Cyber Warfare Command and Control

Dr. Norm Howes, Institute for Defense Analyses
howes@ida.org

Dr. Mike Mezzino, Univ. of Houston-Clear Lake
mezzino@cl.uh.edu

John Sarkesain, Missile Defense Agency
john.sarkesain@mda.osd.mil

15 June 04

Briefing at a Glance

- Current Cyber Defense Issues
- Solutions Concepts and Approach
- *CyberC2* Architecture
- A Look Inside *CyberC2*
- Questions and Discussion

Current Cyber Defense Issues

- **Organizational Issues**
  - Kinetic warfare C2 organization structure inappropriate for cyber warfare
    - Cyber warfare attacks measured in seconds whereas Kinetic warfare attacks measured in hours to days
    - Hierarchical structure with periodic reporting introduces delays
    - Limitation of being a member of only one cell at a time
  - Static model does not allow adaptation to the dynamics of the situation
- **Operational Issues**
  - No tradition of strategy and tactics in cyber warfare
    - One-sided battle where attacker strikes all the blows and defender responds so slowly that the attacker often gets away unknown
  - Little appreciation of the value of deception and maneuver in cyber warfare
  - No overall concept of cyber command and control to guide responses
  - Over reliance on security devices that are only partially effective
  - Not using output of security devices to respond effectively to attacks

Current Cyber Defense Issues (continued)

- **Technical Issues**
  - Cyber warfare C2 systems do not yet exist even though technologies exist to enable them and benefit cyber defense
    - Dynamic virtual cells
    - Mobile agent patrols
    - Dynamic reconfiguration
    - IP address hopping
    - Real-time collaboration tools
  - Beneficial cyber defense technologies are not widely used
    - Vendors do not yet see a potential market for these technologies
    - Cyber defense systems do not yet demand them
    - Network operations personnel do not understand how to use them

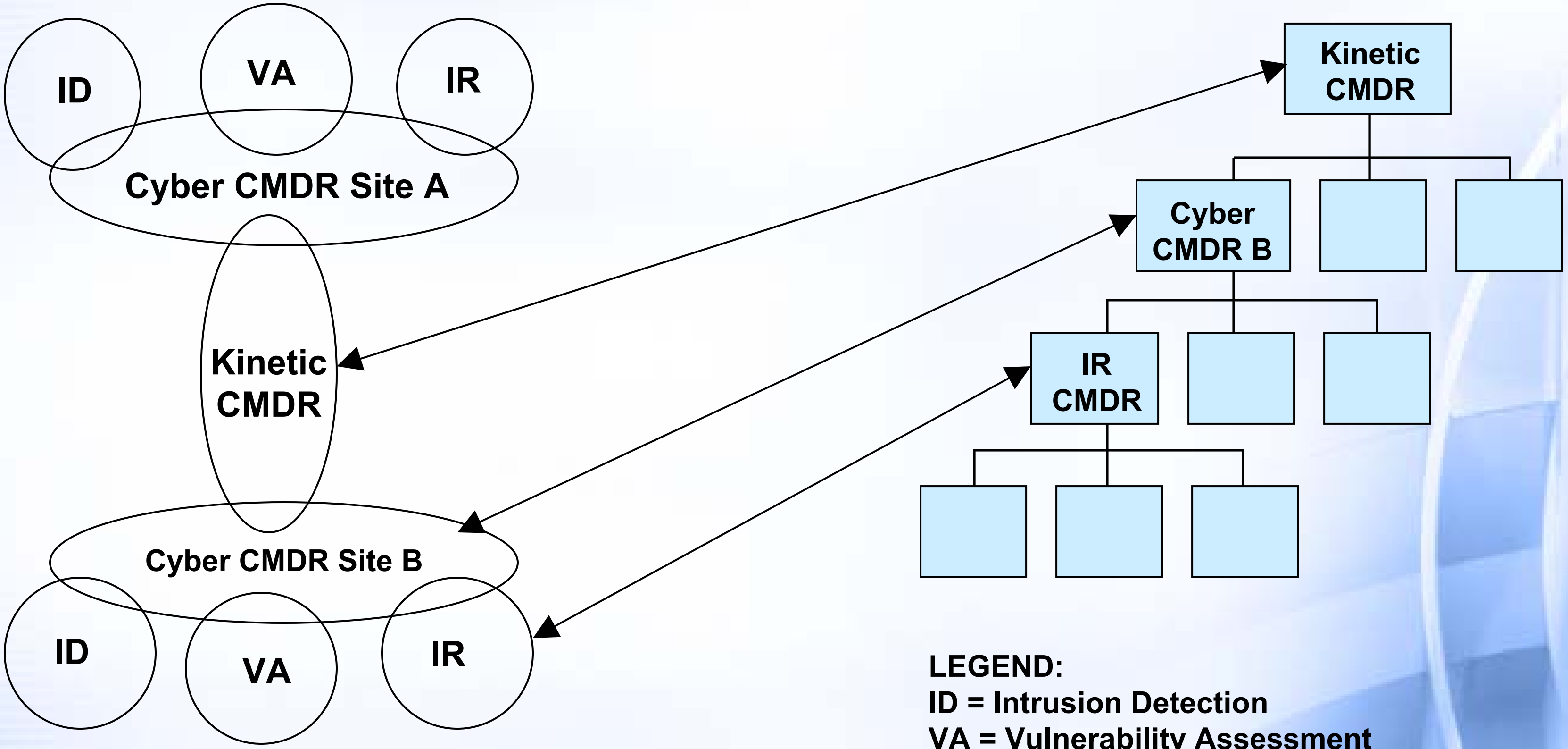
Organizational Solution

- Virtual Cell organizational model
  - More flexible than physical cells in a command center
    - Supports individuals belonging to multiple cells simultaneously
    - Dynamic joining of cells to bring in remote commanders or specialists
  - Dynamic creation, relocation, and decommissioning of virtual cells
    - Makes cells harder to attack
    - Makes cells much more fault-tolerant

Virtual Cells vs. Physical Cells

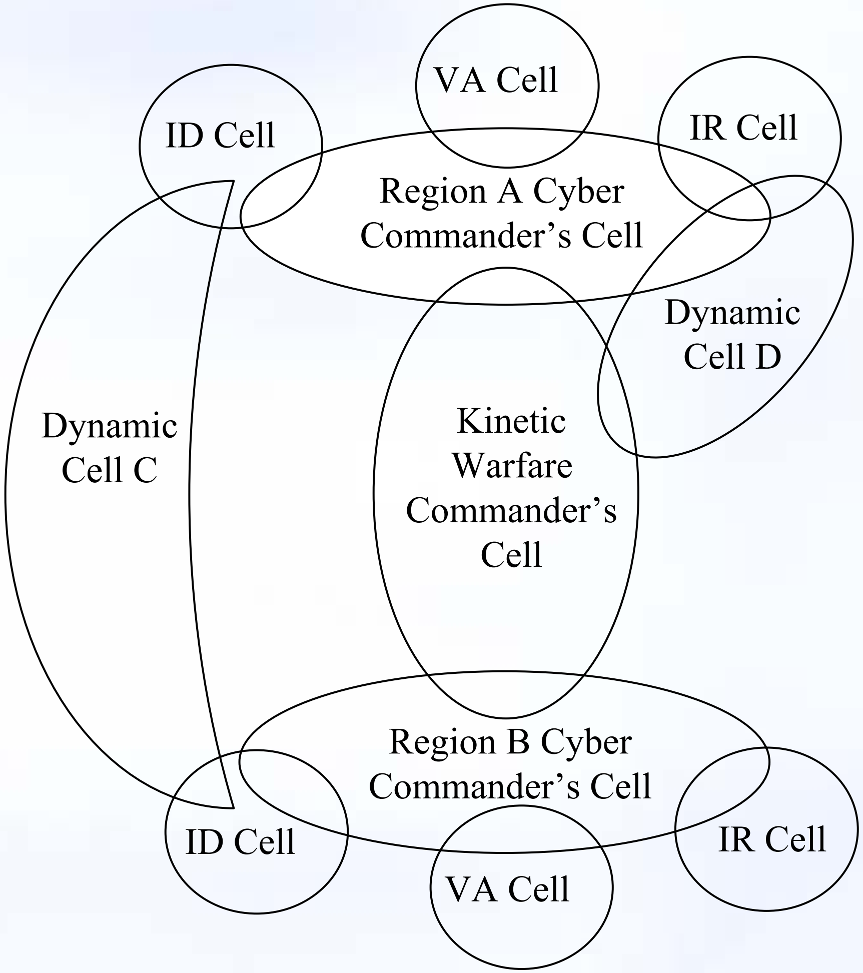
Characterized by:
- Membership relationship
- Peer-to-peer structure

Characterized by:
- Reports to relationship
- Hierarchical structure



LEGEND:
ID = Intrusion Detection
VA = Vulnerability Assessment
IR = Intrusion Response
FOG = Front Office Group

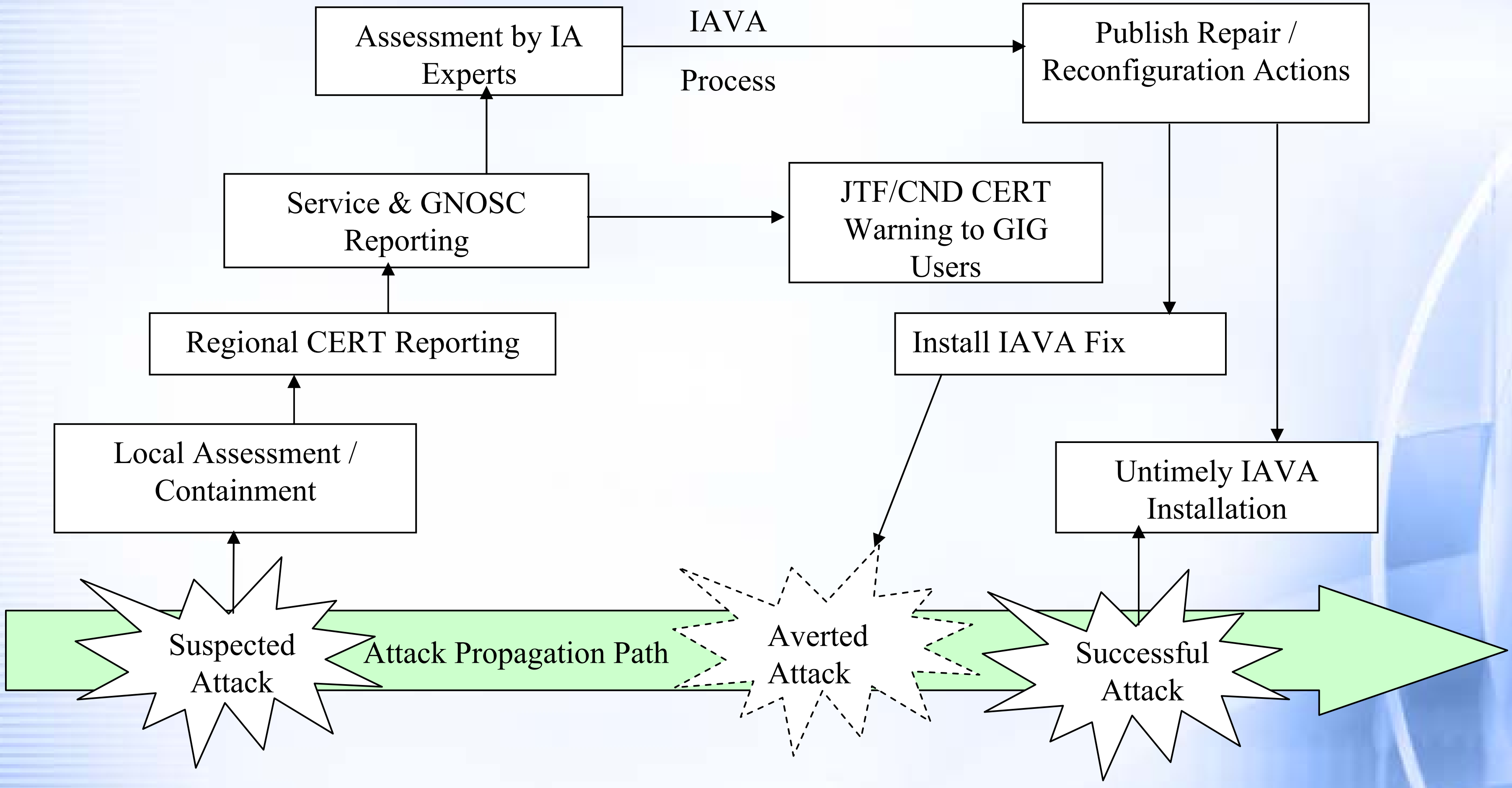
Dynamic Cells vs. Core Cells


VA Cell
ID Cell
IR Cell
Region A Cyber Commander's Cell
Dynamic Cell D
Dynamic Cell C
Kinetic Warfare Commander's Cell
Region B Cyber Commander's Cell
ID Cell
IR Cell
VA Cell

Operational Solution

- **IA CONOPS**
  - Based on virtual cell organization
  - Promotes uses of deception and maneuver
    - Dynamic system reconfiguration / Honeynets
    - Mobile agent patrols
    - Secure publish and subscribe communications
  - Supports situation awareness
    - Enterprise Network Display (common cyber operational picture)
    - Cyber Order of Battle Display
    - Attack Status Display
    - Vulnerability Status Display
  - Supports Course of Action (COA) formulation, execution, and tracking
  - Integrated Simulations and war gaming tools
  - Anticipatory (rather than reactive) architecture
  - Integrated Operations, Testing, and Training

Current Intrusion Detection & Response Process



Assessment by IA Experts

IAVA

Process

Publish Repair / Reconfiguration Actions

Service & GNOSC Reporting

JTF/CND CERT Warning to GIG Users

Regional CERT Reporting

Install IAVA Fix

Local Assessment / Containment

Untimely IAVA Installation

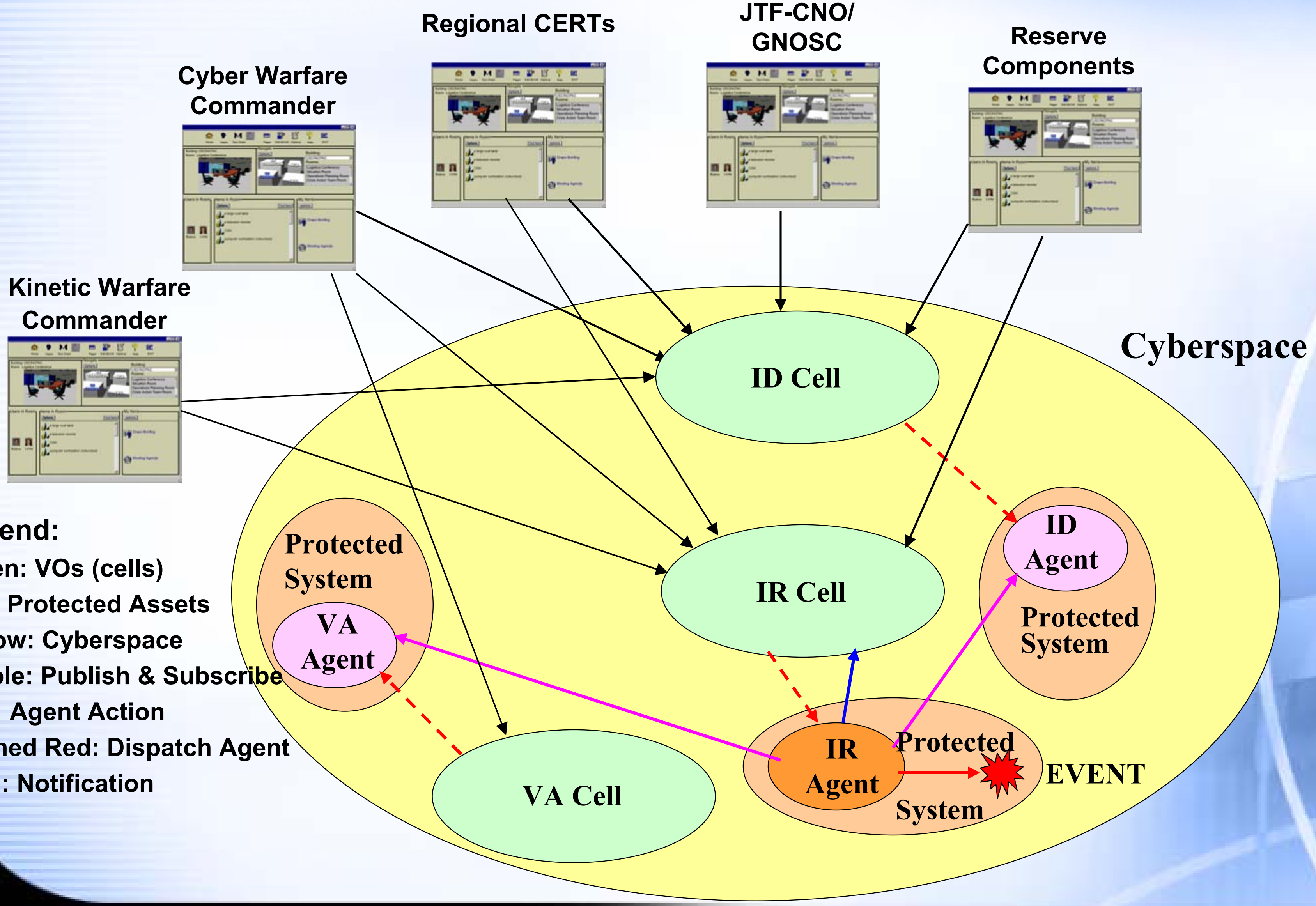
Suspected Attack

Attack Propagation Path

Averted Attack

Successful Attack

CyberC^2 Operational Model



Legend:

Green: VOs (cells)

Tan: Protected Assets

Yellow: Cyberspace

Purple: Publish & Subscribe

Red: Agent Action

Dashed Red: Dispatch Agent

Blue: Notification

Technical Solution

- Use the strategy of dynamic real-time collaboration to enhance coordination of cyber knowledge and maintain cyber situational awareness

- Use the tactic of maneuver by employing dynamic logical reconfiguration to keep virtual cells and critical processes on the move

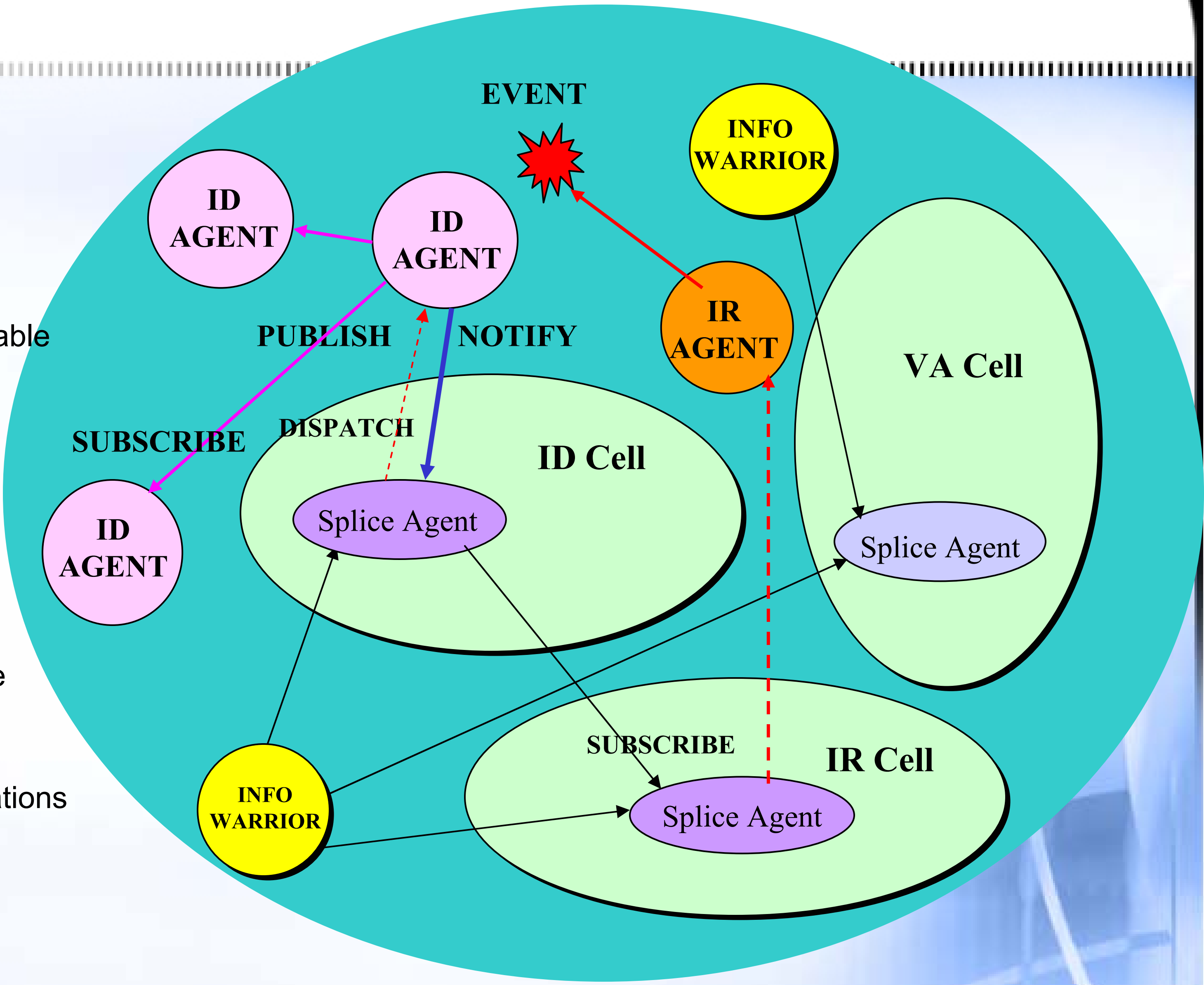
- Use the tactic of deception by employing IP address hopping to continually show potential attackers a different logical architecture

- Use the tactic of maneuver by employing mobile agent patrols to seek out constantly changing vulnerabilities and intruding processes

- Use deception by shepherding intruders into honeynets to observe their strategy and tactics

CyberC^2 SYSTEM MODEL

- Java
  - Security model
  - Agents
  - Exchange executable content
- Splice
  - Publish
  - Subscribe
  - Shared dataspace
  - Persistent
  - Agent dispatching
  - Agent communications

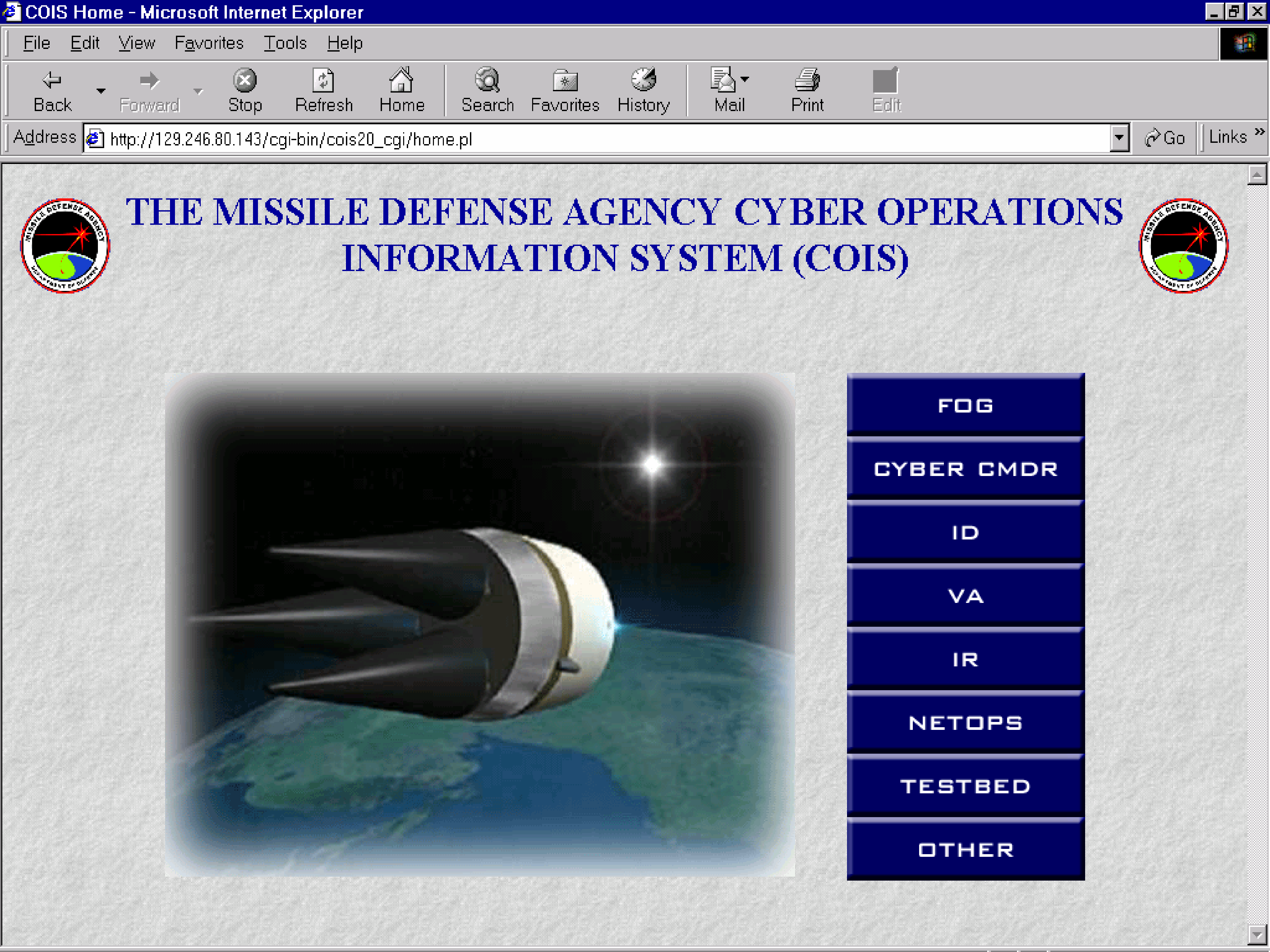


Working Group History

- Requirements Working Group (RWG)
  - Established April 2002
  - Members from MDA, NSWC, IDA, SEI, CSC, Sparta
- Architectural Working Group (AWG)
  - Established March 2003
  - Members from MDA, IDA, SEI, CSC, QI, Univ. Houston

CyberC² Status June 04

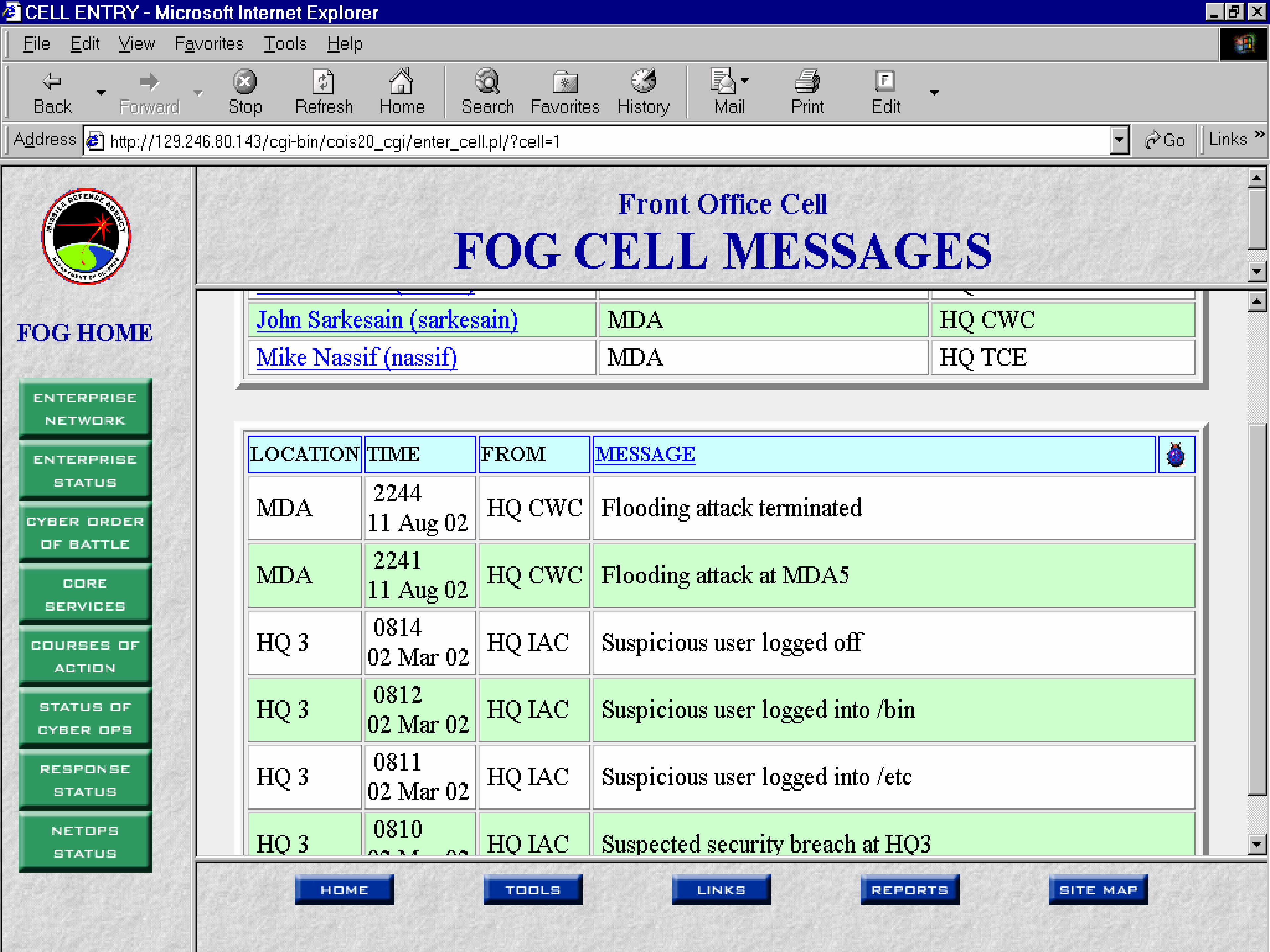
- Completed documents:
  - ***Information Assurance Operations Center (IAOC) CONOPS***
  - ***Cyber Operations Information System (COIS) Users Manual***
- In development:
  - ***IA/CND Concept of Operations (CONOPS)***
  - ***CyberC² Users Manual***
  - Prototype *CyberC²* tool-set (Version 3 for Linux and Windows delivered 4/05/04)
- *CyberC²* during 2004:
  - Testbeds operational at IDA and Houston sites
  - Work on secure high performance publish and subscribe messaging infrastructure underway



COIS Home - Microsoft Internet Explorer

Address http://129.246.80.143/cgi-bin/cois20_cgi/home.pl

THE MISSILE DEFENSE AGENCY CYBER OPERATIONS INFORMATION SYSTEM (COIS)

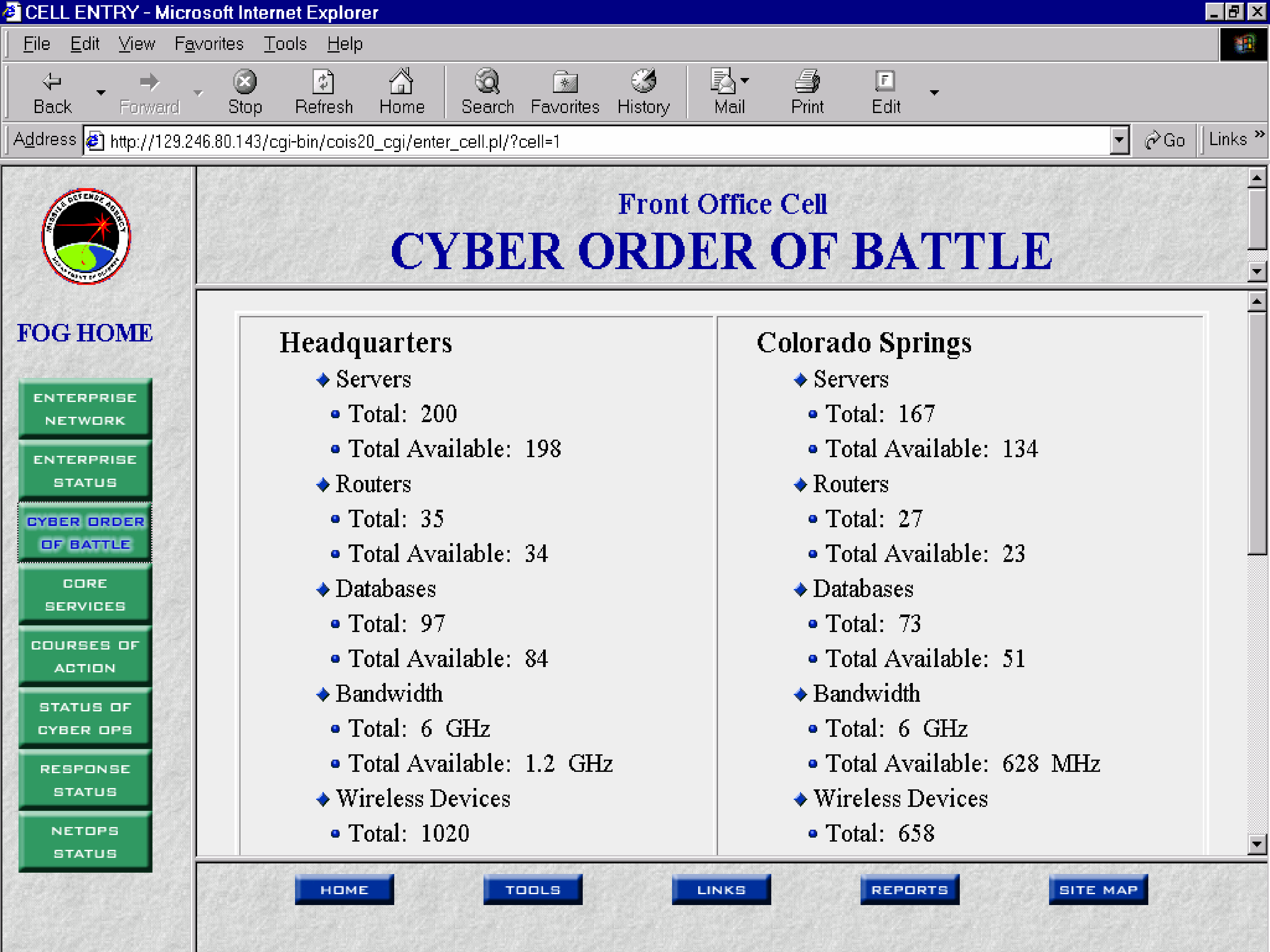


Front Office Cell

FOG CELL MESSAGES

John Sarkesain (sarkesain)	MDA	HQ CWC
Mike Nassif (nassif)	MDA	HQ TCE

LOCATION	TIME	FROM	MESSAGE
MDA	2244 11 Aug 02	HQ CWC	Flooding attack terminated
MDA	2241 11 Aug 02	HQ CWC	Flooding attack at MDA5
HQ 3	0814 02 Mar 02	HQ IAC	Suspicious user logged off
HQ 3	0812 02 Mar 02	HQ IAC	Suspicious user logged into /bin
HQ 3	0811 02 Mar 02	HQ IAC	Suspicious user logged into /etc
HQ 3	0810	HQ IAC	Suspected security breach at HQ3



Address http://129.246.80.143/cgi-bin/cois20_cgi/enter_cell.pl/?cell=1

Front Office Cell

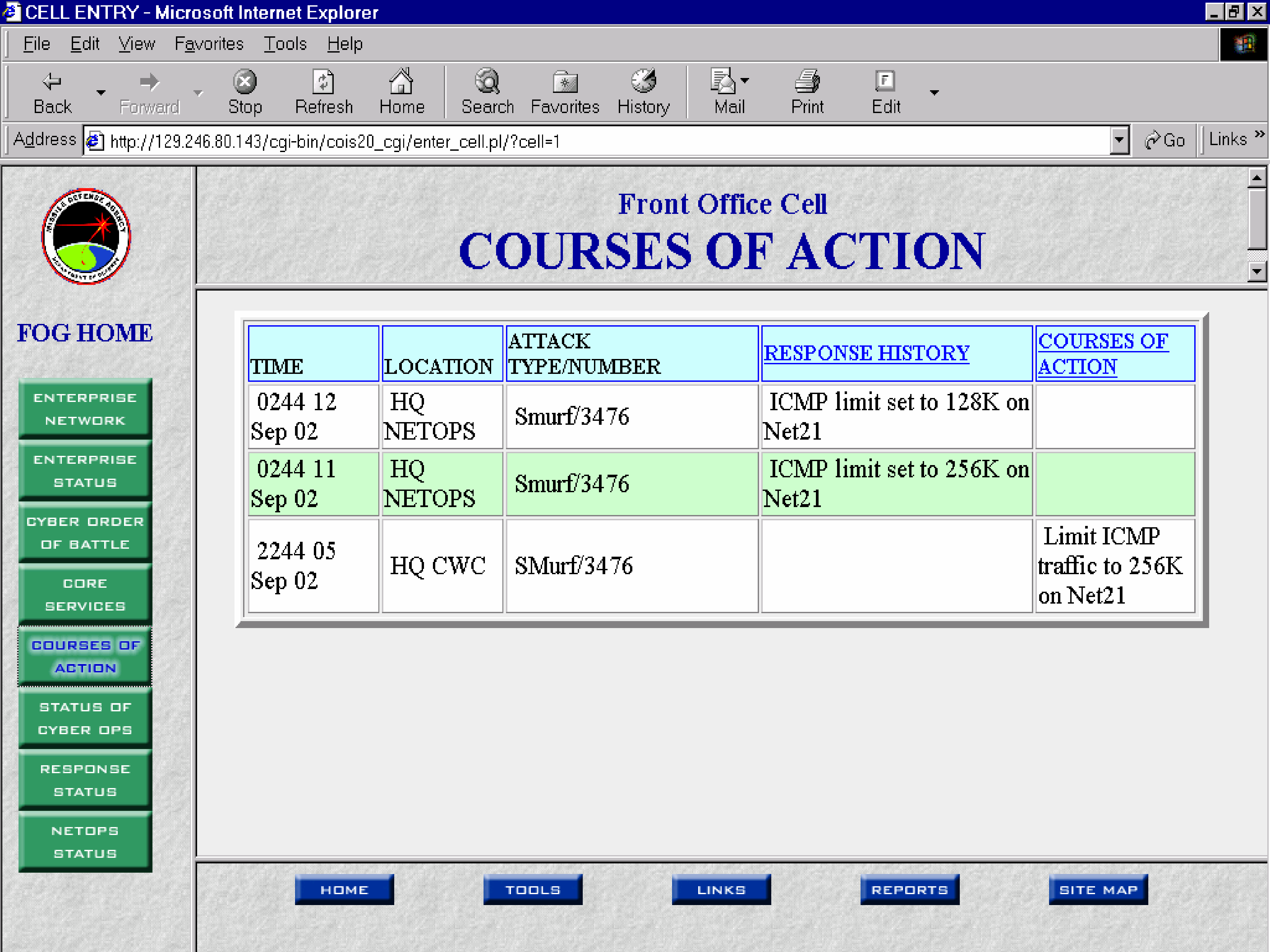
CYBER ORDER OF BATTLE

Headquarters

- Servers
  - Total: 200
  - Total Available: 198
- Routers
  - Total: 35
  - Total Available: 34
- Databases
  - Total: 97
  - Total Available: 84
- Bandwidth
  - Total: 6 GHz
  - Total Available: 1.2 GHz
- Wireless Devices
  - Total: 1020

Colorado Springs

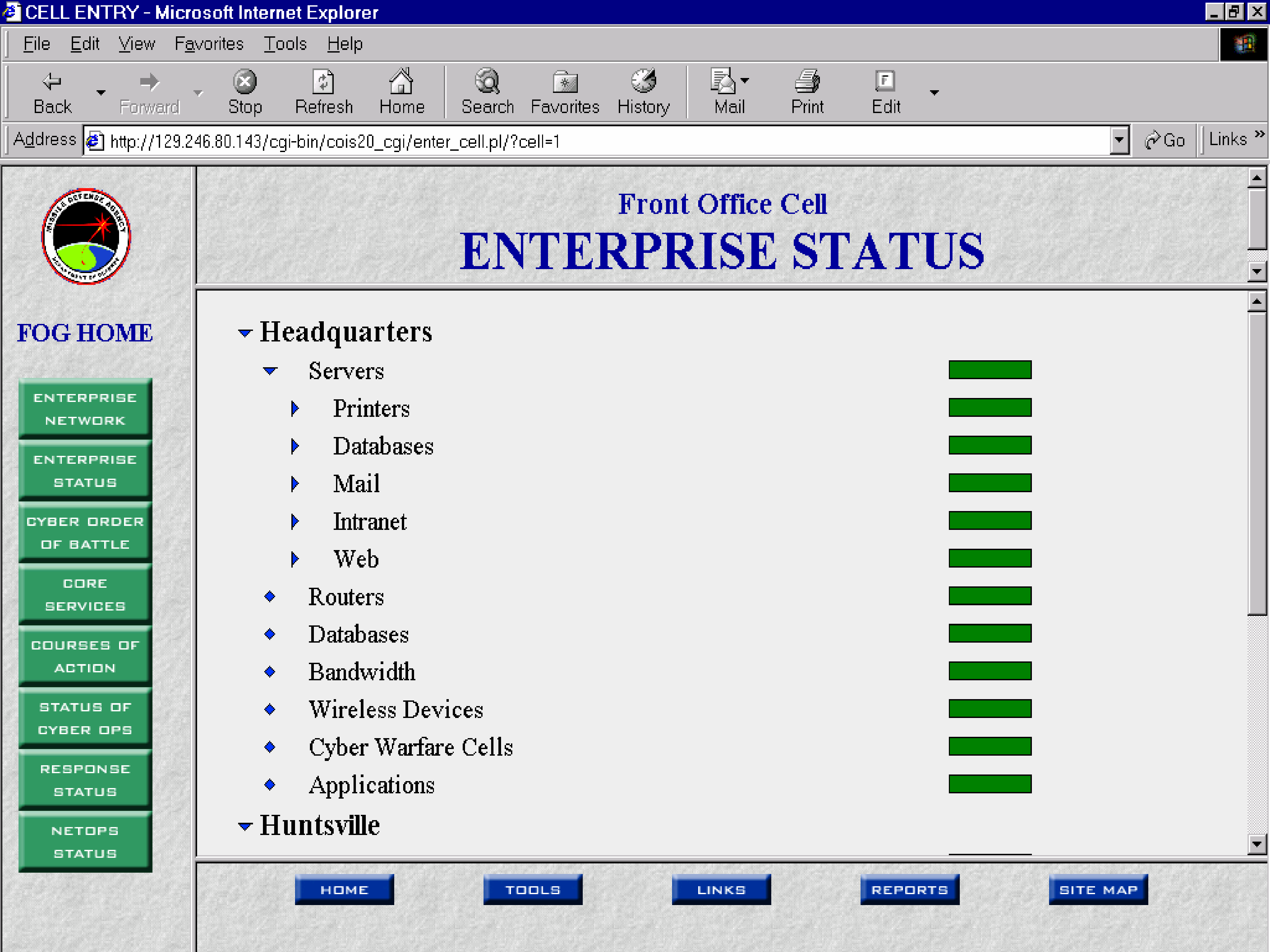
- Servers
  - Total: 167
  - Total Available: 134
- Routers
  - Total: 27
  - Total Available: 23
- Databases
  - Total: 73
  - Total Available: 51
- Bandwidth
  - Total: 6 GHz
  - Total Available: 628 MHz
- Wireless Devices
  - Total: 658



Front Office Cell

COURSES OF ACTION

TIME	LOCATION	ATTACK TYPE/NUMBER	RESPONSE HISTORY	COURSES OF ACTION
0244 12 Sep 02	HQ NETOPS	Smurf/3476	ICMP limit set to 128K on Net21	
0244 11 Sep 02	HQ NETOPS	Smurf/3476	ICMP limit set to 256K on Net21	
2244 05 Sep 02	HQ CWC	SMurf/3476		Limit ICMP traffic to 256K on Net21



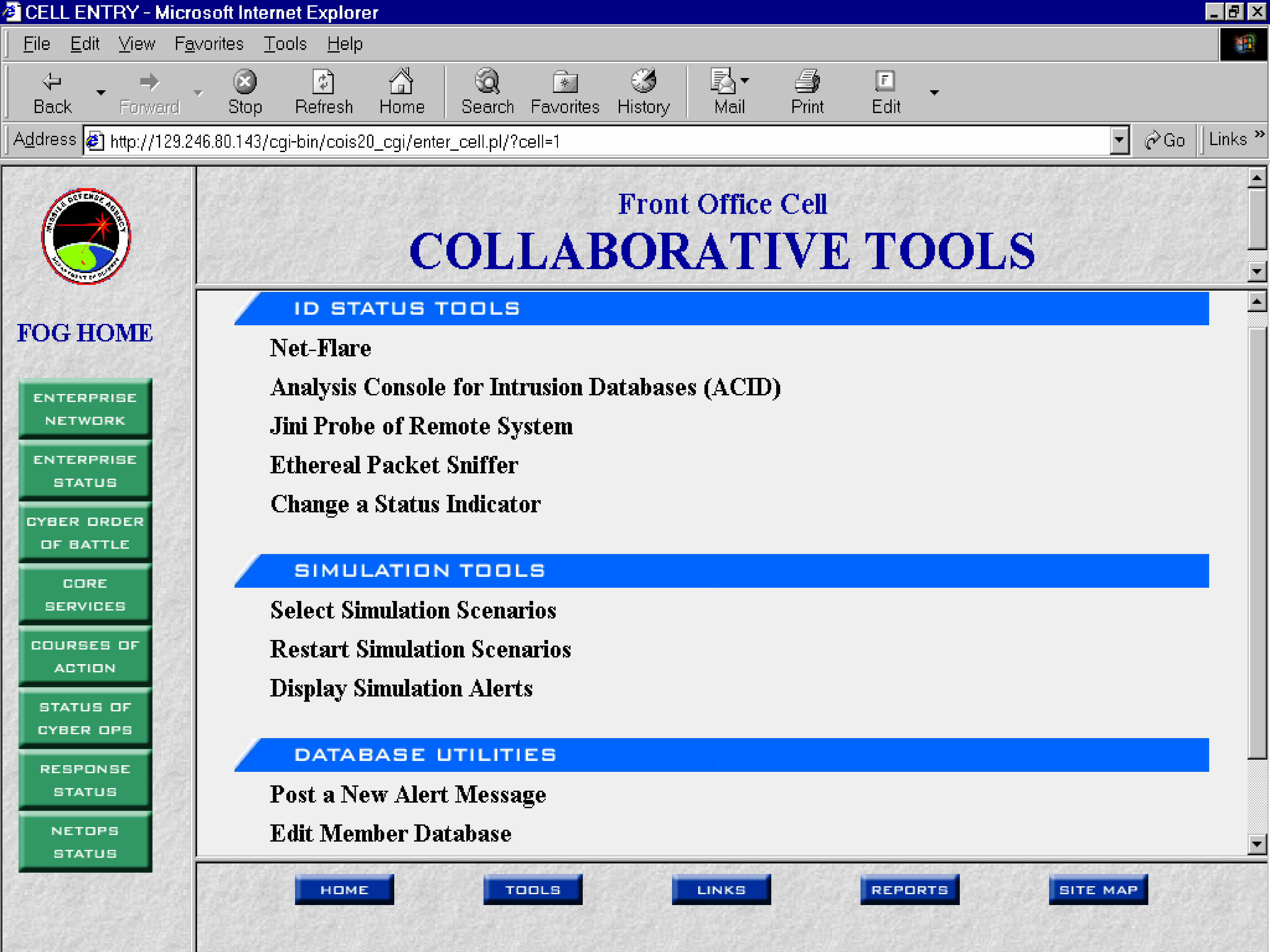
CELL ENTRY - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Address
Go
Links

http://129.246.80.143/cgi-bin/cois20_cgi/enter_cell.pl/?cell=1

Front Office Cell

ENTERPRISE STATUS

- Headquarters
  - Servers 🟩
    - Printers 🟩
    - Databases 🟩
    - Mail 🟩
    - Intranet 🟩
    - Web 🟩
  - Routers 🟩
  - Databases 🟩
  - Bandwidth 🟩
  - Wireless Devices 🟩
  - Cyber Warfare Cells 🟩
  - Applications 🟩
- Huntsville



Front Office Cell

COLLABORATIVE TOOLS

ID STATUS TOOLS

Net-Flare

Analysis Console for Intrusion Databases (ACID)

Jini Probe of Remote System

Ethereal Packet Sniffer

Change a Status Indicator

SIMULATION TOOLS

Select Simulation Scenarios

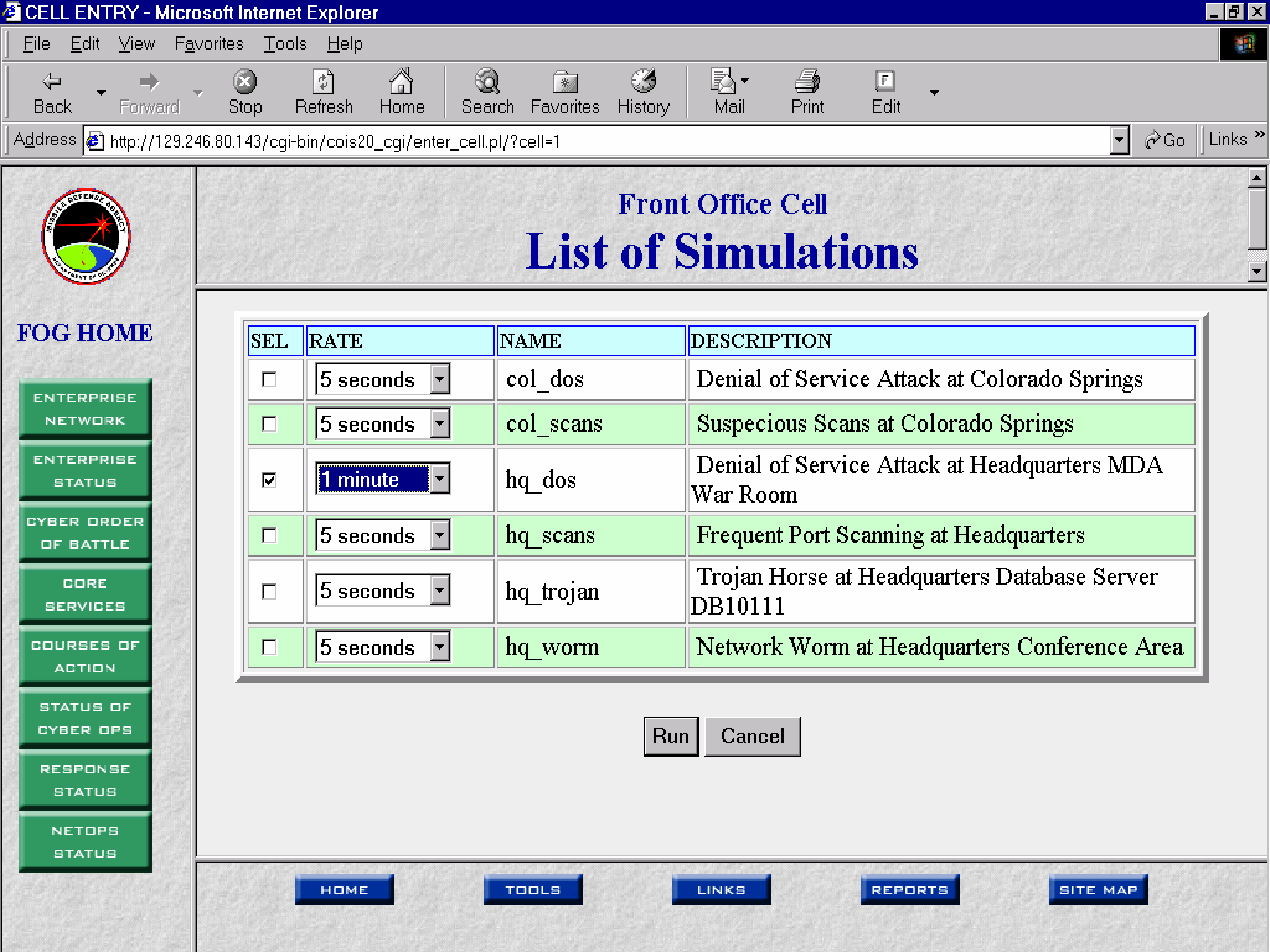
Restart Simulation Scenarios

Display Simulation Alerts

DATABASE UTILITIES

Post a New Alert Message

Edit Member Database

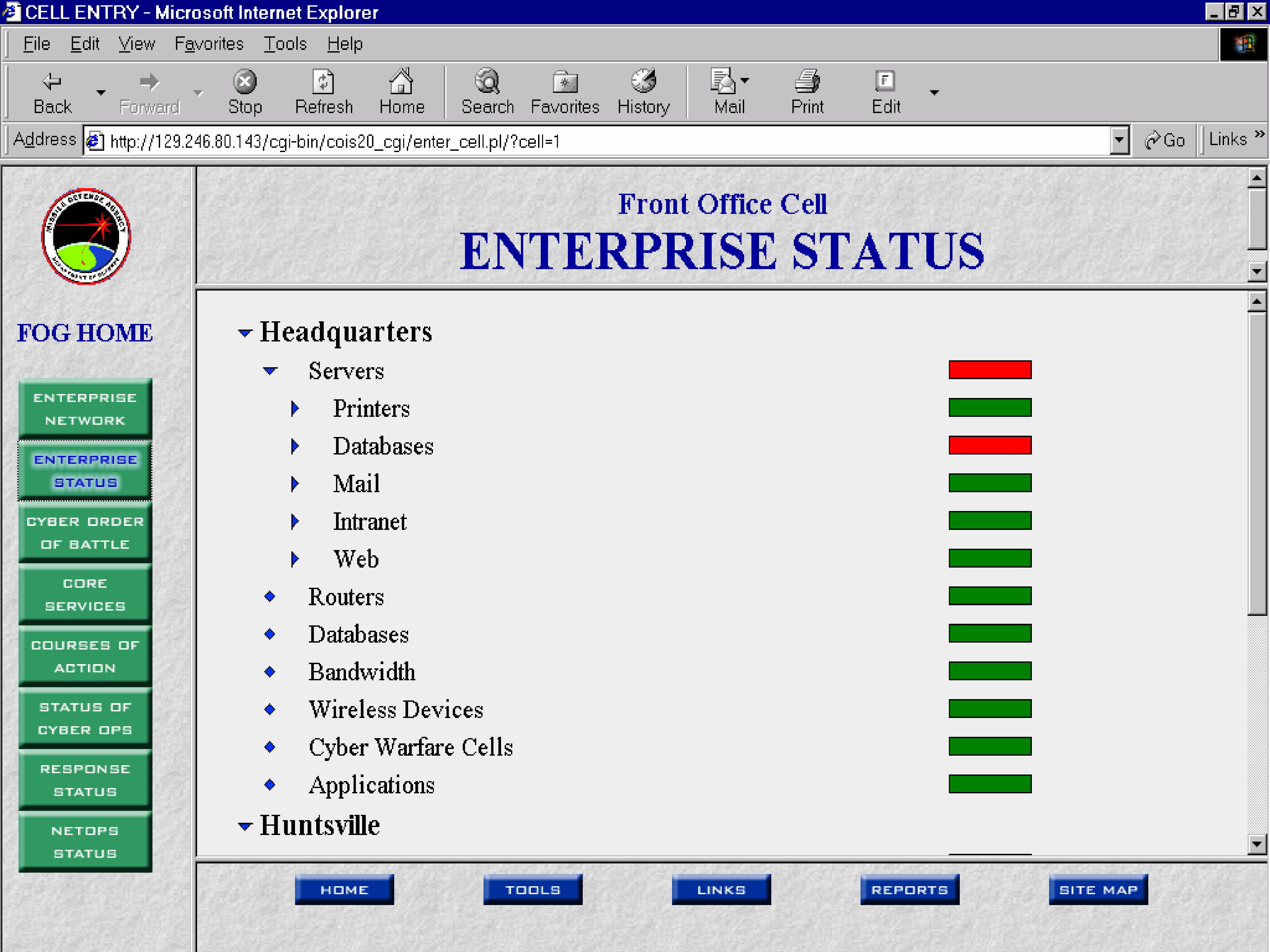


Front Office Cell

List of Simulations

SEL	RATE	NAME	DESCRIPTION
□	5 seconds	col_dos	Denial of Service Attack at Colorado Springs
□	5 seconds	col_scans	Suspecious Scans at Colorado Springs
☑	1 minute	hq_dos	Denial of Service Attack at Headquarters MDA War Room
□	5 seconds	hq_scans	Frequent Port Scanning at Headquarters
□	5 seconds	hq_trojan	Trojan Horse at Headquarters Database Server DB10111
□	5 seconds	hq_worm	Network Worm at Headquarters Conference Area

Run Cancel

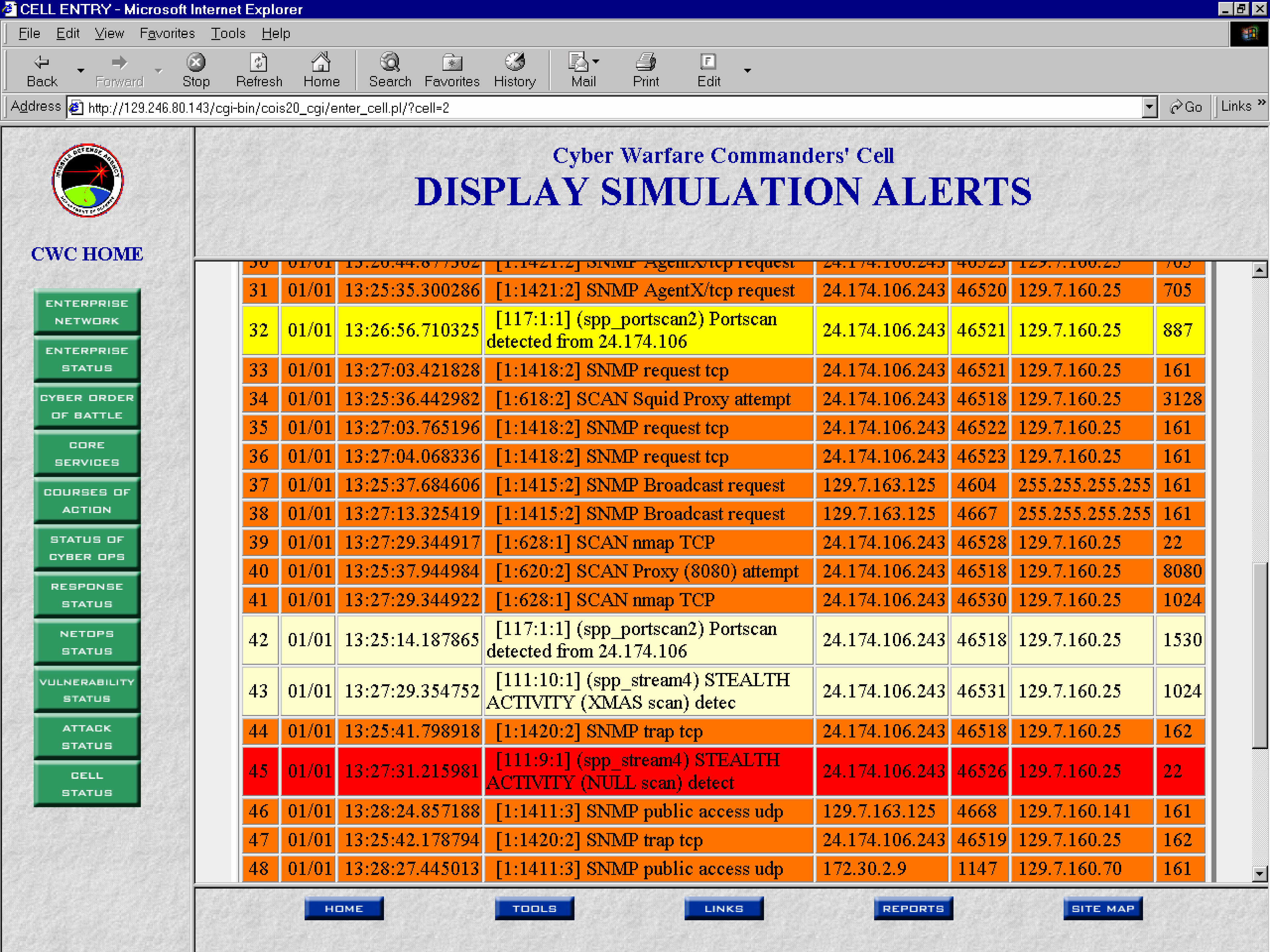

CELL ENTRY - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Address
Go
Links

http://129.246.80.143/cgi-bin/cois20_cgi/enter_cell.pl/?cell=1

Front Office Cell

ENTERPRISE STATUS

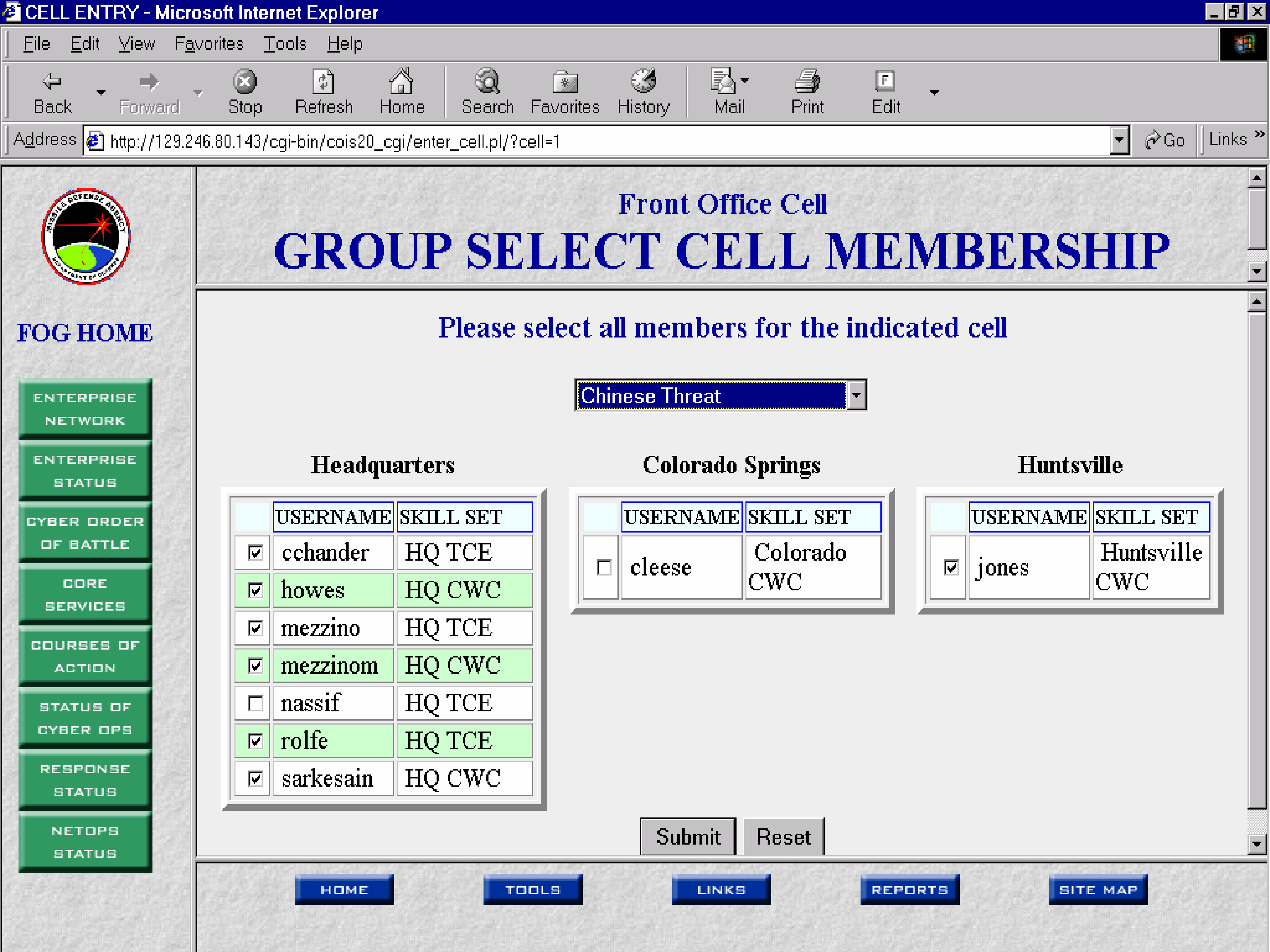
▼ **Headquarters**	
▼ Servers	🟥
▶ Printers	🟩
▶ Databases	🟥
▶ Mail	🟩
▶ Intranet	🟩
▶ Web	🟩
◆ Routers	🟩
◆ Databases	🟩
◆ Bandwidth	🟩
◆ Wireless Devices	🟩
◆ Cyber Warfare Cells	🟩
◆ Applications	🟩
▼ **Huntsville**	



Cyber Warfare Commanders' Cell

DISPLAY SIMULATION ALERTS

30	01/01	13:25:44.877562	[1:1421:2] SNMP AgentX/tcp request	24.174.106.243	46525	129.7.160.25	705
31	01/01	13:25:35.300286	[1:1421:2] SNMP AgentX/tcp request	24.174.106.243	46520	129.7.160.25	705
32	01/01	13:26:56.710325	[117:1:1] (spp_portscan2) Portscan detected from 24.174.106	24.174.106.243	46521	129.7.160.25	887
33	01/01	13:27:03.421828	[1:1418:2] SNMP request tcp	24.174.106.243	46521	129.7.160.25	161
34	01/01	13:25:36.442982	[1:618:2] SCAN Squid Proxy attempt	24.174.106.243	46518	129.7.160.25	3128
35	01/01	13:27:03.765196	[1:1418:2] SNMP request tcp	24.174.106.243	46522	129.7.160.25	161
36	01/01	13:27:04.068336	[1:1418:2] SNMP request tcp	24.174.106.243	46523	129.7.160.25	161
37	01/01	13:25:37.684606	[1:1415:2] SNMP Broadcast request	129.7.163.125	4604	255.255.255.255	161
38	01/01	13:27:13.325419	[1:1415:2] SNMP Broadcast request	129.7.163.125	4667	255.255.255.255	161
39	01/01	13:27:29.344917	[1:628:1] SCAN nmap TCP	24.174.106.243	46528	129.7.160.25	22
40	01/01	13:25:37.944984	[1:620:2] SCAN Proxy (8080) attempt	24.174.106.243	46518	129.7.160.25	8080
41	01/01	13:27:29.344922	[1:628:1] SCAN nmap TCP	24.174.106.243	46530	129.7.160.25	1024
42	01/01	13:25:14.187865	[117:1:1] (spp_portscan2) Portscan detected from 24.174.106	24.174.106.243	46518	129.7.160.25	1530
43	01/01	13:27:29.354752	[111:10:1] (spp_stream4) STEALTH ACTIVITY (XMAS scan) detec	24.174.106.243	46531	129.7.160.25	1024
44	01/01	13:25:41.798918	[1:1420:2] SNMP trap tcp	24.174.106.243	46518	129.7.160.25	162
45	01/01	13:27:31.215981	[111:9:1] (spp_stream4) STEALTH ACTIVITY (NULL scan) detect	24.174.106.243	46526	129.7.160.25	22
46	01/01	13:28:24.857188	[1:1411:3] SNMP public access udp	129.7.163.125	4668	129.7.160.141	161
47	01/01	13:25:42.178794	[1:1420:2] SNMP trap tcp	24.174.106.243	46519	129.7.160.25	162
48	01/01	13:28:27.445013	[1:1411:3] SNMP public access udp	172.30.2.9	1147	129.7.160.70	161



Address: http://129.246.80.143/cgi-bin/cois20_cgi/enter_cell.pl/?cell=1

Front Office Cell

GROUP SELECT CELL MEMBERSHIP

Please select all members for the indicated cell

Chinese Threat

Headquarters

	USERNAME	SKILL SET
☑	cchander	HQ TCE
☑	howes	HQ CWC
☑	mezzino	HQ TCE
☑	mezzinom	HQ CWC
□	nassif	HQ TCE
☑	rolfe	HQ TCE
☑	sarkesain	HQ CWC

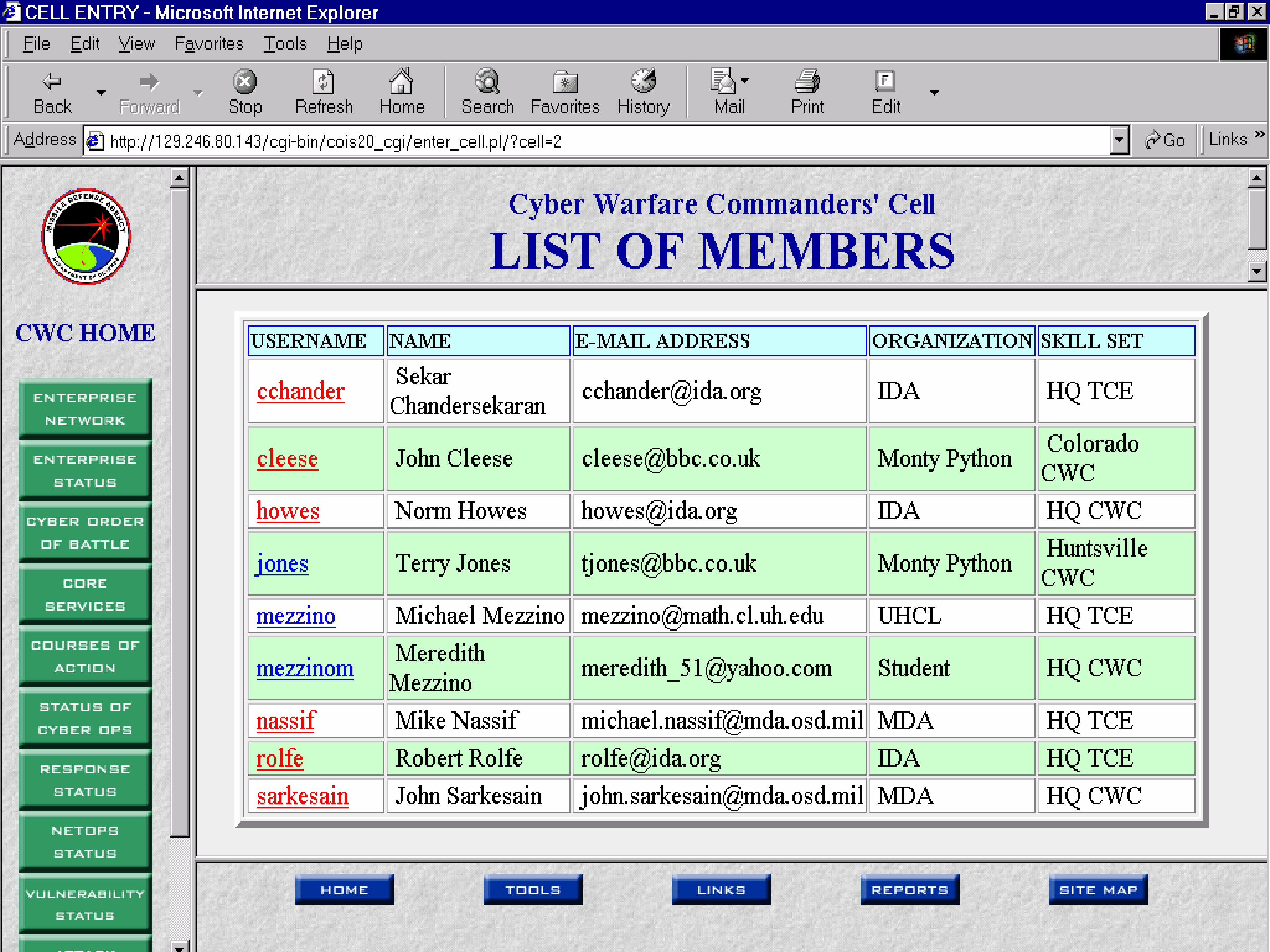
Colorado Springs

	USERNAME	SKILL SET
□	cleese	Colorado CWC

Huntsville

	USERNAME	SKILL SET
☑	jones	Huntsville CWC

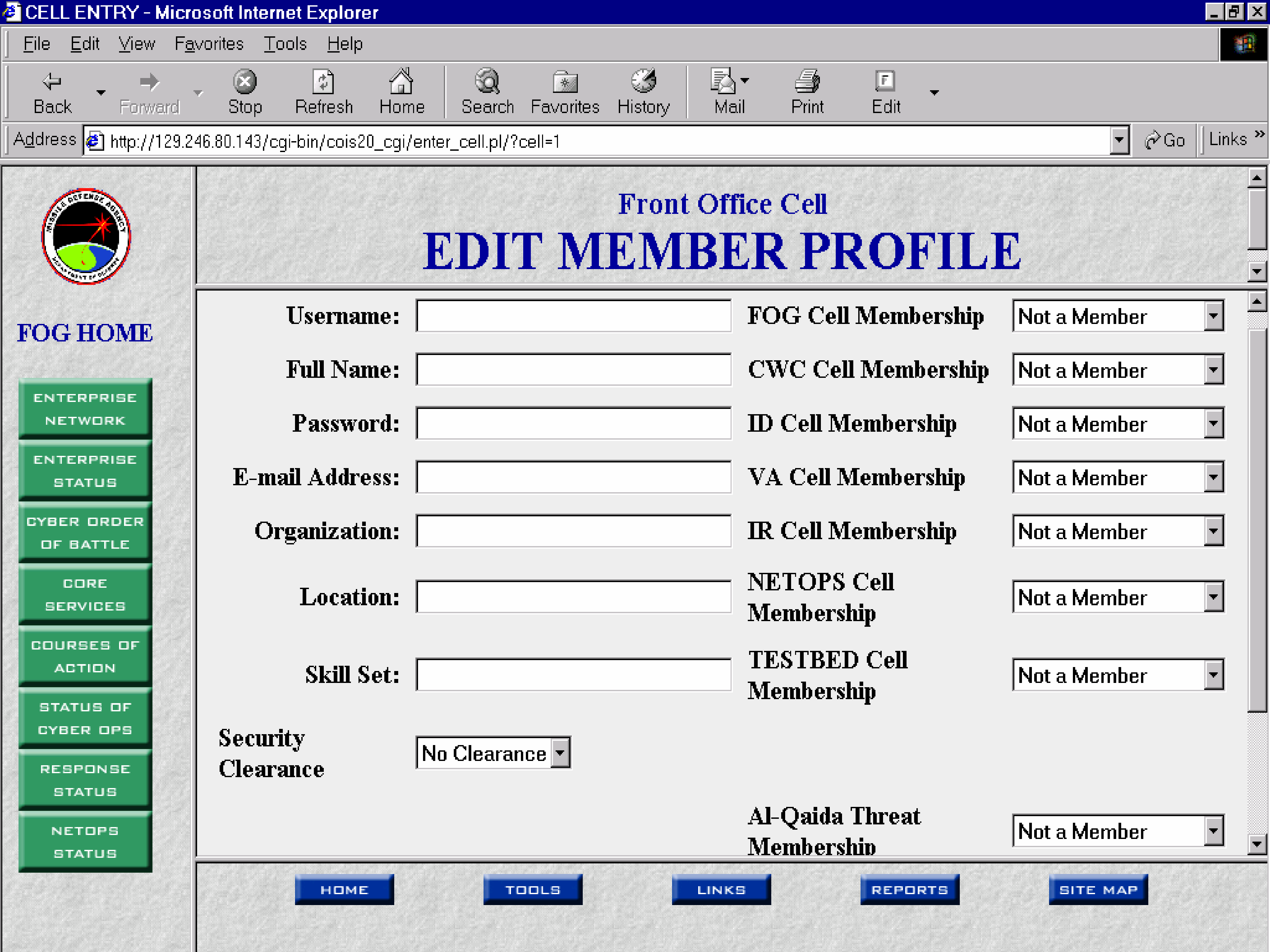
Submit Reset



Cyber Warfare Commanders' Cell

LIST OF MEMBERS

USERNAME	NAME	E-MAIL ADDRESS	ORGANIZATION	SKILL SET
cchander	Sekar Chandersekaran	cchander@ida.org	IDA	HQ TCE
cleese	John Cleese	cleese@bbc.co.uk	Monty Python	Colorado CWC
howes	Norm Howes	howes@ida.org	IDA	HQ CWC
jones	Terry Jones	tjones@bbc.co.uk	Monty Python	Huntsville CWC
mezzino	Michael Mezzino	mezzino@math.cl.uh.edu	UHCL	HQ TCE
mezzinom	Meredith Mezzino	meredith_51@yahoo.com	Student	HQ CWC
nassif	Mike Nassif	michael.nassif@mda.osd.mil	MDA	HQ TCE
rolfe	Robert Rolfe	rolfe@ida.org	IDA	HQ TCE
sarkesain	John Sarkesain	john.sarkesain@mda.osd.mil	MDA	HQ CWC



Front Office Cell

EDIT MEMBER PROFILE

Username:		FOG Cell Membership	Not a Member
Full Name:		CWC Cell Membership	Not a Member
Password:		ID Cell Membership	Not a Member
E-mail Address:		VA Cell Membership	Not a Member
Organization:		IR Cell Membership	Not a Member
Location:		NETOPS Cell Membership	Not a Member
Skill Set:		TESTBED Cell Membership	Not a Member
Security Clearance	No Clearance		
		Al-Qaida Threat Membership	Not a Member