Transportation Cyber Security

Edward Fok
Federal Highway Administration – Resource Center
Operations Technical Service Team

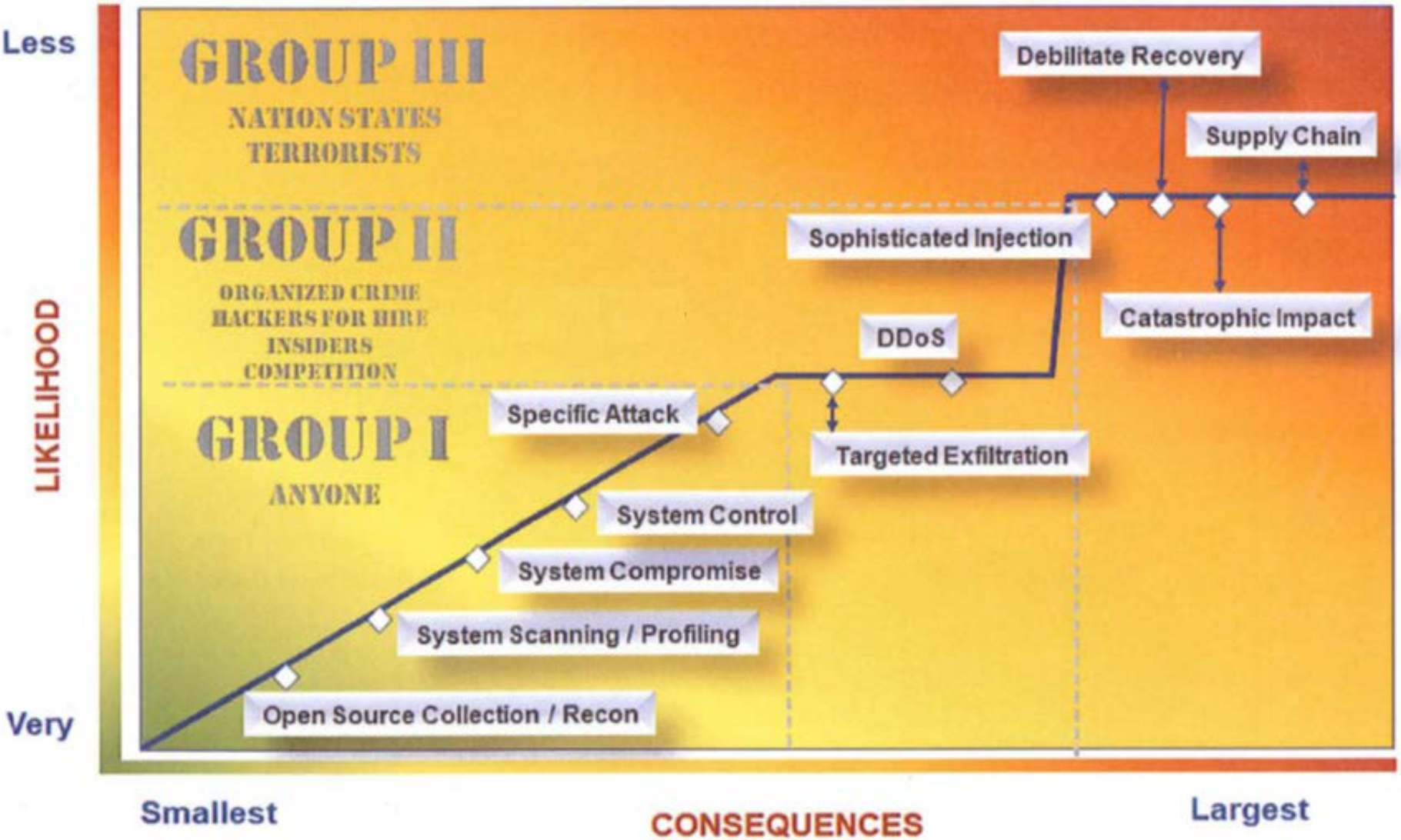
What are we trying to protect

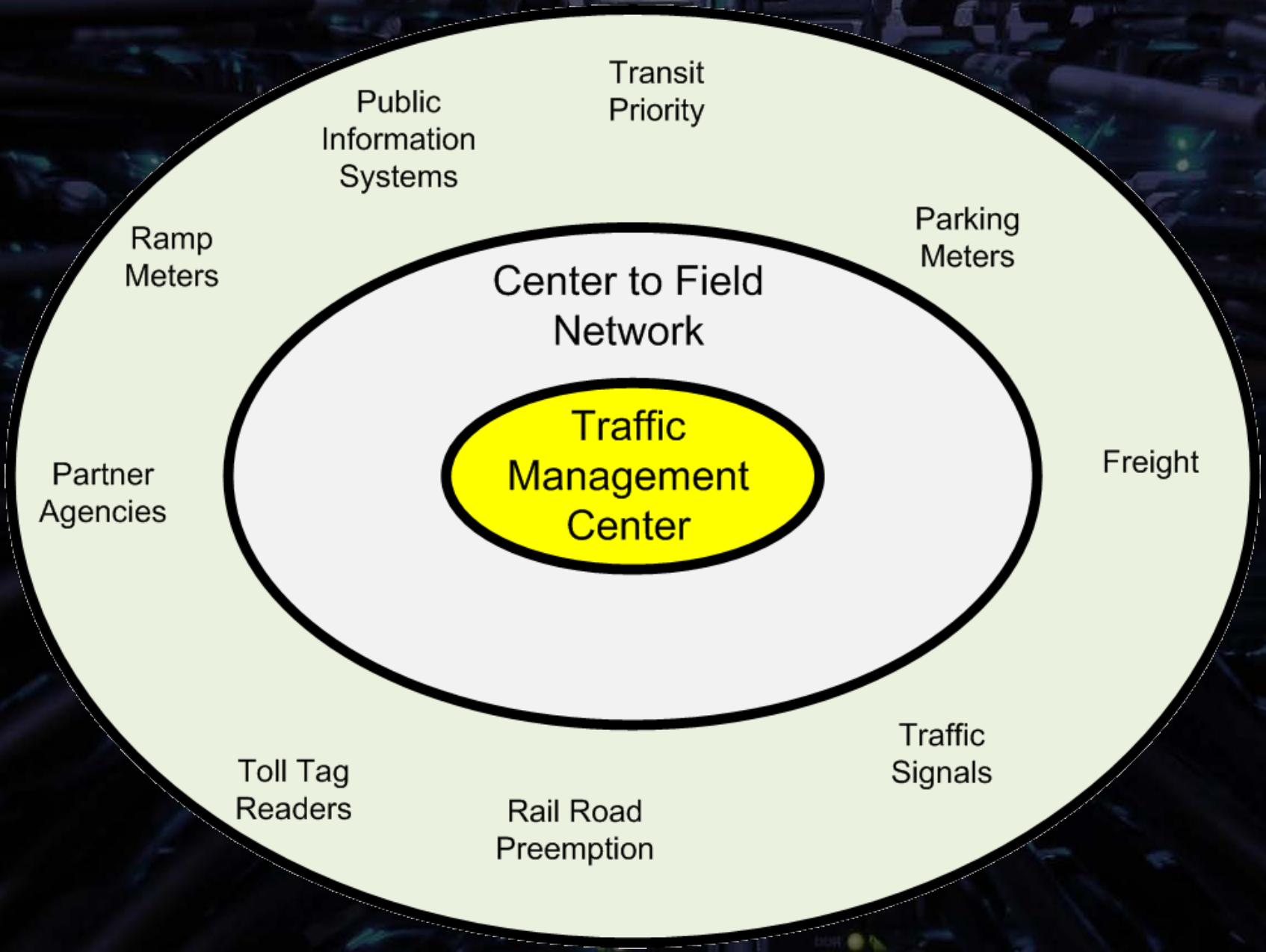
- Safe surface operation
- Efficient surface mobility
- Reliable and trusted information to the public

Why Surface Transportation?

- Hacker mentality: Naturally curious
- Hacker mentality = Mountain climber mentality
- Engineers build system to function

The Risk Curve




Transit Priority
Public Information Systems
Ramp Meters
Parking Meters
Center to Field Network
Traffic Management Center
Partner Agencies
Freight
Traffic Signals
Toll Tag Readers
Rail Road Preemption


GET
RUBY
RUBY
SUNRAY


SMOKE
WEED
EVRYDAY

myBART

Contests
Discounts
Free Events
Destinations

Join myBART
About myBART
BART.gov
Trip Planner
BARTtv

CONTESTS | DISCOUNTS | EVENTS | DESTINATIONS

MEMBERS LOG IN

Welcome to myBART!

myBART sends out a free weekly email full of entertainment news, ticket giveaways and big discounts to events happening close to BART stations.

Become a myBART member to enter our contests for a chance to win some free tickets, or explore the site right now to see this week's discount offers and find something fun to do that you can ride BART to.

myBART. Providing weekly reasons to get off the couch.

Join Now | Already a Member

```
   :::    :::     ::::::::  :::::::::        :::::::::      :::     :::::::::  :::::::::::        :::     ::::::::  ::::::::::: :::::::::::  ::::::::  ::::    :::
   :+:    :+:    :+:    :+: :+:    :+:       :+:    :+:   :+: :+:   :+:    :+:     :+:          :+: :+:  :+:    :+:     :+:         :+:     :+:    :+: :+:+:   :+:
+:+:+:+:+:+:+:+: +:+    +:+ +:+    +:+       +:+    +:+  +:+   +:+  +:+    +:+     +:+         +:+   +:+ +:+            +:+         +:+     +:+    +:+ :+:+:+  +:+
   +#+    +:+    +#+    +:+ +#++:++#+        +#++:++#+  +#++:++#++: +#++:++#:      +#+        +#++:++#++: +#+            +#+         +#+     +#+    +:+ +#+ +:+ +#+
+#+#+#+#+#+#+#+#+ +#+    +#+ +#+              +#+    +#+ +#+     +#+ +#+    +#+     +#+        +#+     +#+ +#+            +#+         +#+     +#+    +#+ +#+  +#+#+#
   #+#    #+#    #+#    #+# #+#              #+#    #+# #+#     #+# #+#    #+#     #+#        #+#     #+# #+#    #+#     #+#         #+#     #+#    #+# #+#   #+#+#
   ###    ###     ########  ###              #########  ###     ### ###    ###     ###        ###     ###  ########      ###     ###########  ########  ###    ####
```

"Sooner or later the people in this country gotta realize the government
does not give a fuck about them. The government doesn't care about you, or your children,
or your rights, or your welfare, or your safety, it simply doesn't give a fuck about you.
It's interested in its own power, that's the only thing, keeping it and expanding it wherever possible."

```
////////////////////////////////////////////////////////////////////////////////////////////////////
### #OpBart #Bart-Action #FREETOPIARY #FREEMERCEDES #FREEBRADLEYMANNING #Justice for Oscar Grant  ###
### No Justice, No Bart ### UA In The Bay ### Bay Of Rage ### Anti-sec #Justice for Charles Hill ###
////////////////////////////////////////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////////////////////////////////////////
###              Your Website has been hacked and database has been leaked by:                   ###
###              #t0nicwater #Bl4ckAbby #NaDa #Tanko #Anonymous #hackers                         ###
////////////////////////////////////////////////////////////////////////////////////////////////////
```

Dear Bay Area Rapid Transit, The People and All Government Agencies,

We are Anonymous, we are your citizens, we are the people, WE DO NOT TOLERATE OPPRESSION FROM ANY GOVERNMENT AGENCY.
BART has proved multiple times that they have no problem exploiting and abusing the people.
First they displayed this by the two recent killings by BART police. Under no circumstance, unless police are shot at,
make police killings acceptable. Non-lethal weapons were available to use during both incidents,
providing even that was necessary, but instead they shot to kill. Next they violated the people's right to assembly and prevented
other bystanders from using emergency services by blocking cell phone signals in order to stop a protest against the BART police murders.
Lastly, they set up this website called mybart.gov and they stored their members information with virtually no security.
The data was stored and easily obtainable via basic sqli. Any 8 year old with a internet connection
could have done what we did to find it. On top of that none of the info, including the passwords,
was encrypted. It is obvious BART does no give a fuck about its customers, funders and tax payers,THE PEOPLE.

The governments and government agencies of the world are becoming tyrannical and oppressive,
and the people are responding and will not take your shit for much longer. The people will fight
this oppression with protests, demonstrations, riots, hacking, ddos, online attacks and by any other means.
We will not allow ourselves to be killed, exploited, or get shitted on. From the streets of Chile,
England, Portland, San Francisco, Oakland, the people are rising up and we will support each other and
stand in solidarity against any injustice. Worldwide resistance is happening,
we will participate in solidarity against oppression. SOLIDARITY IS OUR WEAPON.

Thus below we are releasing the User Info Database of MyBart.gov, to show that BART doesn't give a shit about
it's customers and riders and to show that the people will not allow you to kill us and censor us. This is
but the one of many actions to come. We apologize to any citizen that has his information published, but
you should go to BART and ask them why your information wasn't secure with them. Also do not worry,
probably the only information that will be abused from this database is that of BART employees.

Greetz to TeaMp0ison, lulzsec, anti-sec, anarchists, anon, bay of rage, No Justice, No BART, UA in the bay,
your anon news, anonymous irc.

World Wide Solidarity, "join us to make 2011 the year of leaks and revolutions."

The Associated Press
@AP

Follow

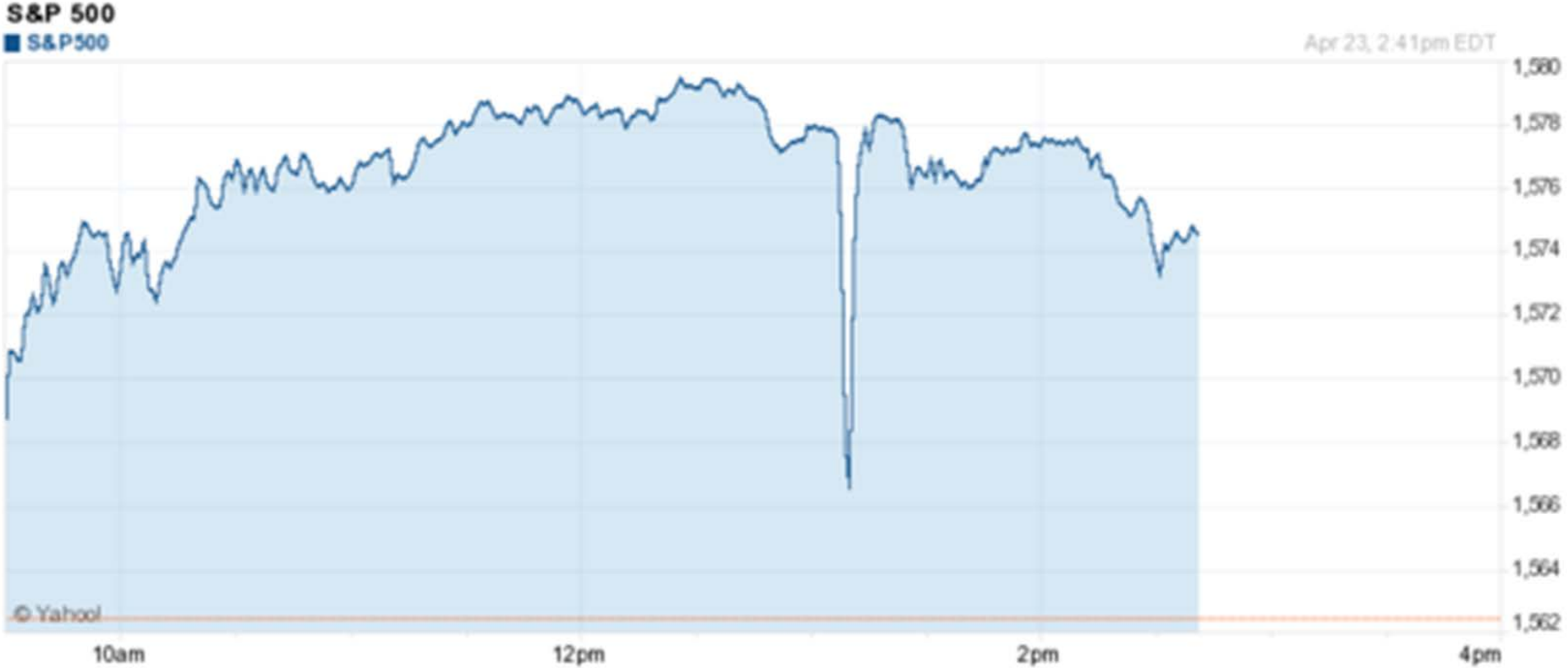
Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

483 RETWEETS

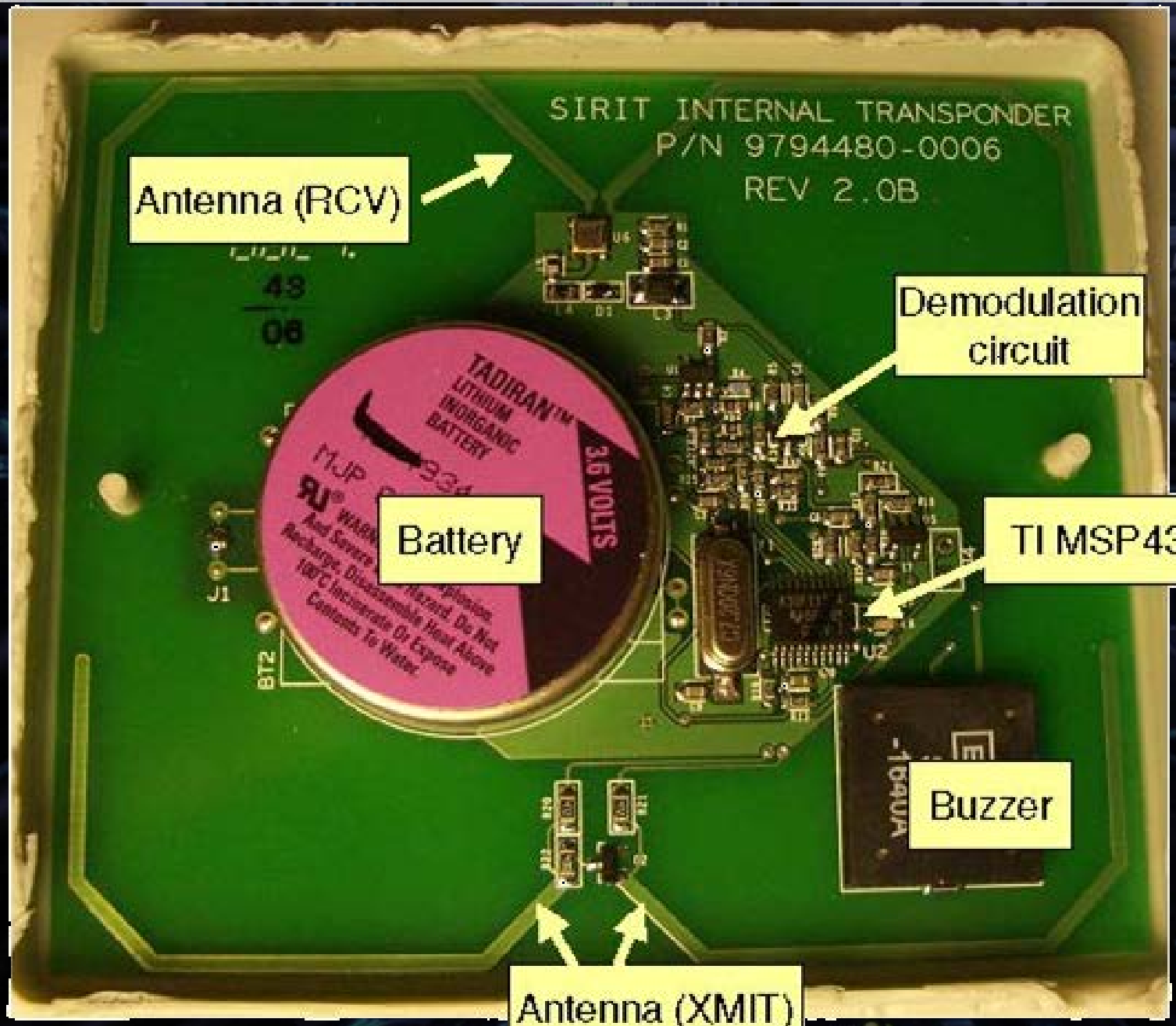
17 FAVORITES

10:07 AM - 23 Apr 13


S&P 500
S&P500
Apr 23, 2:41pm EDT
1,580
1,578
1,576
1,574
1,572
1,570
1,568
1,566
1,564
1,562
© Yahoo!
10am
12pm
2pm
4pm


303 21
303 25


MPK ŁÓDŹ
SP4ZOY


SIRIT INTERNAL TRANSPONDER
P/N 9794480-0006
REV 2.0B
Antenna (RCV)
Demodulation circuit
Battery
TI MSP430
Buzzer
Antenna (XMIT)
TADIRAN
LITHIUM INORGANIC BATTERY
3.6 VOLTS

Field Devices

- Attackers are not traffic engineers
- Examples:
  - Highway-to-hell-hacking-toll-systems (2008)
  - The Anatomy of a Subway Hack (2008)
  - “Smart” Parking Meter Implementation, Globalism, and You (2009)
  - How to hack a country’s transport network (2012)

Field Networks

- Wire Theft
- Wireless Systems
  - Leased
  - Owned (APCO P25, 4.9GHz)

THE WALL STREET JOURNAL.
WSJ.com

NOVEMBER 21, 2008, 2:26 P.M. ET

Obama's Cellphone Account Breached by Verizon Employees

Page | News | Sports | Business | Entertainment | Opinion | Lifestyle

New User? Register | Sign In | Help

Preview Mail w/ Y! Toolbar

YAHOO! ANSWERS

Search

HOME | BROWSE CATEGORIES | ABOUT

Ask

What would you like to ask?

Continue

What are you looking for?

Search Y! Ans

Timmy

How do you hack into a tornado siren warning system and trigger the sirens from your home computer?

I'm totally just curious - I'm not planning on doing this

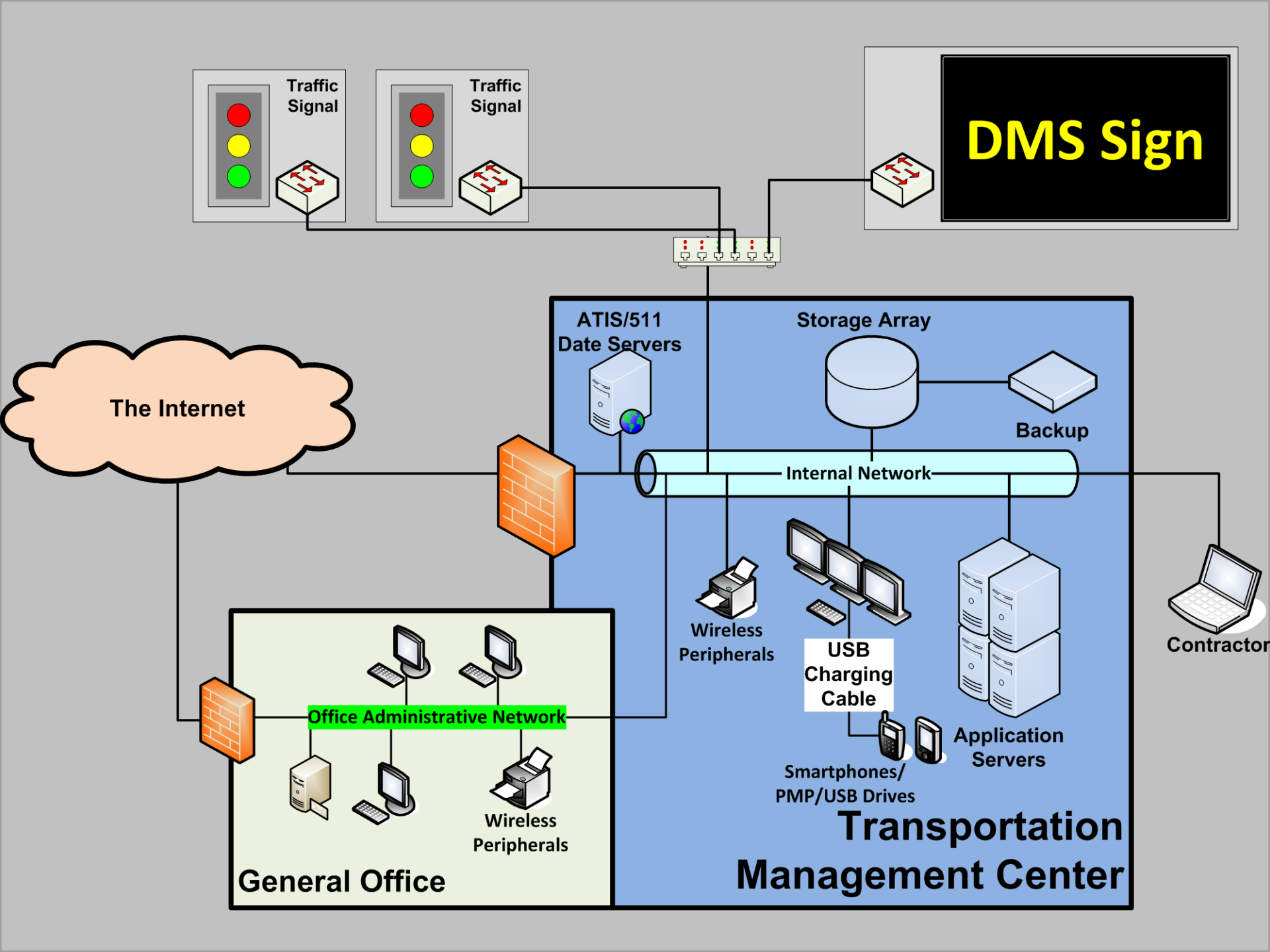
2 years ago

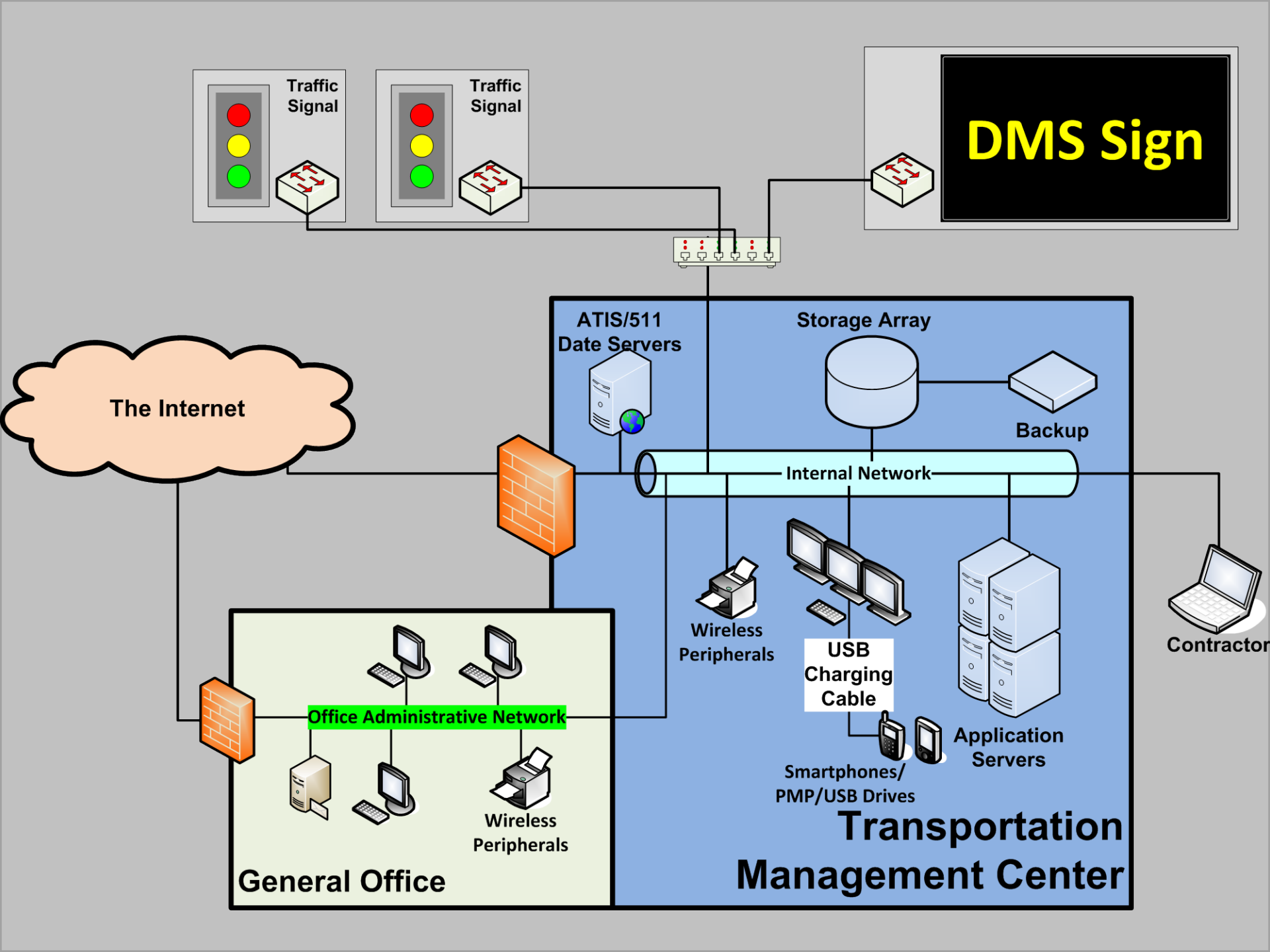
Report A

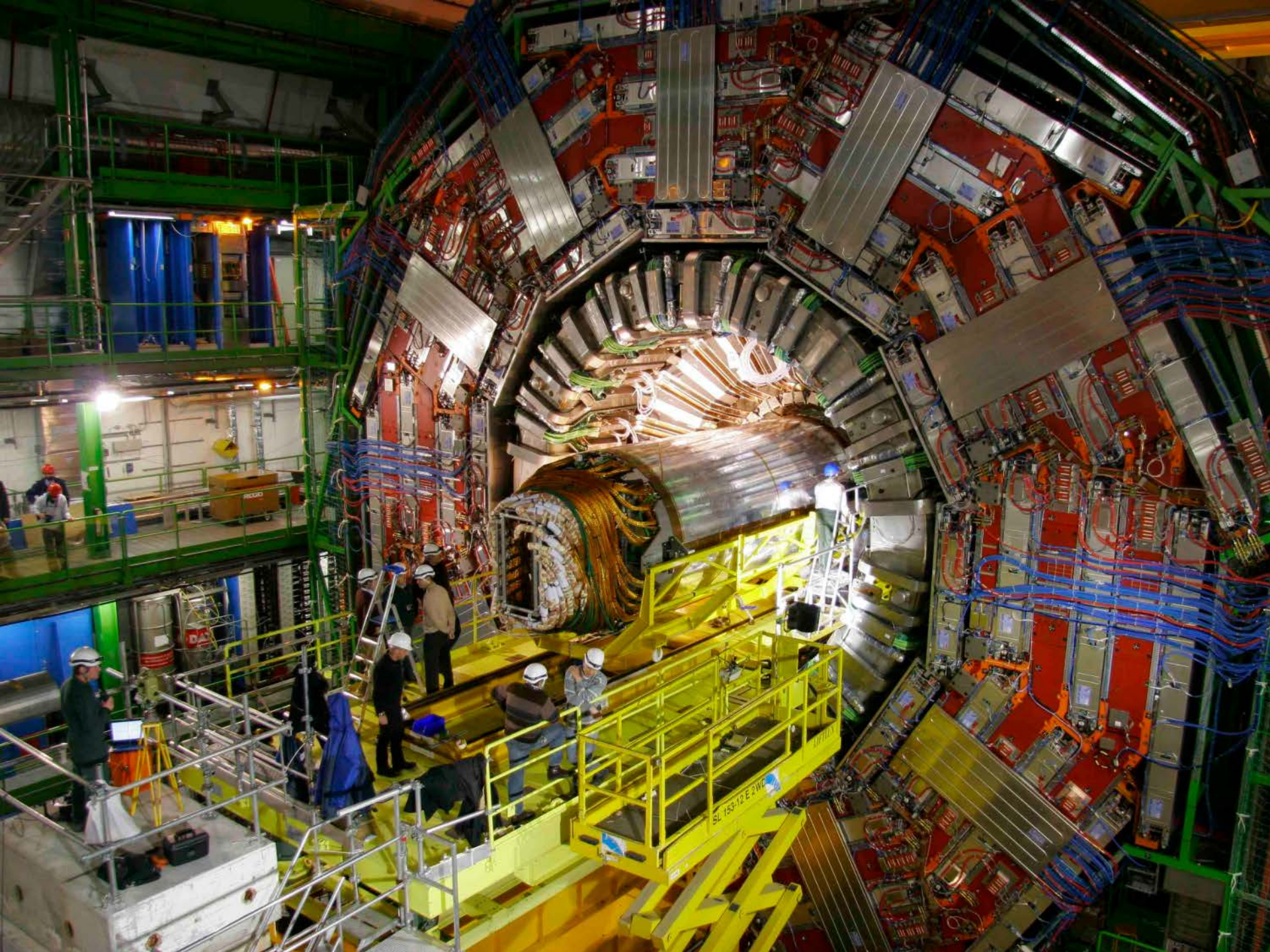
Source	Destination	Protocol	Info
Cisco_Broadcast		IEEE	Probe Request, SN=2332, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=2951, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=2960, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=3983, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=3023, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=176, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=302, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=320, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=329, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=347, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=356, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=365, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=374, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=383, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=392, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=401, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=410, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=419, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=428, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=437, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=455, FN=0, Flags=.....C, SSID=
Cisco_Broadcast		IEEE	Probe Request, SN=464, FN=0, Flags=.....C, SSID=

sorry bro not tellin'

..but there are default SSIDs :)


Traffic Signal
Traffic Signal
DMS Sign
ATIS/511 Date Servers
Storage Array
Backup
The Internet
Internal Network
Wireless Peripherals
USB Charging Cable
Application Servers
Contractor
Office Administrative Network
Smartphones/ PMP/USB Drives
Wireless Peripherals
General Office
Transportation Management Center


Traffic Signal
Traffic Signal
DMS Sign
ATIS/511 Date Servers
Storage Array
Backup
The Internet
Internal Network
Wireless Peripherals
USB Charging Cable
Application Servers
Contractor
Office Administrative Network
Smartphones/ PMP/USB Drives
Wireless Peripherals
General Office
Transportation Management Center

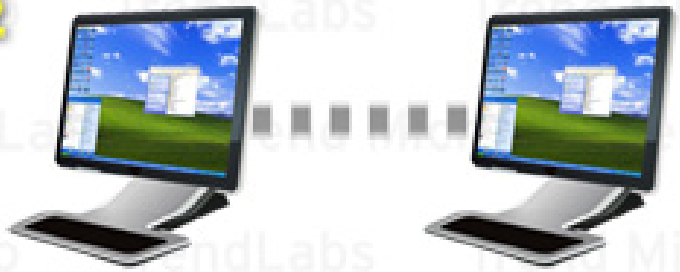


1

It exploits the following vulnerabilities in Microsoft Windows to spread copies of itself via networks and removable drives:

- MS08-067
- MS10-061
- MS10-046

2

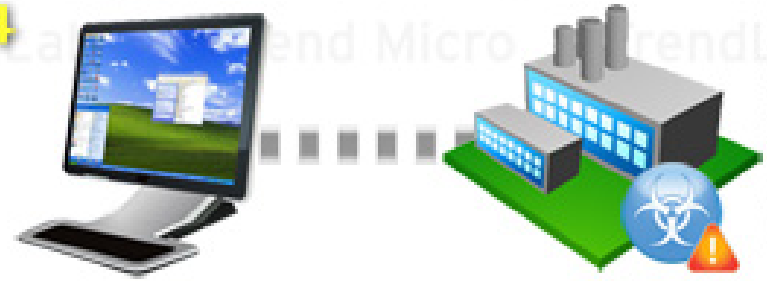


It installs server and client components to vulnerable systems to execute certain back-door functions to any client that it can connect to.

3

It connects to a remote server to test for internet connection and to send and receive commands from a remote malicious user.

4



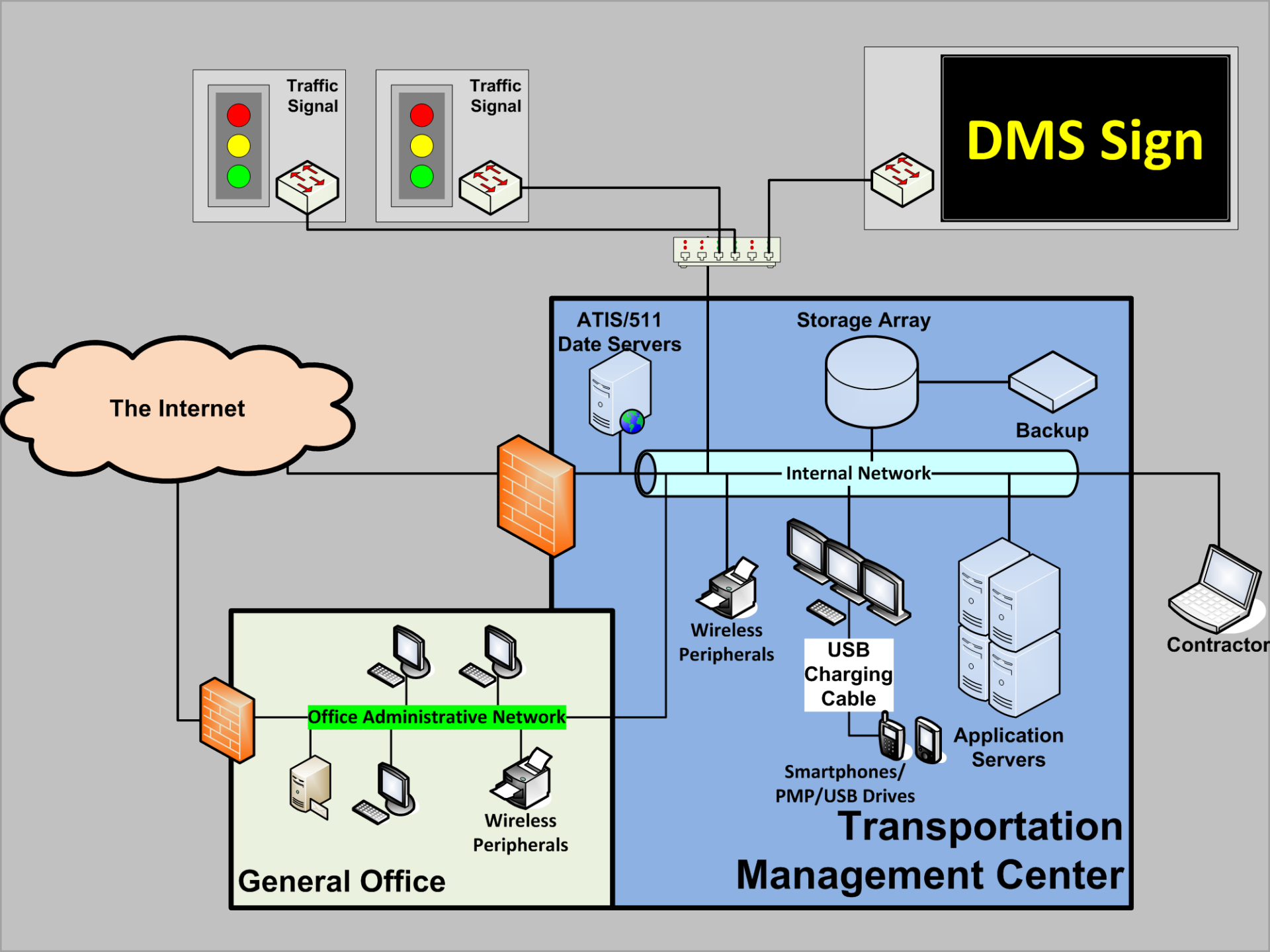
It attempts to gain access to the back-end SQL database of WinCC SQL server using CVE-2010-2772 to allow an attacker to view project databases and information from vulnerable SCADA systems.

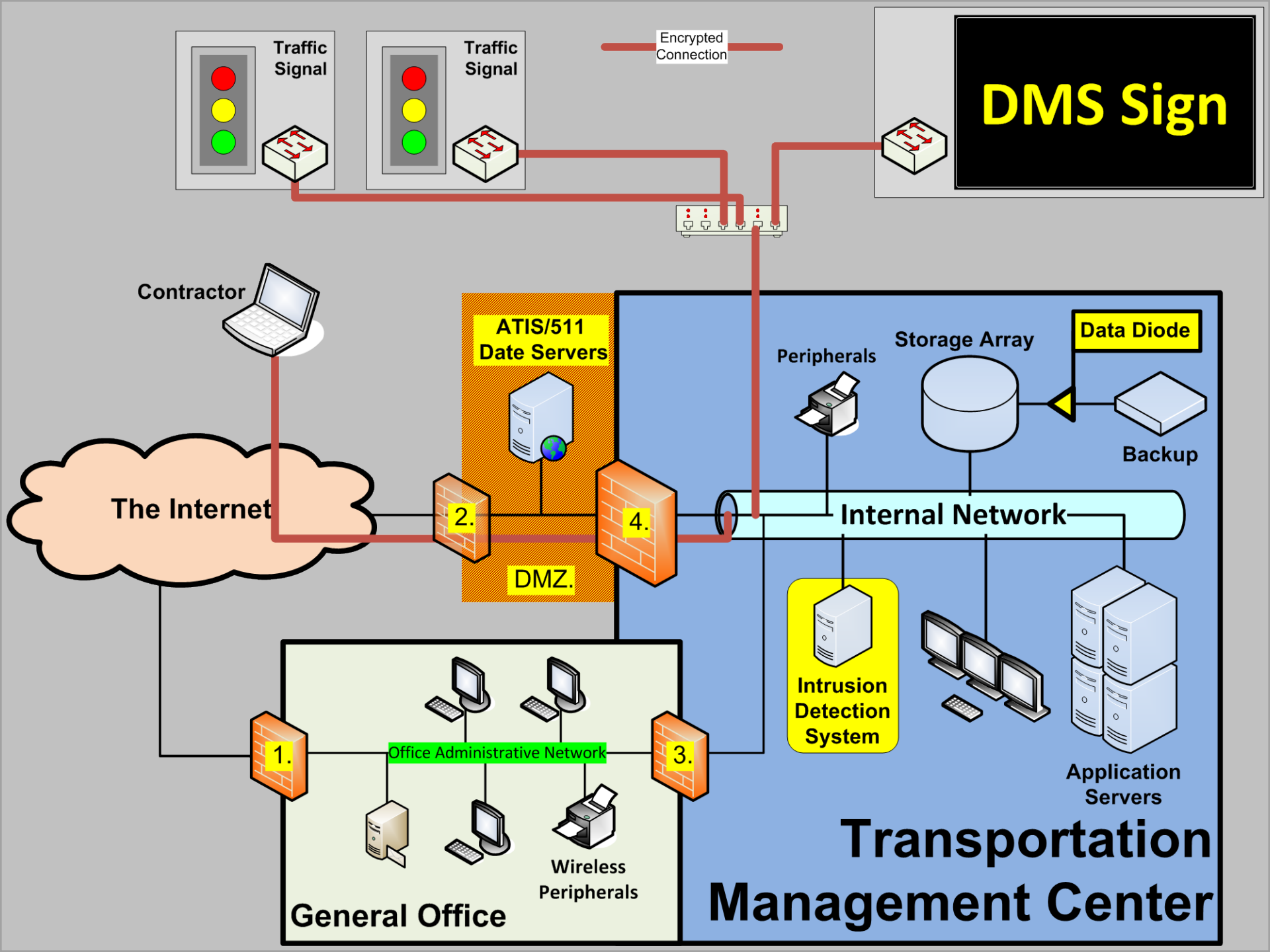
The Washington Post

Humming along with technology, until it's not

Computer meltdown creates traffic-light chaos in Montgomery

By Ashley Halsey III
Washington Post Staff Writer
Thursday, November 5, 2009


Traffic Signal
Traffic Signal
DMS Sign
ATIS/511 Date Servers
Storage Array
Backup
The Internet
Internal Network
Wireless Peripherals
USB Charging Cable
Application Servers
Contractor
Office Administrative Network
Smartphones/ PMP/USB Drives
Wireless Peripherals
General Office
Transportation Management Center


Traffic Signal
Traffic Signal
Encrypted Connection
DMS Sign
Contractor
ATIS/511 Date Servers
Peripherals
Storage Array
Data Diode
Backup
The Internet
2.
4.
Internal Network
DMZ.
Intrusion Detection System
Application Servers
1.
Office Administrative Network
3.
Wireless Peripherals
General Office
Transportation Management Center

Fannie Mae Logic Bomb Would Have Caused Weeklong Shutdown

By Kevin Poulsen ✉ January 29, 2009 | 10:41 am | Categories: Threats

A logic bomb allegedly planted by a former engineer at mortgage finance company Fannie Mae last fall would have decimated all 4,000 servers at the company, causing millions of dollars in damage and shutting down Fannie Mae for a least a week, prosecutors say.

System Configuration Files

Edit System Configuration: Default_RTD.qsc

General | Torque/Analog | Digital/CAN

Torque Tables

These tables control torque limits acting on the motor over its speed range. The 100% Accel table controls maximum motoring, the 100% Brake table controls maximum generation, and the Creep table controls torques when "zero torque" is requested.

RPM:	0	300	600	900	1200	1500	1910	2100	2400	2700	3000	3300
100% Accel Torque	200	200	200	200	200	200	200	200	200	200	191	173
	0kW	6kW	13kW	19kW	25kW	31kW	40kW	44kW	50kW	57kW	60kW	60kW
100% Brake Torque	-200	-200	-200	-200	-200	-200	-200	-200	-200	-200	-191	-173
	-0kW	-6kW	-13kW	-19kW	-25kW	-31kW	-40kW	-44kW	-50kW	-57kW	-60kW	-60kW
☐ Creep Torque	0	0	0	0	0	0	0	0	0	0	0	0
	0kW	0kW	0kW	0kW	0kW	0kW	0kW	0kW	0kW	0kW	0kW	0kW

Speed Safety

In situations where the motor speed goes over these speed limits, the system will reduce the motoring torque to prevent the motor from going faster.

	Forward Direction	Reverse Direction
Speed Limit (RPM):	3600	-3600
RPM Range for Torque Reduction:	300	300
Torque Limiting over Range:	◉ Accel->Zero Torque ○ Accel->Brake Torque	◉ Accel->Zero Torque ○ Accel->Brake Torque

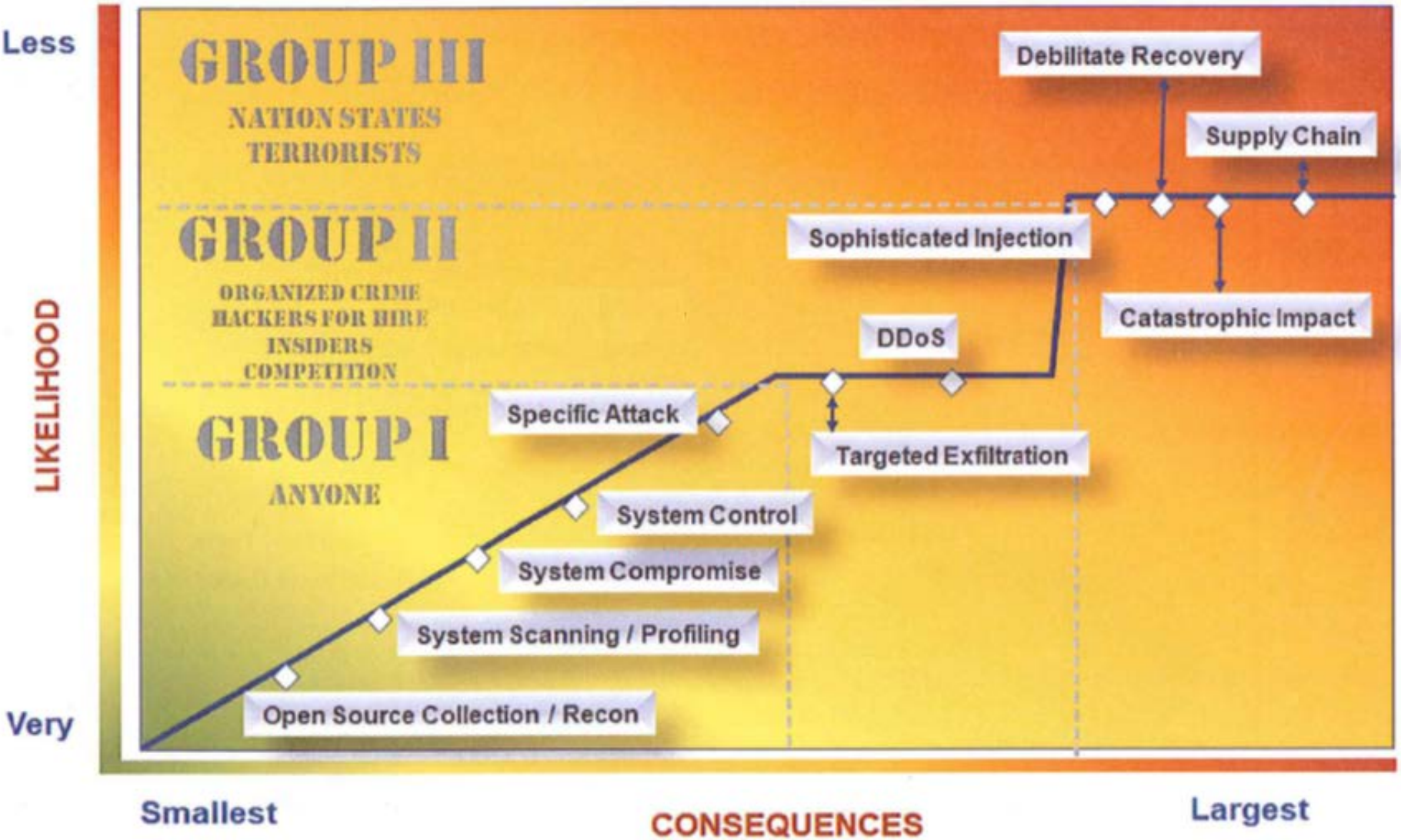
☐ Quadratic

Hand Controller Settings

Note: Values in volts. Range: -0.5V - 5.5V

	Accelerator	Brake
Maximum Error:	5.5	4.75
Maximum Allowed:	4.5	4.5
Minimum Allowed:	0.5	0.5
Minimum Error:	-0.1	-0.5

The Risk Curve



Where to Get HELP!

Multi-State Information Sharing & Analysis Center (MS-ISAC)

http://msisac.cisecurity.org

Computer Emergency Response Team (CERT)

- http://www.cert.org
- Document: Roadmap to Secure Control Systems in the Transportation Sector
- Very good source on Insider Threat and Prevention

Microsoft Technet

ISO/IEC 27000

Information Security Forum

"Standard of Good Practice"

Industrial Control Systerm-CERT Self Assessment

http://ics-cert.us-cert.gov/Assessments

National Institute of Standards and Technology

http://csrc.nist.gov/index.html

SANS Institute

- http://www.sans.org
- http://ics.sans.org

National Vulnerability Database

http://nvd.nist.gov

AntiVirus

- http://av-comparatives.org/
- EICAR virus scanner tester