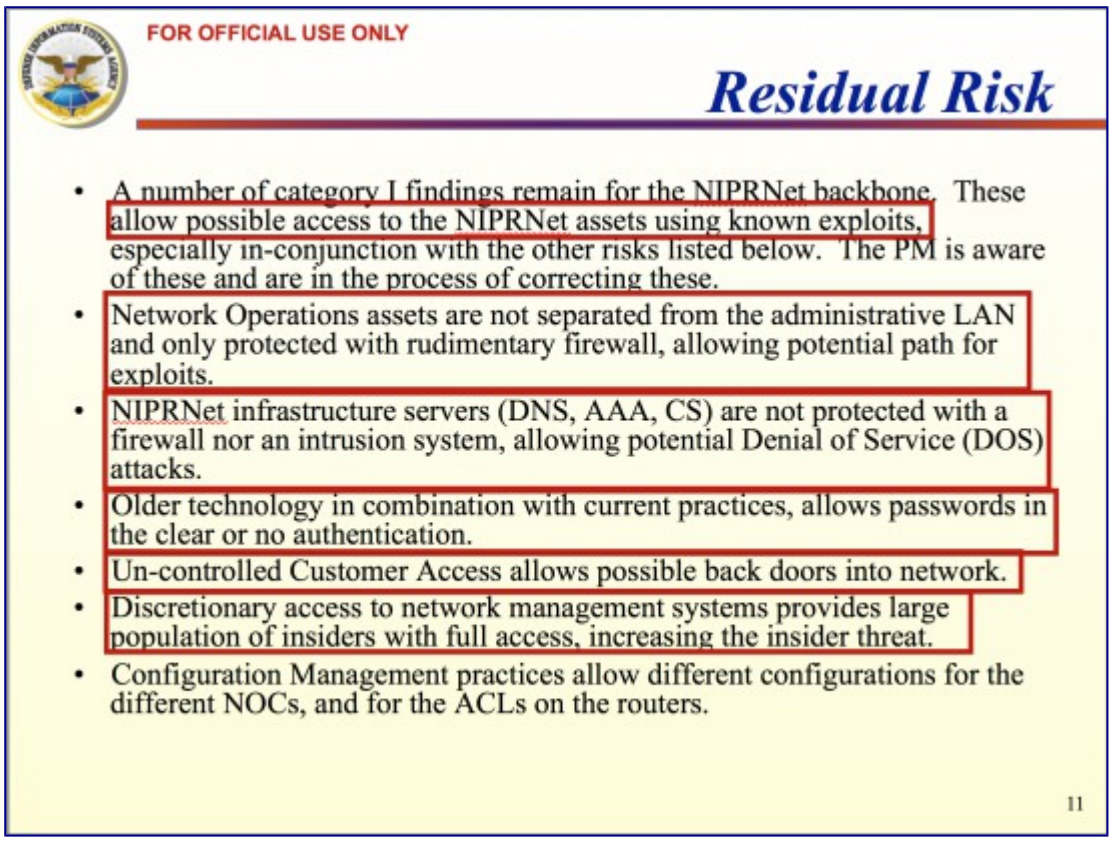
FOR OFFICIAL USE ONLY

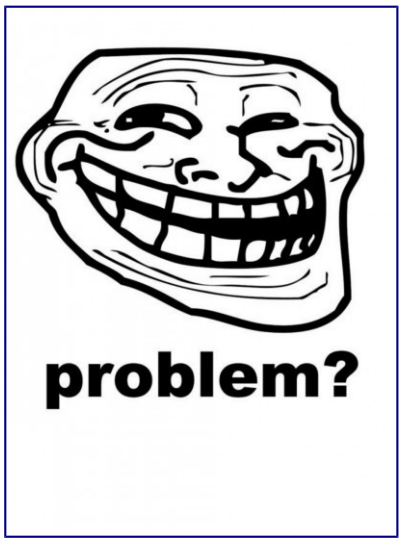
Current Findings

Finding Type	Columbus	NIC	USB	PAC	EUR	NIPRNet Totals
CAT 1						
Initial	29	10	5	12	9	65
Worked-Off	27	9	5	12	9	62
Current	**2**	**1**	**0**	**0**	**0**	**3**
CAT 2						
Initial	353	243	38	186	140	960
Worked-Off	262	233	38	155	139	827
Current	**91**	**10**	**0**	**31**	**1**	**133**
CAT 3						
Initial	152	84	32	88	33	389
Worked-Off	96	81	32	83	33	325
Current	**56**	**3**	**0**	**5**	**0**	**64**
CAT 4						
Initial	32	1	3	14	11	61
Worked-Off	28	0	3	12	11	54
Current	**4**	**1**	**0**	**2**	**0**	**7**
Total						
Initial	566	338	78	300	193	1475
Worked-Off	413	323	78	262	192	1268
Current	**153**	**15**	**0**	**38**	**1**	**207**

***As of 21 Apr 2003. Numbers based on FSO Database with new findings from Columbus**

9





Problem?

Problems don't happen only with networks security.

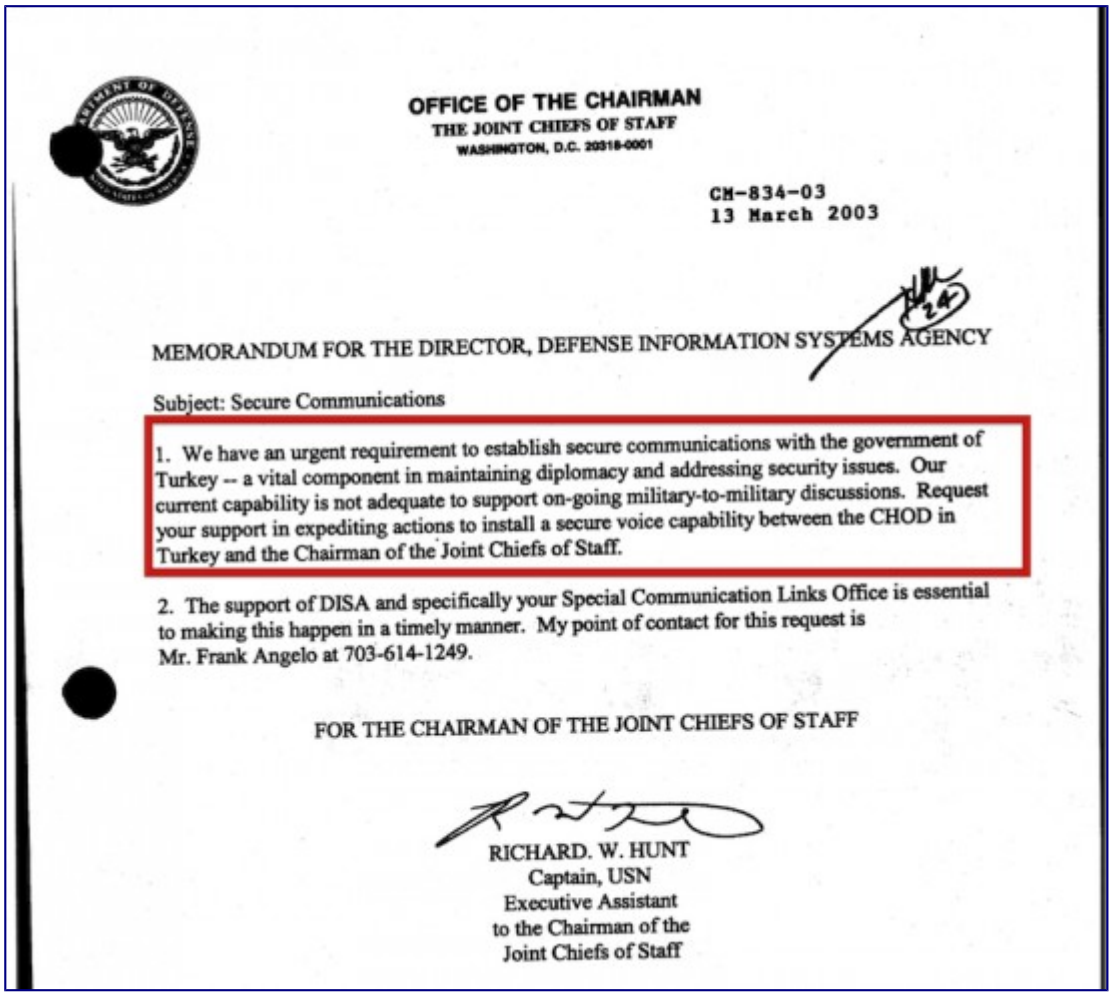
The Iraqi war began on March 20, 2003 with Iraq's invasion (codenamed « Operation Iraqi Freedom ») by the coalition led by the United States.

But guess what…

Seven days before, on March 13, the Office of the Chairman at the Joint Chiefs of Staff requested a secured line with the turkish government. At the time, they didn't have any…

Why did they asked for such a secured line? Captain Obvious probably told them that they needed an official approval before flying some F16 over Turkey…

C4n I Haz a PhoN3 L1n3 pleAz ?



OFFICE OF THE CHAIRMAN
THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-0001

CM-834-03
13 March 2003

MEMORANDUM FOR THE DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

Subject: Secure Communications

1. We have an urgent requirement to establish secure communications with the government of Turkey -- a vital component in maintaining diplomacy and addressing security issues. Our current capability is not adequate to support on-going military-to-military discussions. Request your support in expediting actions to install a secure voice capability between the CHOD in Turkey and the Chairman of the Joint Chiefs of Staff.

2. The support of DISA and specifically your Special Communication Links Office is essential to making this happen in a timely manner. My point of contact for this request is Mr. Frank Angelo at 703-614-1249.

FOR THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF

RICHARD. W. HUNT
Captain, USN
Executive Assistant
to the Chairman of the
Joint Chiefs of Staff

Shit happens. Not only with networks security, not only with phone lines… But also with the bandwidth when you want to wage war on the Universe.

Wait… A war ? Two Wars ? Three wars ? Chill out! We don't have enough bandwidth, says the Army!

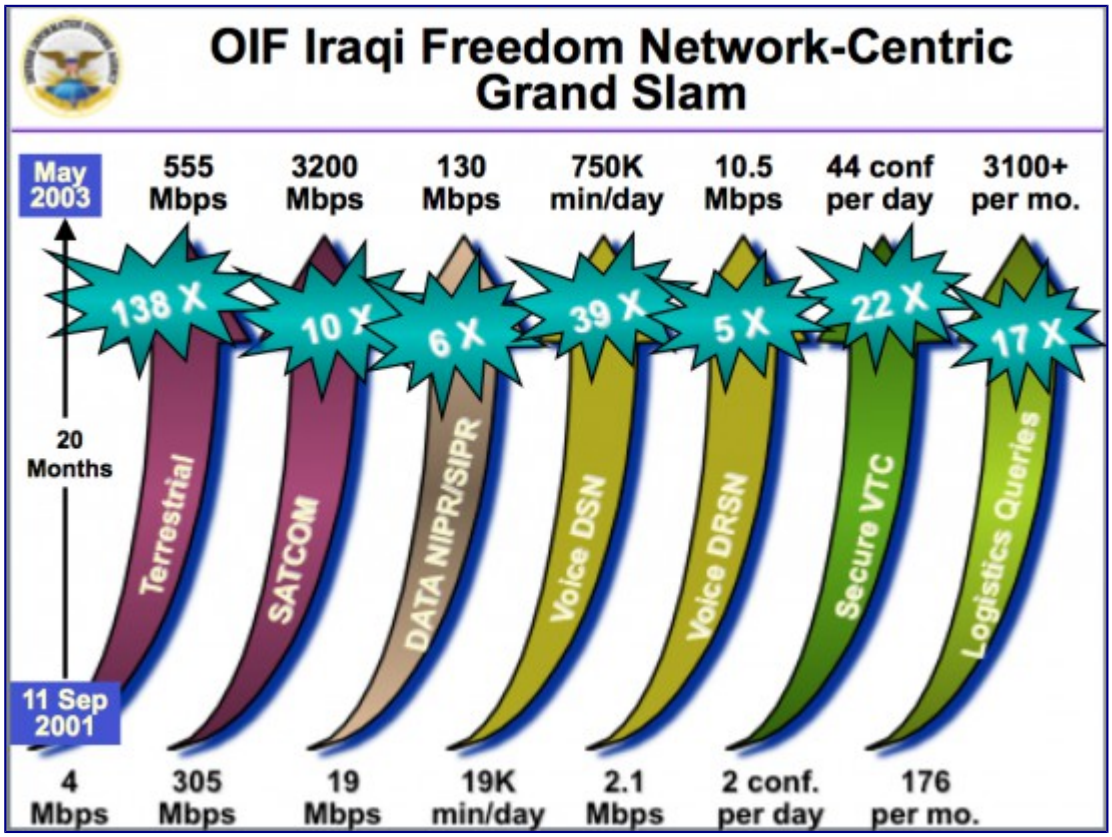
9/11 led to the Afghan war (OEF), the Iraq war (OIF) and the infamous global war on

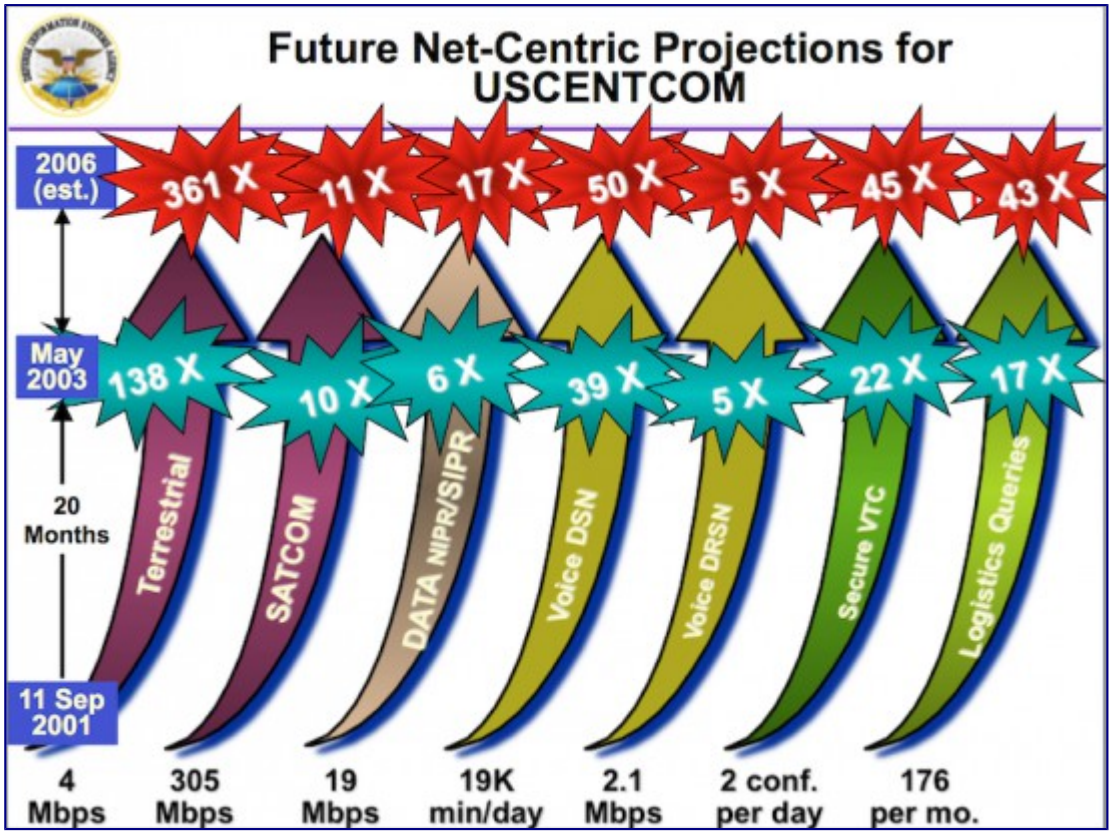
terror (GWOT). But, unprepared, the USA did not have enough bandwidth for such a plan. Houston, we have a problem…

Let's read what the Army has to say about that:

> *Upgrades since 9/11/01 have more than tripled the amount of DISN services bandwidth pre-positioned to support Warfighter STEP entries. (Jan 2003)*
>
> *Domain growth from 60 IDNX nodes to 213 nodes in 7 months (From October 2002- April 2003 – in the 2004 report : US DISA GWOT & OIF LESSONS LEARNED).*
>
> *BANDWIDTH FUELS TRANSFORMATIONAL WARFARE (Jan 2004)*
> *Finding: Strategic C4ISR requires high bandwidth to support today's net-centric warfare. Deployed forces are dependent upon bandwidth to disseminate large data and imagery files, conduct VTC's and collaborative planning with command personnel around the globe, and receive real-time intelligence information on the battlefield. Recent OEF/OIF/GWOT operations in the Central Region that were enabled by exponential increases in conventional bandwidth clearly demonstrated the value and feasibility of net-centric operations, but greater flexible response in providing bandwidth across all echelons of the GIG, especially at the tactical level, are needed in support of GWOT's current and probable missions.*
>
> *Context:*
>
> ***Current Military Satellite (MILSAT) constellation does not have the capability to provide sufficient bandwidth to support strategic C4ISR requirements. MILSAT only provided approximately 20% of the C4ISR bandwidth required in support of OEF/OIF/GWOT missions. The remaining 80% had to be acquired from commercial sources***.

Now, if your eyes bleeded over the design of the PRISM slides, here's more:





Dealing with a coalition in Iraq and Afghanistan proved to be difficult. For example when the USA had to give access to the Iridium :

> *From: Moriarty, Patrick Col*
> *Sent: Monday, March 31, 2003 6:20 AM*
> *To: Staton, Charles Col; Depalma, Evelyn; Sabin, Roger; Higgins, Frank COL;*

Lee, Gary COL; Fiedler, George Col; Bashore, John; Geist, Michael; 'Miller, Marcus Col (S)'
Cc: Ponturiero, Augustine J. LCDR; Reilly, Daniel Maj
Subject: FW: PROVISION OF SECURE EMSS (IRIDIUM) TO UK – LESSONS IDENTIFIED
All,
A couple of weeks ago, we (LCDR Ponturiero Wg Cdr Goslin) went through a goat rope trying to get Iridium handsets to the Brits. As Wg Cdr Ian Goslin points out, the success of making this happen was directly attributable to personalities and not processes. Ian believes we (DOD and DISA) need to take advantage of the valuable lessons learned in making this provisioning happen and establish a clear process with clear delineation of responsibilities so that ***the next time we need to provision to one of our coalition partners, we aren't as screwed up as « Hogan's Goat.****"*
Attached is Cdr Goslin's proposed solution, or starting point for a solution. As he states, « The key features of the new process need to address the areas that caused greatest difficulty in providing EMSS service to the UK i.e. a lack of a single US advocate for the request; no timely identification of who could/should authorize the request; unclear legal authority to provide the service; and difficulty in actually paying for the service. »

Operation Iraqi Freedom was soooo… well prepared. You've read about Turkey. Now read about « *spectrum management* » :

SPECTRUM MANAGEMENT IN A GWOT ENVIRONMENT
Findings: The Joint Spectrum Management Element (JSME) was stood up late in the planning process for Operation Iraqi Freedom (OIF). Stand up of the JSME must take place in the earliest phases of the OPLAN planning process. Trained spectrum managers are required at the component and JTF levels to functionally interact with adjacent and higher level spectrum managers. ***Radars used by maritime and land forces during OIF were not deconflicted amongst each other and resulted in unresolved Electromagnetic Interference (EMI).*** *During OIF CFLCC had to establish a complex numbering scheme in order to track frequencies as units moved through phase of the operation. Finally, Multi-emitter platforms:* ***AWACS, JSTARS, and Commando Solo were not completely cleared to operate in Host Nation (Turkey). The EMI was so severe that it affected the capability for shipboard radars to monitor the airspace for self-protection****.*
(US DISA GWOT & OIF LESSONS LEARNED) 2004 – Booz Allen Hamilton

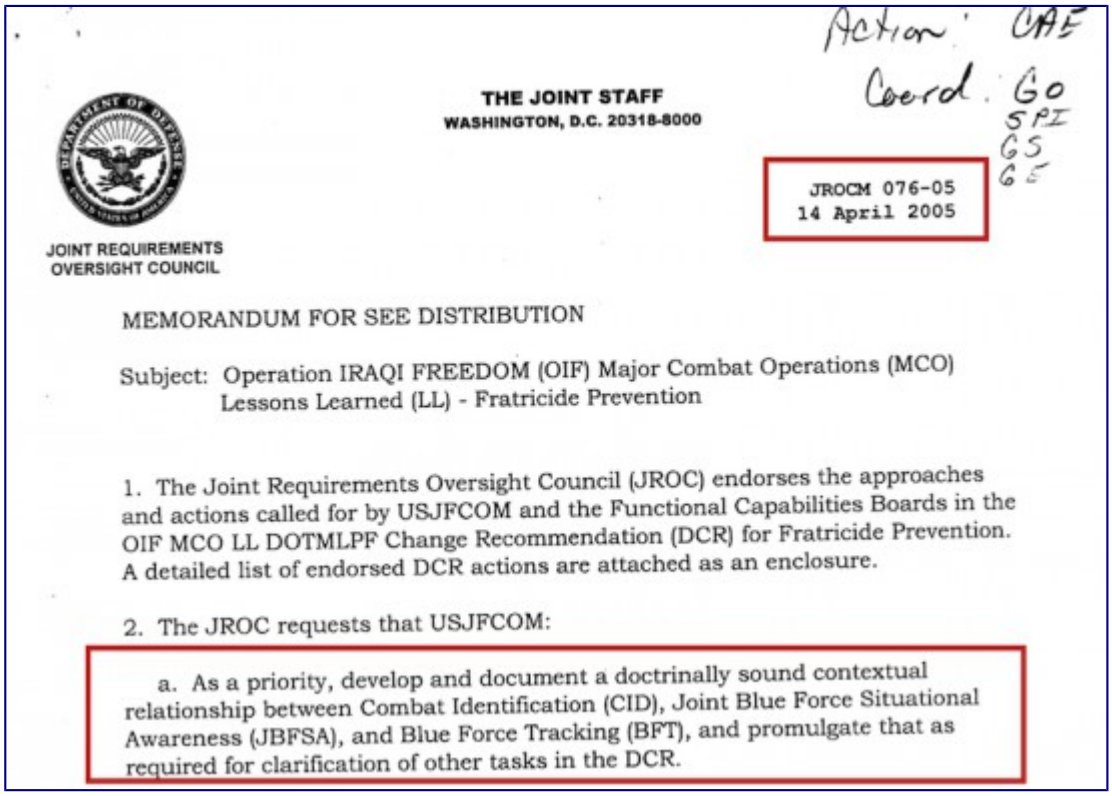
When it comes to sharing information and networks with other members of the Coalition… It's… Complicated. The USA is happy to get more men. It's OK if they get killed. But it's not OK to provide them with the same information given to the US « Warfighter ».

The warfighter (CENTCOM J3 and CENTAF) stated operational need to have instantaneous information sharing ***with certain carefully selected coalition partners***. This meant giving these partners physical access to particular workstations attached to the SIPRNET, and logical access from these workstations to a small number of key servers that are also attached to the SIPRNET.
This type of direct access by coalition partners to machines on U.S. Secret networks had never been done before.
Errors were made and some non-releasable data was posted and

shared even with all of the processes in place to prevent it. The real time policy monitoring capability was helpful in quickly and thoroughly cleaning up/resolving the spill.

Let's look further into theses documents… You may be too young to remember, but in the early stage of OEF, OIF, coalition members used to shoot each other. They called it « *Fratricide*« .

The US Army tried to act. Slowly.



Action: CAE
Coord: GO
SPI
GS
GE

THE JOINT STAFF
WASHINGTON, D.C. 20318-8000

JROCM 076-05
14 April 2005

JOINT REQUIREMENTS OVERSIGHT COUNCIL

MEMORANDUM FOR SEE DISTRIBUTION

Subject: Operation IRAQI FREEDOM (OIF) Major Combat Operations (MCO) Lessons Learned (LL) - Fratricide Prevention

1. The Joint Requirements Oversight Council (JROC) endorses the approaches and actions called for by USJFCOM and the Functional Capabilities Boards in the OIF MCO LL DOTMLPF Change Recommendation (DCR) for Fratricide Prevention. A detailed list of endorsed DCR actions are attached as an enclosure.

2. The JROC requests that USJFCOM:

a. As a priority, develop and document a doctrinally sound contextual relationship between Combat Identification (CID), Joint Blue Force Situational Awareness (JBFSA), and Blue Force Tracking (BFT), and promulgate that as required for clarification of other tasks in the DCR.

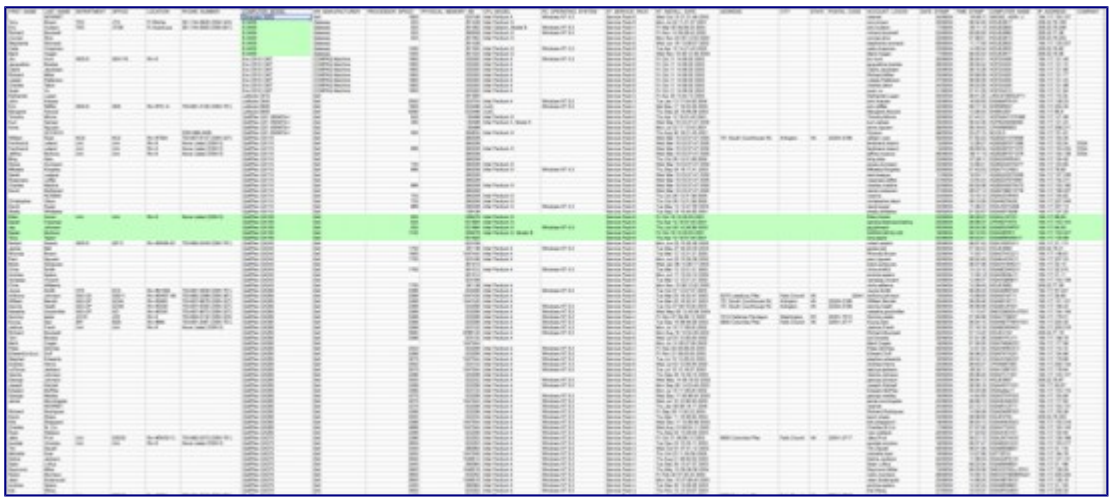
OIF started in 2003. The Joint Requirements Oversight Council Memorandum (JROCM) was issued on April 2005 and the actions would take place 12 or 24 month later. Like « *Analyse contributing causes of OEF and OIF MCO fratricide events* »…

Data leaks someone ?

Emails, logins, everything was in the wild. Use google and you'll find tons of them.

	A	B	C	D	E	F	G	H	I	J
1	Computer Name	Primary User	Organization	SMTP Address	Manufacturer	Computer Model	CPU Speed	Size MB	Total Memory	Operating System
2	DSC731	HILDENBJ	CONUS	SMTP:HildenbJ@scott.disa.smil.mil	Gateway	E-3400	933	38162	512	Microsoft Windows NT
3	DSC772	SCHULTER	CONUS	SMTP:SchulteR@scott.disa.smil.mil	Gateway	E-3400	933	38162	512	Microsoft Windows NT
4	DSC274	COXC	CONUS	SMTP:CoxC@scott.disa.smil.mil	Gateway	E-3400	933	38162	512	Microsoft Windows NT
5	DSC358	FAHSLJ	CONUS	SMTP:FahsLJ@scott.disa.smil.mil	Gateway	E-3400	933	38162	512	Microsoft Windows NT
6	DSC081	OTTINGEP	CONUS	SMTP:OttingeP@scott.disa.smil.mil	Gateway	E-3400	933	38162	512	Microsoft Windows NT
7	DSC367	SIEGEL1J	CONUS	SMTP:Siegel1J@scott.disa.smil.mil	Gateway	E-3400	933	38162	512	Microsoft Windows NT
8	DSC087	PAUKENM	CONUS	SMTP:PaukenM@scott.disa.smil.mil	Gateway	E-3400	933	38162	256	Microsoft Windows NT
9	DSC365	ALMGRENG	CONUS	SMTP:AlmgrenG@scott.disa.smil.mil	Gateway	E-3400	933	3815	512	Microsoft Windows NT
10	DSC365	ALMGRENG	CONUS	SMTP:AlmgrenG@scott.disa.smil.mil	Gateway	E-3400	933	3815	512	Microsoft Windows NT
11	DSC216	GREENZO	CONUS	SMTP:GreenZO@scott.disa.smil.mil	Gateway	E-3400	933	38162	512	Microsoft Windows NT
12	DSC366	FIKEE	CONUS	SMTP:FikeE@scott.disa.smil.mil	Gateway	E-4200	500	3079	128	Microsoft Windows NT
13	DSC360	DINTELMC	CONUS	SMTP:DintelmC@scott.disa.smil.mil	Gateway	E-4200	700	28623	384	Microsoft Windows NT
14	DSC148	HUNDM	CONUS	SMTP:HundM@scott.disa.smil.mil	Gateway	E-4200	700	9758	384	Microsoft Windows NT
15	DSC175	KOENENB	CONUS	SMTP:KoenenB@scott.disa.smil.mil	Gateway	E-4200	700	19694	384	Microsoft Windows NT
16	DSC374	BATES2C	CONUS	SMTP:Bates2C@scott.disa.smil.mil	Gateway	E-4200	700	12158	384	Microsoft Windows NT
17	DSC047	FARMERR	CONUS	SMTP:FarmerR@ncr.disa.smil.mil	Gateway	E-4400	866	38162	512	Microsoft Windows NT
18	DSC410	BAKARICS	CONUS	SMTP:BakaricS@scott.disa.smil.mil	Gateway	E-4400	866	38162	512	Microsoft Windows NT
19	DSC039	HIBBERTJ	CONUS	SMTP:HibbertJ@ncr.disa.smil.mil	Gateway	E-4400	866	38162	512	Microsoft Windows NT
20	DSC720	ROGERSL	CONUS	Unknown	Gateway	E-4400	866	38162	512	Microsoft Windows NT
21	PNTS72066C	GARNETTA	CONUS	SMTP:GarnettA@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	866	19069	256	Microsoft Windows NT
22	DSC239	HEFFRONM	CONUS	SMTP:HeffronM@scott.disa.smil.mil	Gateway		400	12409	384	Microsoft Windows NT
23	DSC699	PATTONT	CONUS	SMTP:PattonT@scott.disa.smil.mil	Gateway		500	38162	384	Microsoft Windows NT
24	DISA-C-N067089	WALKER3R	CSD	SMTP:Walker3R@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 500MTbr+	500	9758	128	Microsoft Windows NT
25	UMDMJ1	MCGRUDEJ	CSD	SMTP:HawkinsJ@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX150	933	19069	254	Microsoft Windows NT
26	DISAGQNM301	MIHELCID	CTO	SMTP:MihelcID@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	14323	256	Microsoft Windows NT
27	N068087	PERRASB	DO	SMTP:RileyD@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 600MTbr+	600	9758	256	Microsoft Windows NT
28	HDF596Z101	MEHLW	DSO	SMTP:MehlW@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	866	38148	512	Microsoft Windows NT
29	HDF2LFLS01	TAKEGUCE	DSO	SMTP:TakegucE@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX150	933	38162	510	Microsoft Windows NT
30	DISAC-FPHGZ	VANDEVED	ECSO-J2	SMTP:VandeVeD@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 600MTbr+	600	38162	256	Microsoft Windows NT
31	LNCPXBEL5Z-C	DORMANR	GE5	SMTP:KellerB@ncr.disa.smil.mil	Dell Computer Corporation	Latitude CPx J650GT	650	11507	128	Microsoft Windows 2000
32	CPKNG45626	SPIELERL	GES-E	SMTP:SpielerL@ncr.disa.smil.mil	DELL	Data not accessible	233	4110	64	Microsoft Windows NT
33	DSC036	SMITH3R	GES-E	SMTP:Smith3R@scott.disa.smil.mil	Gateway	E-4400	866	38162	512	Microsoft Windows NT
34	DISA-C-0016	CUNNINGD	GES-E	SMTP:CunningD@ncr.disa.smil.mil	Micron Electronics, Inc.	Millennia/Client Pro	333	8008	128	Microsoft Windows NT
35	DISA-C-0004	ARATAP	GES-E	SMTP:ArataP@ncr.disa.smil.mil	Not Found	Not Found	300	8008	96	Microsoft Windows NT
36	DISAN059752	SCHOOTJ	GES-E	SMTP:SchootJ@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 266MTbr	266	6181	320	Microsoft Windows NT
37	DISC-C-GB4DY	RURAKS	GES-E	SMTP:RurakS@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 400MTbr+	400	19694	192	Microsoft Windows NT
38	DISA-C-483EL	DENNIS2M	GES-E	SMTP:DennisM@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 600MTbr+	600	4102	256	Microsoft Windows NT
39	DISA-C-33ACZ	JAINP	GES-E	SMTP:JainP@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 600MTbr+	600	12982	256	Microsoft Windows NT
40	DN011	BUB	GES-E	SMTP:BuB@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	667	14590	128	Microsoft Windows 2000
41	CONDO110GW3Y30B	YOUNGC	GES-E	SMTP:YoungC@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	667	14323	256	Microsoft Windows 2000
42	CPKN100866	MORRISSC	GES-E	SMTP:MorrisC@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	667	14323	128	Microsoft Windows NT
43	CDNDG110GVCN10B	HUNTERE	GES-E	SMTP:HunterE@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	667	14323	256	Microsoft Windows 2000
44	CDNDG110YT230B	LEK	GES-E	SMTP:LeK@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	667	14323	256	Microsoft Windows 2000
45	CDNDG110220X101	JUY	GES-E	SMTP:JuY@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	14590	256	Microsoft Windows 2000
46	DISC-C-N054657	THOMSW	GES-E	SMTP:ThomsW@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	6181	256	Microsoft Windows NT
47	DISC-C-N054657	THOMSW	GES-E	SMTP:ThomsW@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	6181	256	Microsoft Windows NT
48	DISA-C-j2tz30B	WILLIA3R	GES-E	SMTP:Willa3R@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	14323	128	Microsoft Windows NT
49	DISA-C-JTZ30B	QUIROZR	GES-E	Unknown	Dell Computer Corporation	OptiPlex GX110	733	14323	128	Microsoft Windows NT
50	CDNDG110027Z30B	FLIOSP	GES-E	Unknown	Dell Computer Corporation	OptiPlex GX110	733	14323	128	Microsoft Windows 2000
51	DNDG0103RZJ101	MEANSD	GES-E	SMTP:MeansD@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	14323	256	Microsoft Windows 2000
52	CDNDG110Y3X101	JONES3B	GES-E	SMTP:Jones3B@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	14590	256	Microsoft Windows 2000
53	CDNDGX110HN3X10	WHITMANJ	GES-E	SMTP:WhitmanJ@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	14590	256	Microsoft Windows 2000
54	DISA-C-DYBZC	TANAKAR	GES-E	SMTP:TanakaR@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	4118	128	Microsoft Windows NT
55	DNDG110H4DJD1	HELSELJ	GES-E	SMTP:HelselJ@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	866	19092	128	Microsoft Windows 2000
56	CDNDG110W6JD1	LAMANNAT	GES-E	SMTP:LaMannaT@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	866	19069	256	Microsoft Windows 2000
57	DISA-C-850VJD1	CUCER	GES-E	SMTP:CuceR@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	866	19092	256	Microsoft Windows NT
58	CPKN076052	ROGERSW	GES-E	SMTP:RogersW@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	933	38162	256	Microsoft Windows NT
59	CPKN076860	VITALEJ	GES-E	SMTP:BanksT@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	933	38146	256	Microsoft Windows NT
60	DISA-C-FW4SV01	RANDLER	GES-E	SMTP:RandleR@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX150	933	19069	254	Microsoft Windows NT
61	DISA-C-097YHN	HOPKINSC	GES-E	SMTP:HopkinsC@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX150	933	19069	254	Microsoft Windows NT
62	CDNDO150378GP01	MAIP	GES-E	SMTP:MaiP@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX150	933	38162	254	Microsoft Windows 2000
63	DISA-C-N060210	BENNETTD	GES-E	SMTP:BennetD@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX150	933	19069	254	Microsoft Windows NT
64	DISCEHQCR	PERRYK	GES-E	SMTP:PerryK@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GXa 233MTbr EM	233	4118	128	Microsoft Windows NT
65	DISC-C-N054660	SMITHT	GES-E	SMTP:SmithT@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GXa 233MTbr EM	233	19469	192	Microsoft Windows NT
66	DISC-C-EFHS3	LAMANNAT	GES-E	SMTP:LaMannaT@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GXa 233MTbr EM	233	4118	64	Microsoft Windows NT
67	DISA-C-DTLVH	REEDAW	GES-E	SMTP:ReedAw@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GXa 233MTbr EM	233	19694	128	Microsoft Windows NT
68	DISC-C-N052925	DEESB	GES-E	Unknown	Dell Computer Corporation	OptiPlex GXa 233MTbr EM	233	4118	192	Microsoft Windows NT
69	DISA-CN053900	RAMEYT	GES-E	SMTP:ColeS@ncr.disa.smil.mil	System Manufacturer	System Name	233	4337	320	Microsoft Windows NT
70	DISA-C-N075137	FEGLEYM	GES-E	SMTP:FegleyM@ncr.disa.smil.mil	System Manufacturer	System Name	500	19539	512	Microsoft Windows NT
71	CPKNO67734	HILLJ	GES-E	SMTP:YoungC@ncr.disa.smil.mil	Dell Computer Corporation	XPST600	600	9726	128	Microsoft Windows NT
72	DISA-C-N075128	JOK	GES-E	Unknown	Dell Computer Corporation	XPS-Z	866	38162	128	Microsoft Windows NT
73	DSC261	RUMPLERP	GIG-BE	SMTP:RumplerP@scott.disa.smil.mil	Gateway	E-4400	866	38162	512	Microsoft Windows NT
74	DISA-C-N054235	BROWNJJ	GIG-BE	SMTP:BrownJJ@ncr.disa.smil.mil	Not Found	Not Found	200	4102	64	Microsoft Windows NT
75	DISA-C-HX18D	MCFADDEA	GIG-BE	SMTP:McFaddeA@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX1 500MTbr+	700	38162	256	Microsoft Windows NT
76	DISA8HDQ401	BROWNJJ	GIG-BE	SMTP:LongC@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX110	733	14323	256	Microsoft Windows NT
77	CDNDO150FVTJT01	CURCIOA	GIG-BE	SMTP:EvansJN@ncr.disa.smil.mil	Dell Computer Corporation	OptiPlex GX150	933	38162	254	Microsoft Windows 2000

Phone numbers, IP addresses… What else ?



Don’t fool yourselves, they know what is going on :

SUBJECT: Trends in Pentagon/NCR Facility Security Violations

When US troops are battling terrorism abroad and the Pentagon itself is a prime target for hostile intelligence, we in OSD have a special responsibility to protect sensitive information of all types. The Secretary and I are thus very concerned over recent data compiled by the Pentagon Force Protection Agency, which indicate that we in OSD are clearly headed for a new high this year in security violations in Pentagon/NCR facilities.

What the data shows is that 93% of our violations resulted from poor physical security, unsafe transmission practices, or improper handling and control of classified items. These violations reach across all levels of OSD, from junior to very senior.

Such violations do not just happen. The first two result largely from carelessness, and the third from lack of knowledge. A contributing factor to all three is over-tasking by supervisors that might suggest that security procedures can be selectively curtailed.

It’s somehow reassuring to see that even if they can tap the whole backbones, get into Google’s and Facebook’s databases, the US Army and the Agencies still have « problems ». Huge ones.