

RSA CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Operation Olympic Games Is the Tom Clancy Spy Story that Changed Everything

SESSION ID: HT-F01

RICK HOWARD

CSO
PALO ALTO NETWORKS
@RACEBANNON99



How Technical Are You?

How Technical Are You?



How Technical Are You?

Have you ever e-mailed the person who works at the desk next to you?



How Technical Are You?

Have you ever e-mailed the person who works at the desk next to you?

Do you maintain a list of 15 phone numbers to reach your family of 3?



How Technical Are You?

Have you ever e-mailed the person who works at the desk next to you?

Do you maintain a list of 15 phone numbers to reach your family of 3?

Have you ever pulled up into your own driveway and used your cell phone to see if anyone is home?



Olympic Games: Introduction



Olympic Games: Introduction

The New York Times



David Sanger



Olympic Games: Introduction



Olympic Games: Introduction



Olympic Games: Introduction



Agenda

1: Story

2: Impact to the Cyber Security Community

2: Impact to the Political World



Olympic Games: Introduction

Great Story

Targeted Reconnaissance

Hacking

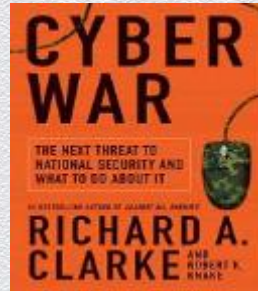
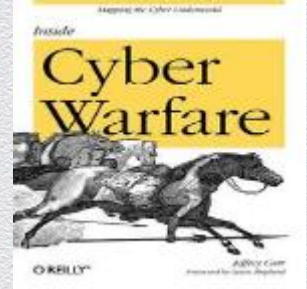
Sabotage

Assassination

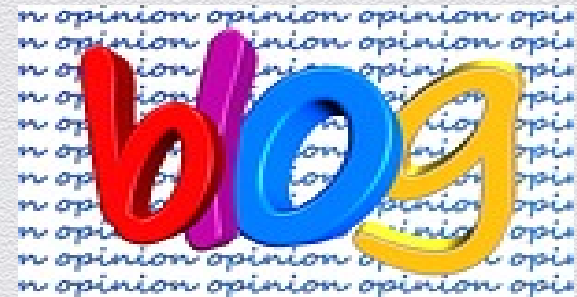
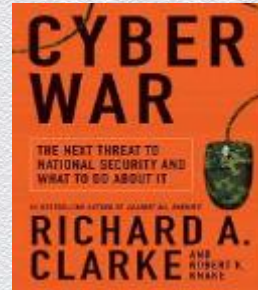
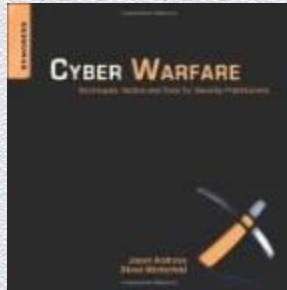
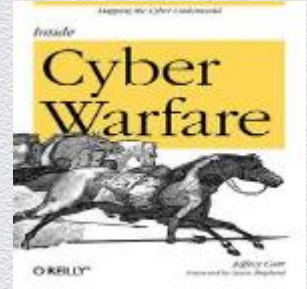
Olympic Games: Cyber Warfare is Inevitable Now



Olympic Games: Cyber Warfare is Inevitable Now



Olympic Games: Cyber Warfare is Inevitable Now



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



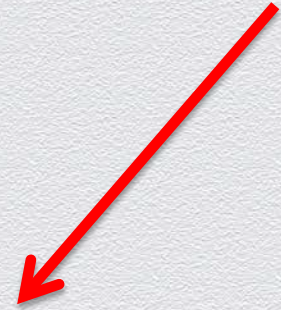
Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public



Olympic Games: Stuxnet Goes Public

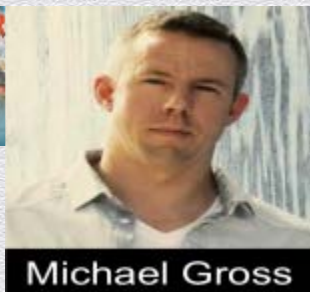


ATTACKERS

Olympic Games: Confront and Conceal



Olympic Games: The Journalists



Michael Gross

The New York Times



David Sanger

WIRED



Kim Zetter



Stuxnet

Olympic Games: The Security Researchers



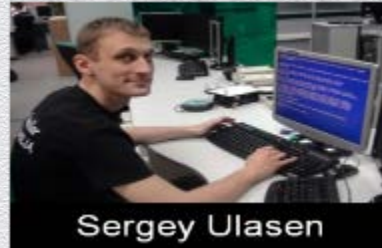
Liam O Murchu



Eric Chien



Nicolas Falliere



Sergey Ulasen



Laboratory of Cryptography and System Security (CrySyS)



Eugene Kaspersky



Ralph Langer



Olympic Games: The Story

Olympic Games: Stuxnet Discovery



Olympic Games: Stuxnet Discovery



Supervisory Control and
Data Acquisition



Olympic Games: Stuxnet Discovery



Supervisory Control and
Data Acquisition



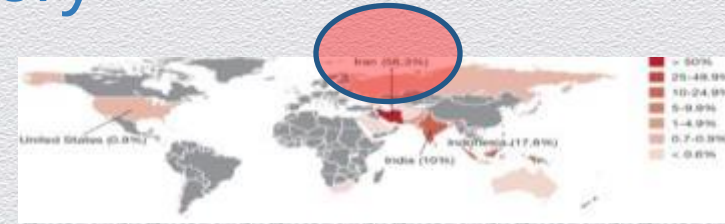
Olympic Games: Stuxnet Discovery



Supervisory Control and
Data Acquisition



Olympic Games: Stuxnet Discovery



Olympic Games: Stuxnet Discovery



Enriched



Olympic Games: Stuxnet Discovery



Olympic Games: Stuxnet Discovery



Olympic Games: The Story



Olympic Games: The Story



Source: NYT Jan 15 2011



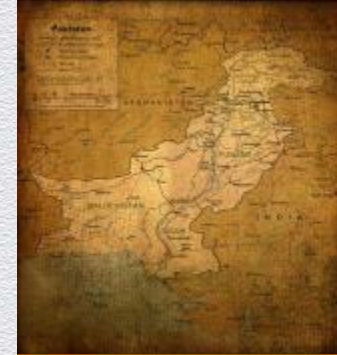
Olympic Games: The Story



First Generation



Centrifuge



Pakistan



A. Q. Khan



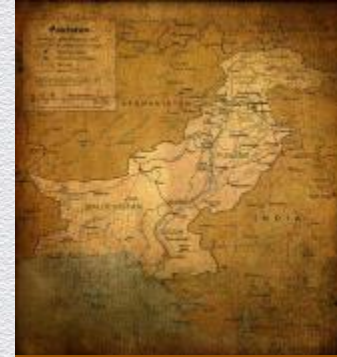
Olympic Games: The Story



First Generation



Centrifuge



Pakistan



A. Q. Khan



Olympic Games: The Story

First Generation



Olympic Games: The Story

First Generation



Enriched



Olympic Games: The Story

First Generation



Enriched

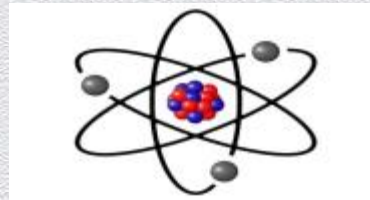


Olympic Games: The Story

First Generation



Enriched

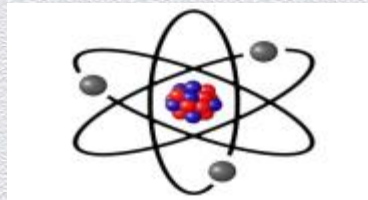


Olympic Games: The Story

First Generation



Enriched

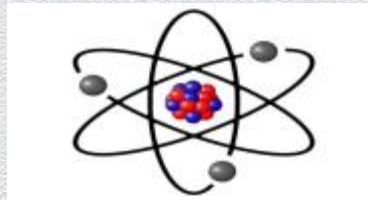


Olympic Games: The Story

First Generation



Enriched



Olympic Games: The Story



1990s

Muammar al-Gaddafi



Olympic Games: The Story



Muammar al-Gaddafi

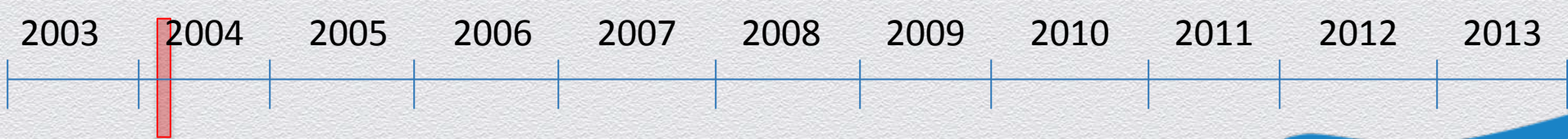


Olympic Games: The Story



P₁

Vulnerabilities



Olympic Games: The Story

NEGEV DESERT



P₁

Vulnerabilities



Olympic Games: The Story



Olympic Games: The Story



Olympic Games: The Story



P₁

Vulnerabilities



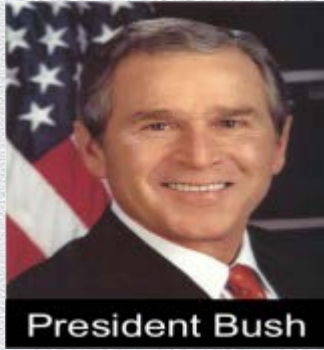
General James Cartwright (Retired)



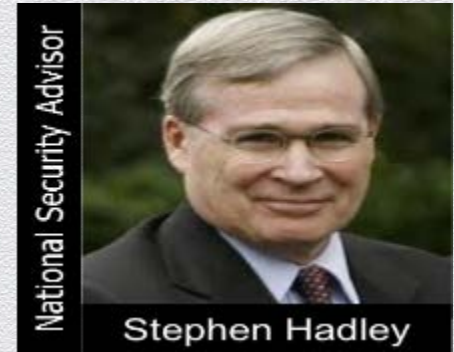
Mike McConnell



Olympic Games: The Story



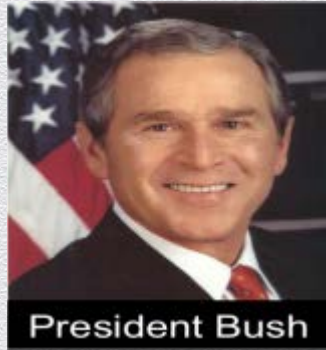
Olympic Games: The Story



Olympic Games: The Story



Olympic Games: The Story



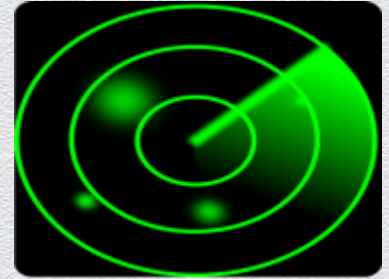
Olympic Games: The Plan

2 PHASE PLAN OLYMPIC GAMES



Olympic Games: The Plan

PHASE 1



Olympic Games: The Plan



PHASE 2

Bug

DELAY & DEGRADE

Enriched



Olympic Games: The Plan

PHASE 1



PHASE 2

Bug



Olympic Games: The Plan



PHASE 1



PHASE 2

Bug



Olympic Games: The Story



PHASE 1

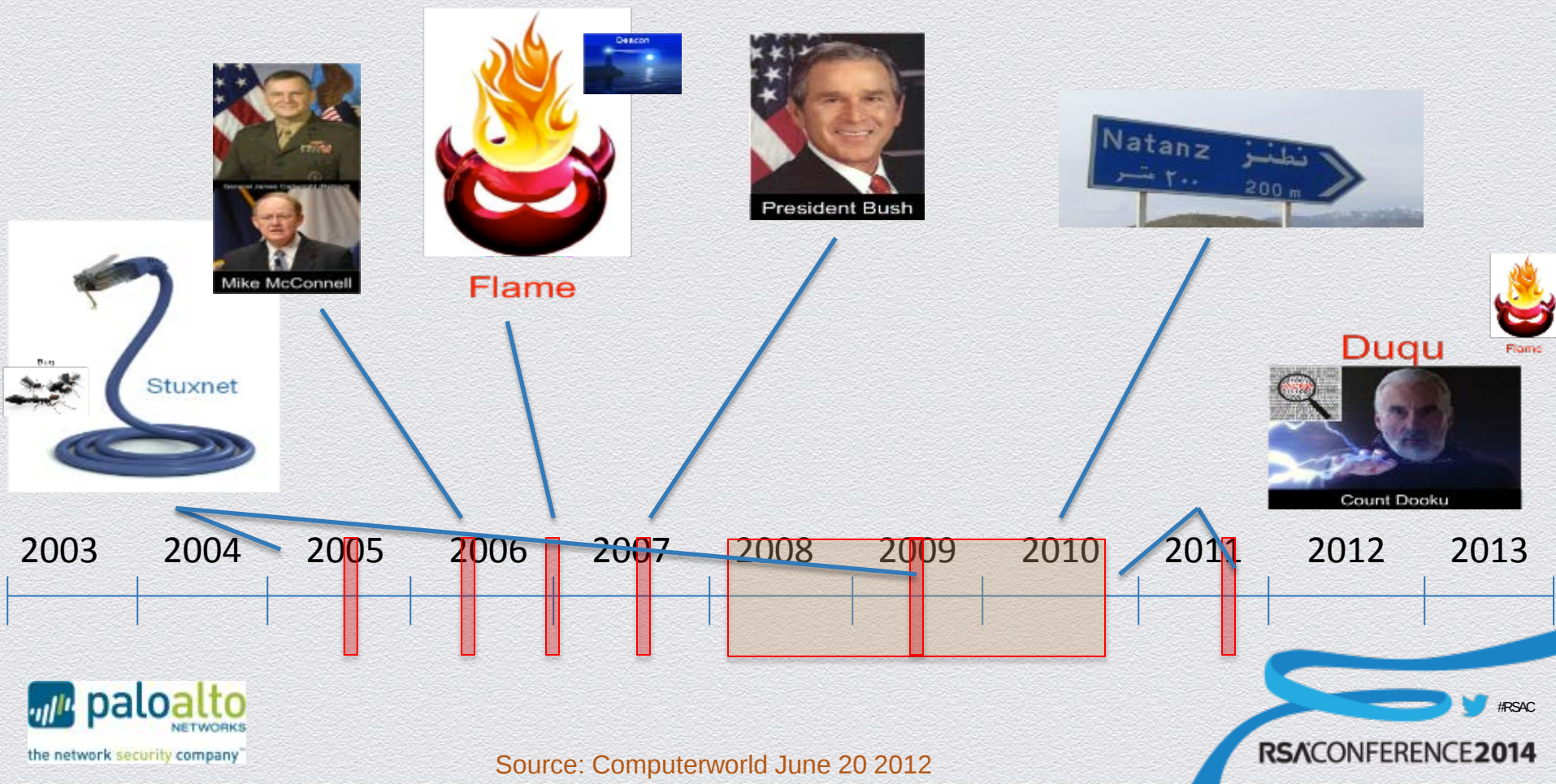


PHASE 2

Bug



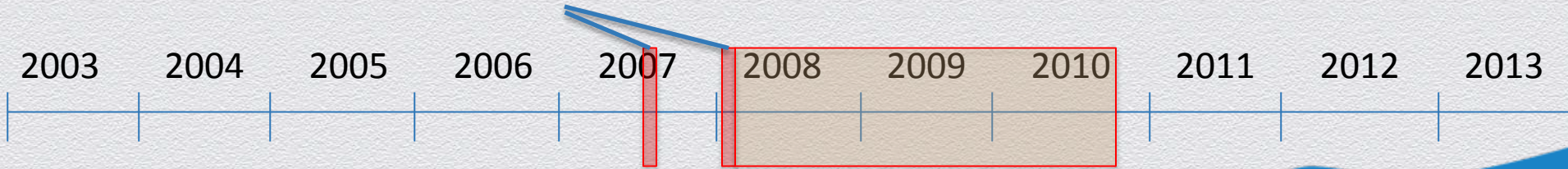
Olympic Games: The Story



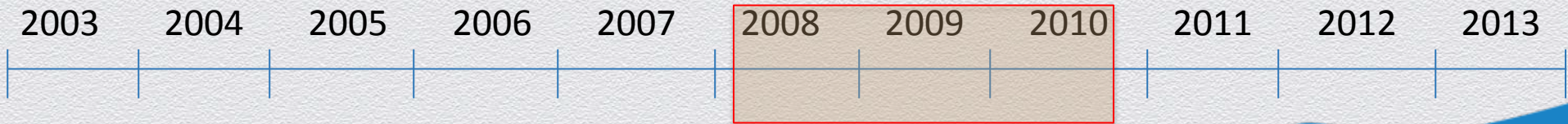
Olympic Games: The Story



Undermine
Electrical
Systems



Olympic Games: The Story



Olympic Games: The Story



SIEMENS

Industrial Control Systems (ICS)



Vulnerabilities



Source: NYT Jan 15 2011



Olympic Games: The Story

SIEMENS

Industrial Control Systems (ICS)



Supervisory Control
and Data Acquisition



NATANZ, IRAN — SITE OVERVIEW



INSTITUTE FOR SCIENCE AND
INTERNATIONAL SECURITY

IMAGE CREDIT: DIGITAL GLOBE
DATE OF IMAGE 16 SEPT 2002

THE NATANZ SITE IS A POTENTIAL URANIUM ENRICHMENT FACILITY,
POSSIBLY A GAS CENTRIFUGE SITE. IT IS LOCATED APPROXIMATELY
100 MILES SOUTH OF TEHRAN.

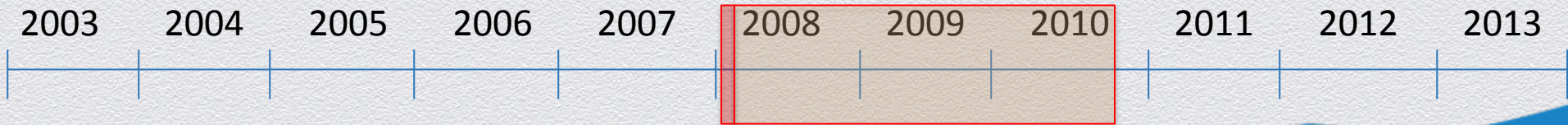
2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013



Olympic Games: The Story



Mission: Ensure the nation's energy security with safe, competitive, and sustainable energy systems and unique national and homeland security capabilities.



Source: Idaho National Laboratory

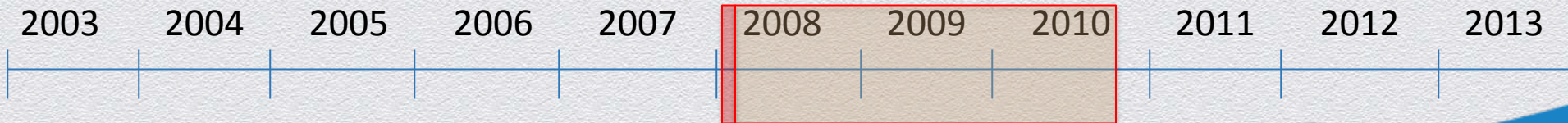


Olympic Games: The Story



P₁

Mission: Ensure the nation's energy security with safe, competitive, and sustainable energy systems and unique national and homeland security capabilities.



Olympic Games: The Story



SIEMENS
Industrial Control Systems (ICS)

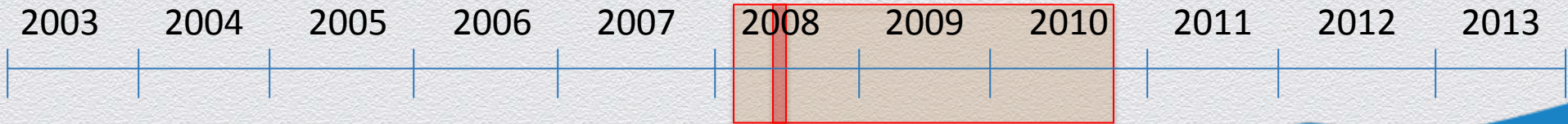
INL
Idaho National Laboratory



Vulnerabilities



Supervisory Control
and Data Acquisition



paloalto
NETWORKS
the network security company™



Source: NYT Jan 15 2011

RSACONFERENCE2014

Olympic Games: The Delivery



Flame



No Internet



Olympic Games: The Delivery



Flame



Stuxnet



NATANZ, IRAN — SITE OVERVIEW



INSTITUTE FOR SCIENCE AND
INTERNATIONAL SECURITY

IMAGE CREDIT: DIGITAL GLOBE
DATE OF IMAGE 16 SEPT 2002

THE NATANZ SITE IS A POTENTIAL URANIUM ENRICHMENT FACILITY, POSSIBLY A GAS CENTRIFUGE SITE. IT IS LOCATED APPROXIMATELY 100 MILES SOUTH OF TEHRAN.



2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013



Olympic Games: The Delivery



Flame



NATANZ, IRAN — SITE OVERVIEW

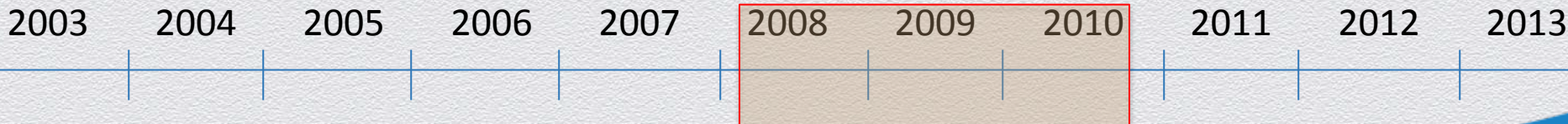


INSTITUTE FOR SCIENCE AND
INTERNATIONAL SECURITY

IMAGE CREDIT: DIGITAL GLOBE
DATE OF IMAGE 16 SEPT 2002

THE NATANZ SITE IS A POTENTIAL URANIUM ENRICHMENT FACILITY,
POSSIBLY A GAS CENTRIFUGE SITE. IT IS LOCATED APPROXIMATELY
100 MILES SOUTH OF TEHRAN.

SIEMENS
Industrial Control Systems (ICS)



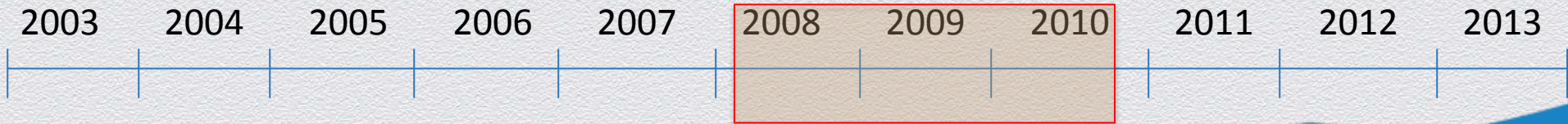
Olympic Games: The Delivery



Flame



Supply Chain



Olympic Games: The Delivery

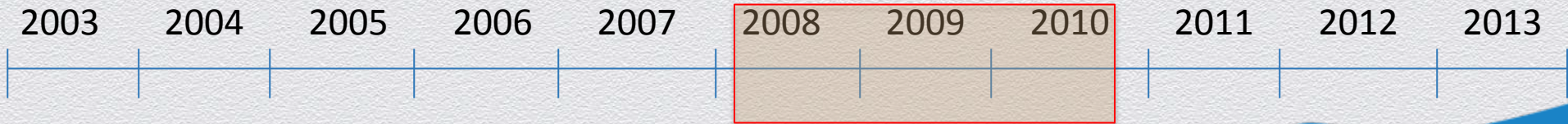


Flame



SIEMENS
Industrial Control Systems (ICS)

Supply Chain



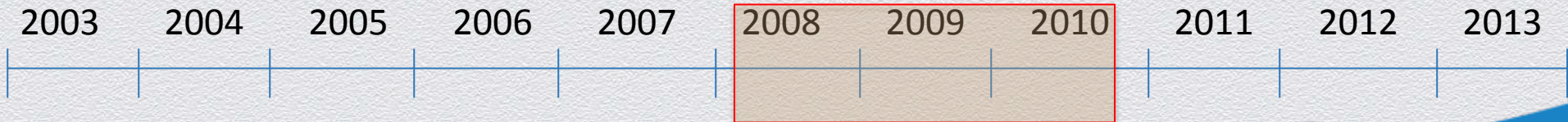
Olympic Games: The Delivery



Flame



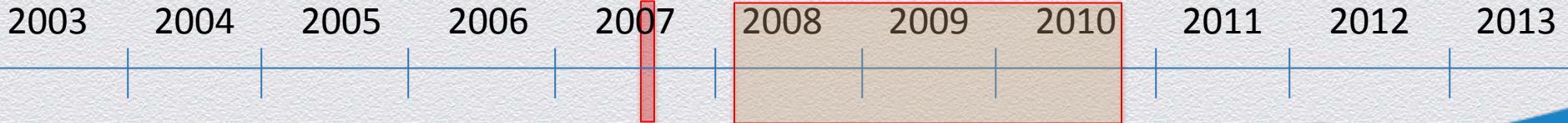
Reliable
Delivery
Mechanism



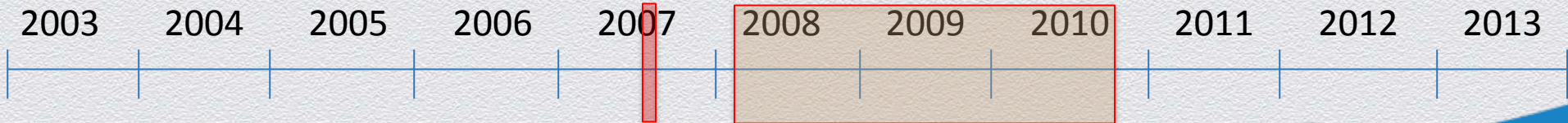
Olympic Games: The Legal Authority



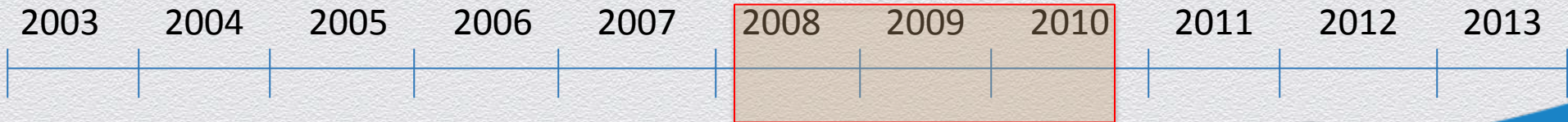
General James Cartwright (Retired)



Olympic Games: The Legal Authority



Olympic Games: The Legal Authority



Olympic Games: The Legal Authority



Olympic Games: The Legal Authority

Title 10 of the United
States Code (USC)



WAR OPERATIONS

Olympic Games: The Legal Authority



Title 10 of the United
States Code (USC)



WAR OPERATIONS

Title 50 of the United
States Code (USC)



COVERT OPERATIONS

Olympic Games: The Legal Authority



Title 10 of the United
States Code (USC)



WAR OPERATIONS

Destroying



Critical
Infrastructure

Olympic Games: The Legal Authority



Title 50 of the United States Code (USC)



COVERT OPERATIONS

Olympic Games: The Legal Authority



Title 50 of the United States Code (USC)



COVERT OPERATIONS



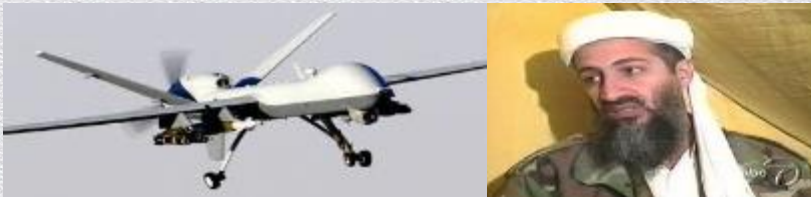
Olympic Games: The Legal Authority



Title 50 of the United States Code (USC)



COVERT OPERATIONS



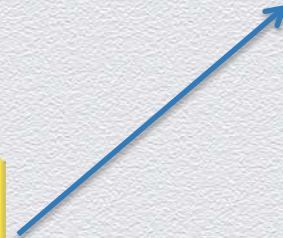
Olympic Games: The Legal Authority



**INTELLIGENCE
COMMITTEES**



**PRESIDENTIAL
FINDING**



Olympic Games: The Legal Authority



Presidential Findings describe influence actions against political, economic or military objectives

**PRESIDENTIAL
FINDING**



Olympic Games: The Legal Authority



Olympic Games: The Legal Authority



Olympic Games: The Legal Authority



Olympic Games: The Legal Authority



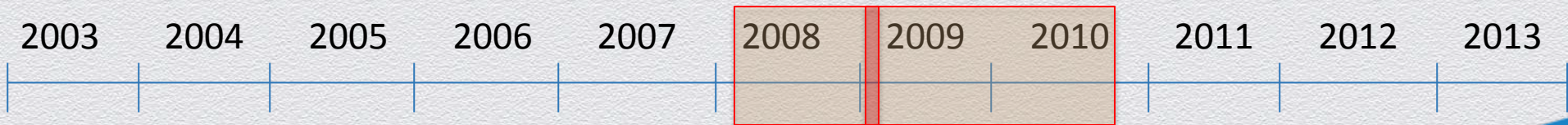
Takes Office 20 January



Olympic Games: The Legal Authority



PRESIDENTIAL FINDINGS



Olympic Games: The Story



P₁

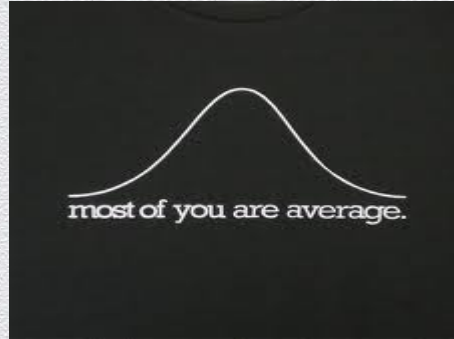


1000 Centrifuges Dismantled



Olympic Games: The Sophistication of Stuxnet

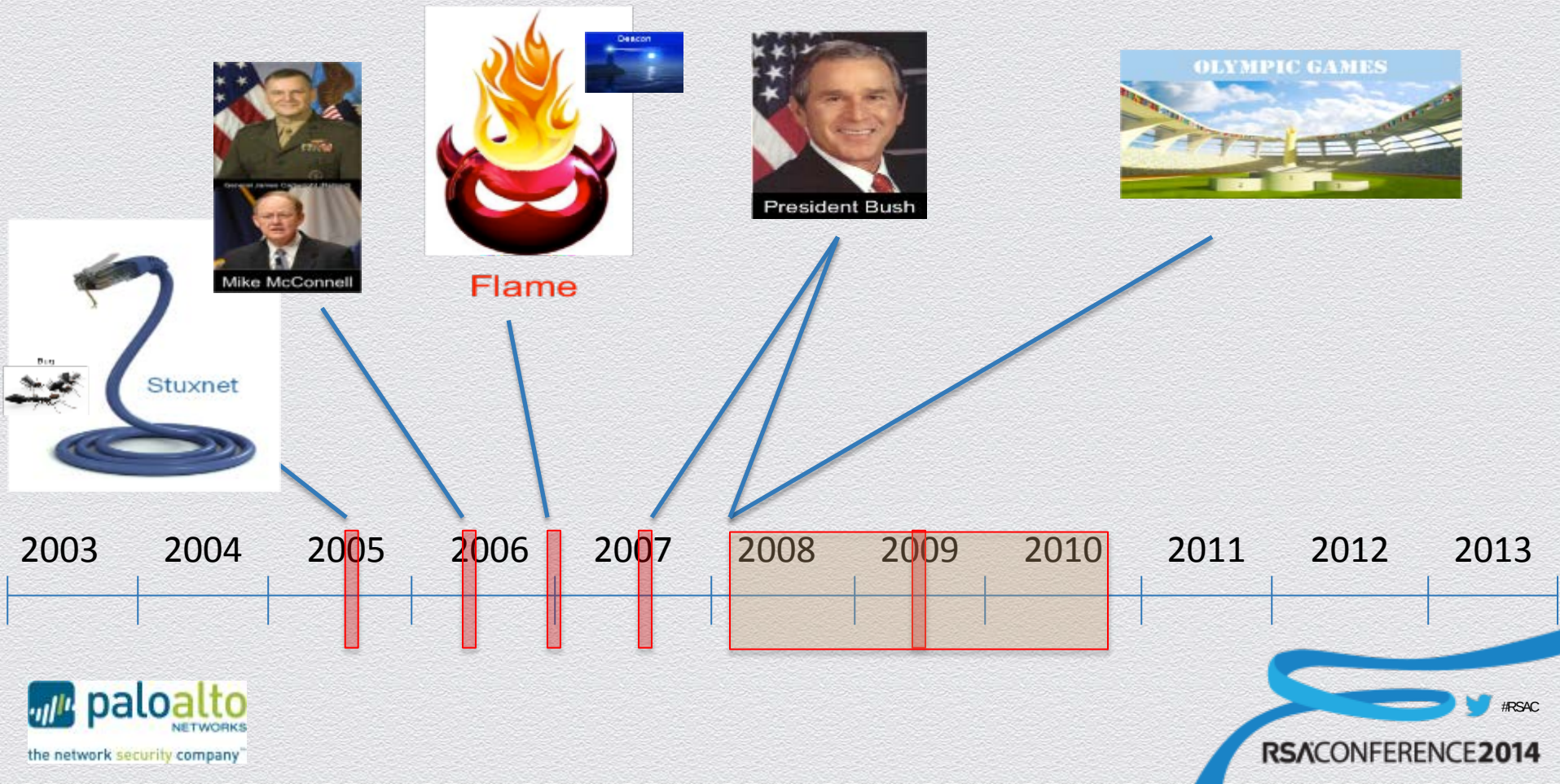
Olympic Games: The Sophistication of Stuxnet



ADVANCED
PLANNING &
EXECUTION



Olympic Games: The Sophistication of Stuxnet



Olympic Games: The Sophistication of Stuxnet

P1 centrifuges at Natanz



Iranian President
Mahmoud Ahmadinejad

Originally published by EurasiaNet.org: 2008



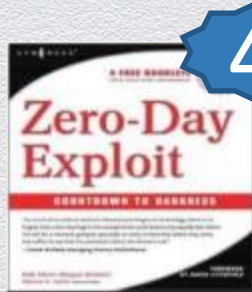
P₁



NEGEV DESERT



Olympic Games: The Sophistication of Stuxnet



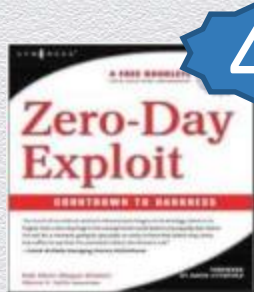
4

Price Range: \$5,000 to \$250,000 each

Olympic Games Price Range:
\$20,000 to \$1 Mil



Olympic Games: The Sophistication of Stuxnet



4

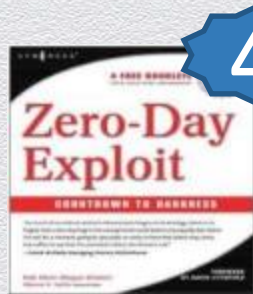
Price Range: \$5,000 to \$250,000 each

Olympic Games Price Range:
\$20,000 to \$1 Mil

Does Not Include the Cost of



Olympic Games: The Sophistication of Stuxnet



4

Price Range: \$5,000 to \$250,000 each

Olympic Games Price Range:
\$20,000 to \$1 Mil

Does Not Include the Cost of



DELAY & DEGRADE

Olympic Games: The Sophistication of Stuxnet

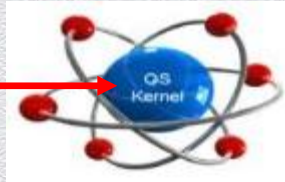
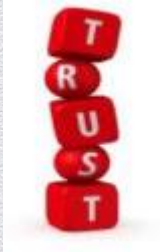
New Tech



Olympic Games: The Sophistication of Stuxnet



Driver Signing



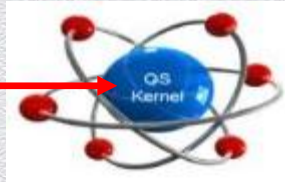
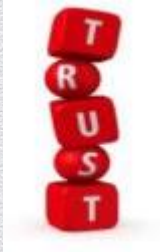
New Tech



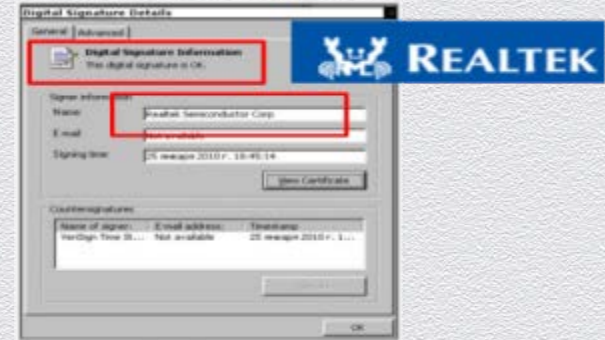
Olympic Games: The Sophistication of Stuxnet



Driver Signing



REALTEK



Source: Dennis Fisher - Kaspersky, July 2010



Source: Costin Raiu - Kaspersky, July 2010

JMicron

New Tech



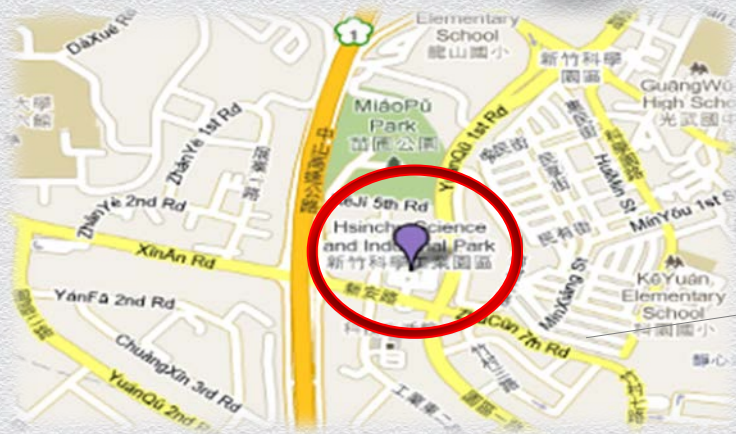
Olympic Games: The Sophistication of Stuxnet

Innovation Road, Hsinchu Science Park, Hsinchu, Taiwan

Realtek Semiconductor Corp. (瑞昱半導體股份有限公司)



JMicron (智微有限公司)



Source: Google Maps



Source: Wolfram Alpha

Olympic Games: The Sophistication of Stuxnet



SIEMENS

Industrial Control Systems (ICS)



Targeted SCADA



Olympic Games: The Sophistication of Stuxnet



SIEMENS

Industrial Control Systems (ICS)



Targeted SCADA

High Precision



Centrifuge

807 Hz and 1210 Hz



RSACONFERENCE2014

Olympic Games: The Sophistication of Stuxnet



SIEMENS

Industrial Control Systems (ICS)



High Precision



Centrifuge

807 Hz and 1210 Hz



Olympic Games: The Sophistication of Stuxnet

High Precision



Centrifuge

807 Hz and 1210 Hz



Olympic Games: The Sophistication of Stuxnet

Enriched



High Precision



Centrifuge

807 Hz and 1210 Hz



SIEMENS

Industrial Control Systems (ICS)



Weeks

Source: Symantec Feb 2011



RSACONFERENCE2014

Olympic Games: The Sophistication of Stuxnet

Enriched



1400 Hz



High Precision



Centrifuge

807 Hz and 1210 Hz



SIEMENS

Industrial Control Systems (ICS)



Olympic Games: The Sophistication of Stuxnet

Enriched



1400 Hz
2 Hz

High Precision



Centrifuge

807 Hz and 1210 Hz



SIEMENS

Industrial Control Systems (ICS)



Olympic Games: The Sophistication of Stuxnet

Enriched



1400 Hz
2 Hz

High Precision



Centrifuge

807 Hz and 1210 Hz



SIEMENS

Industrial Control Systems (ICS)



Olympic Games: The Sophistication of Stuxnet



2 Hz

1400 Hz

High Precision



807 Hz and 1210 Hz



Olympic Games: The Sophistication of Stuxnet

High Precision



Centrifuge

807 Hz and 1210 Hz

1400 Hz
2 Hz



SIEMENS

Industrial Control Systems (ICS)

Olympic Games: The Story



P₁

P1 centrifuges at Natanz



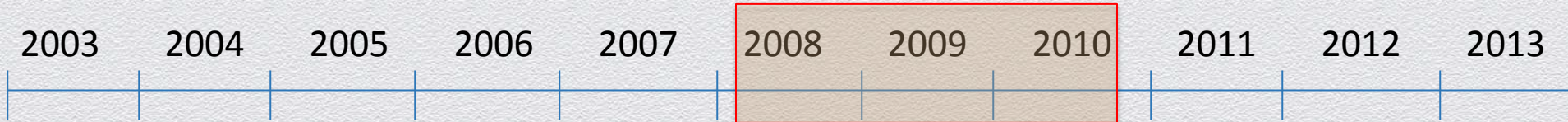
Iranian President
Mahmoud Ahmadinejad

Originally published by EurasiaNet.org: 2008



But Not Uniformly

1000 Centrifuges Dismantled



Olympic Games: The Story



P₁

P1 centrifuges at Natanz



Iranian President
Mahmoud Ahmadinejad

Originally published by EurasiaNet.org: 2008



But Not Uniformly



1000 Centrifuges Dismantled



Olympic Games: Swinging for the Fences



Olympic Games: Swinging for the Fences



Olympic Games: Swinging for the Fences



Flame



1000



Olympic Games: Swinging for the Fences



Olympic Games: Swinging for the Fences



½ of all 9,000 Centrifuges are idle



Olympic Games: Swinging for the Fences



E S C A P E S



Olympic Games: Swinging for the Fences



E S C A P E S

SIEMENS

Industrial Control Systems (ICS)



Olympic Games: Swinging for the Fences



E S C A P E S

SIEMENS

Industrial Control Systems (ICS)



Olympic Games: The First Cyber Skirmish

Olympic Games: The First Cyber Skirmish



Olympic Games: The First Cyber Skirmish

Windows Server 2008

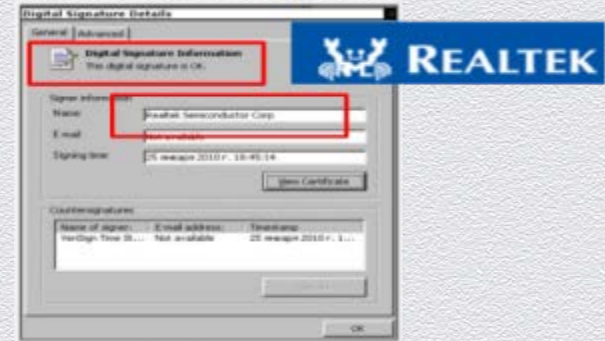
Driver Signing



6 Days



REALTEK

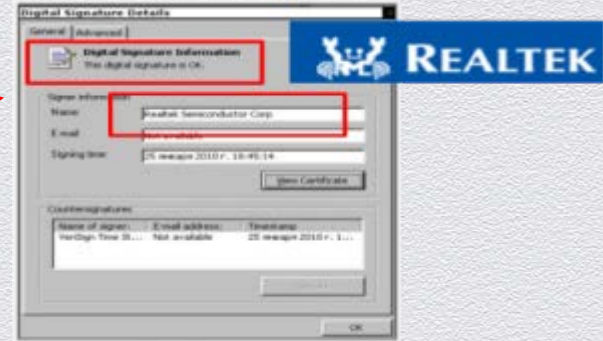


Source: Dennis Fisher - Kaspersky, July 2010

Punch – Counterpunch

2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013

Olympic Games: The First Cyber Skirmish



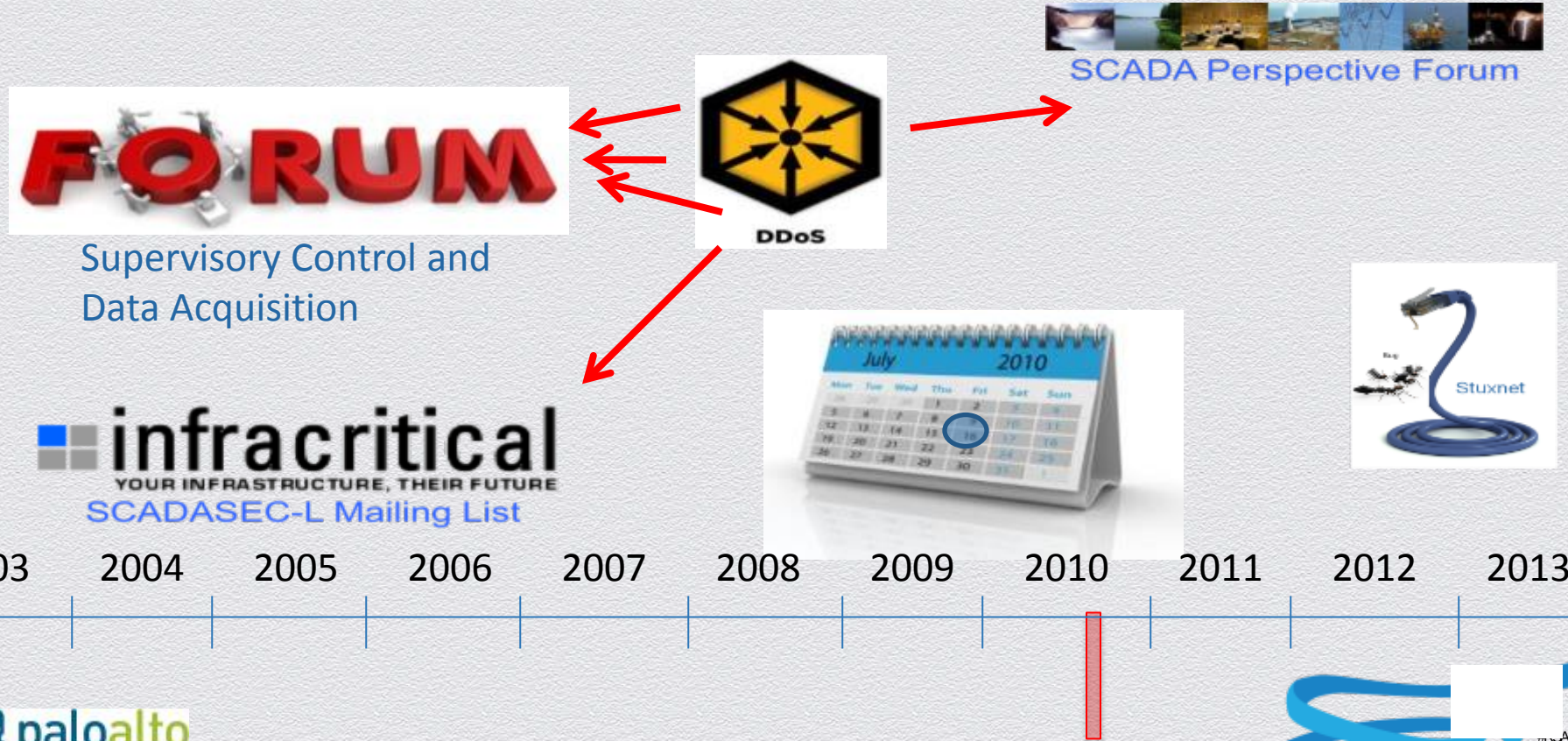
Source: Dennis Fisher - Kaspersky, July 2010



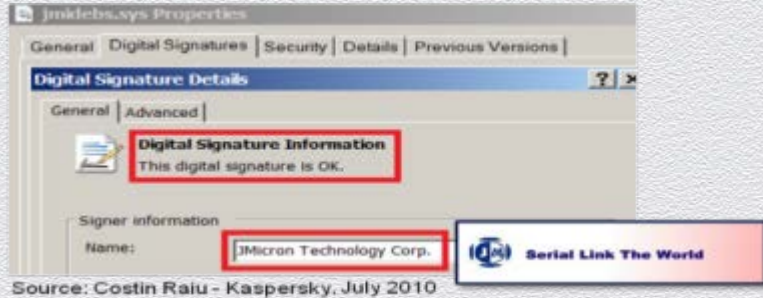
Source: Symantec Feb 2011



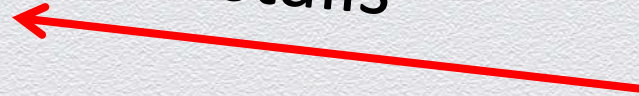
Olympic Games: The First Cyber Skirmish



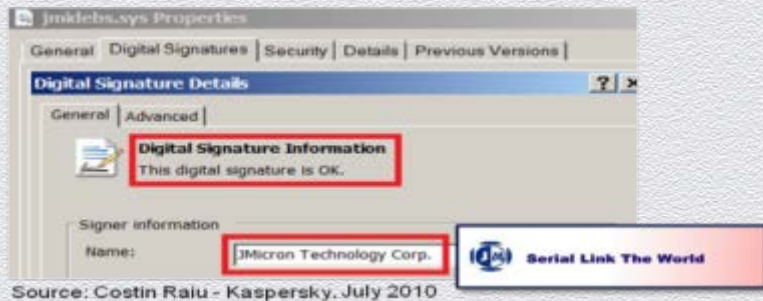
Olympic Games: The First Cyber Skirmish



Installs



Olympic Games: The First Cyber Skirmish

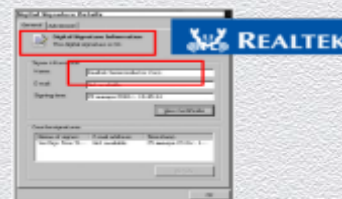


Olympic Games: The First Cyber Skirmish

SKIRMISH



Source: Gordon Hahn, Kaspersky, July 2010



Source: Dennis Fisher, Kaspersky, July 2010

The Battle for the Driver Certificates

Olympic Games: Then Endgame - Assassination



30,000 Iranian Computers infected



Olympic Games: Then Endgame - Assassination



30,000 Iranian Computers infected



½ of all 9,000 Centrifuges are idle



Olympic Games: Then Endgame - Assassination



Enriched



Olympic Games: Then Endgame - Assassination

Enriched



6 Days Later

Source: The Economist Dec 16 2010

Olympic Games: Then Endgame - Assassination

Enriched



6 Days Later

Olympic Games: Then Endgame - Assassination

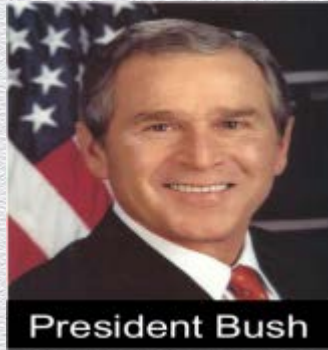


DELAY & DEGRADE

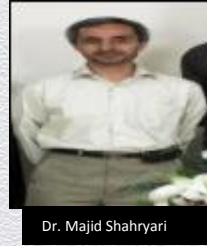
Enriched



Olympic Games: Then Endgame - Assassination



Olympic Games: Then Endgame - Assassination



Dr. Majid Shahryari



Dr. Fereidun Abbasi



9 Days Later

Source: NYT Nov 29 2010

Olympic Games: Then Endgame - Assassination



Olympic Games: Then Endgame - Assassination



Source: Crethi Plethi Blog

<http://www.crethiplethi.com/ahmadmjad-shahryari-for-assassination-of-iranian-academics/sahnic-court/res/iran-islamic-countries/2010/>



Source: CNN

<http://www.iranian.com/main/2010/nov/majid-shahriari>



Olympic Games: Then Endgame - Assassination

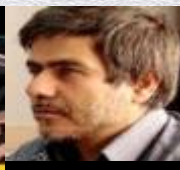


Dr. Majid Shahryari

Assassinated

Source: Crethi Plethi Blog

<http://www.crethiplethi.com/ahmadmjad-shahryari-for-assassination-of-iranian-academics/sahnic-counters/iran-islamic-countries/2010/>



Dr. Fereidun Abbasi

Source: CNN

<http://www.iranian.com/main/2010/nov/majid-shahriari>



Olympic Games: Then Endgame - Assassination



Dr. Majid Shahryari

Assassinated

Source: Crethi Plethi Blog

<http://www.crethiplethi.com/ahmadmjad-shahryari-for-assassination-of-iranian-academics/sahnic-counters/iran-islamic-countries/2010/>



Dr. Fereidun Abbasi

Assassination Attempt

Source: CNN

<http://www.iranian.com/main/2010/nov/majid-shahriari>



Olympic Games: Then Endgame - Assassination



**Masoud
Mohammadi**
Assassinated
January 2010



**Majid
Shahryari**
Assassinated
November 2010



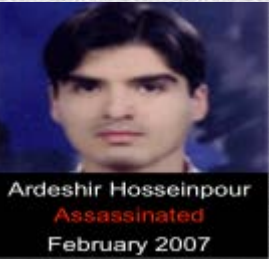
**Fereidun
Abbasi**
**Assassination
Attempt**
November 2010



**Darioush
Rezaeinejad**
Assassinated
July 2011

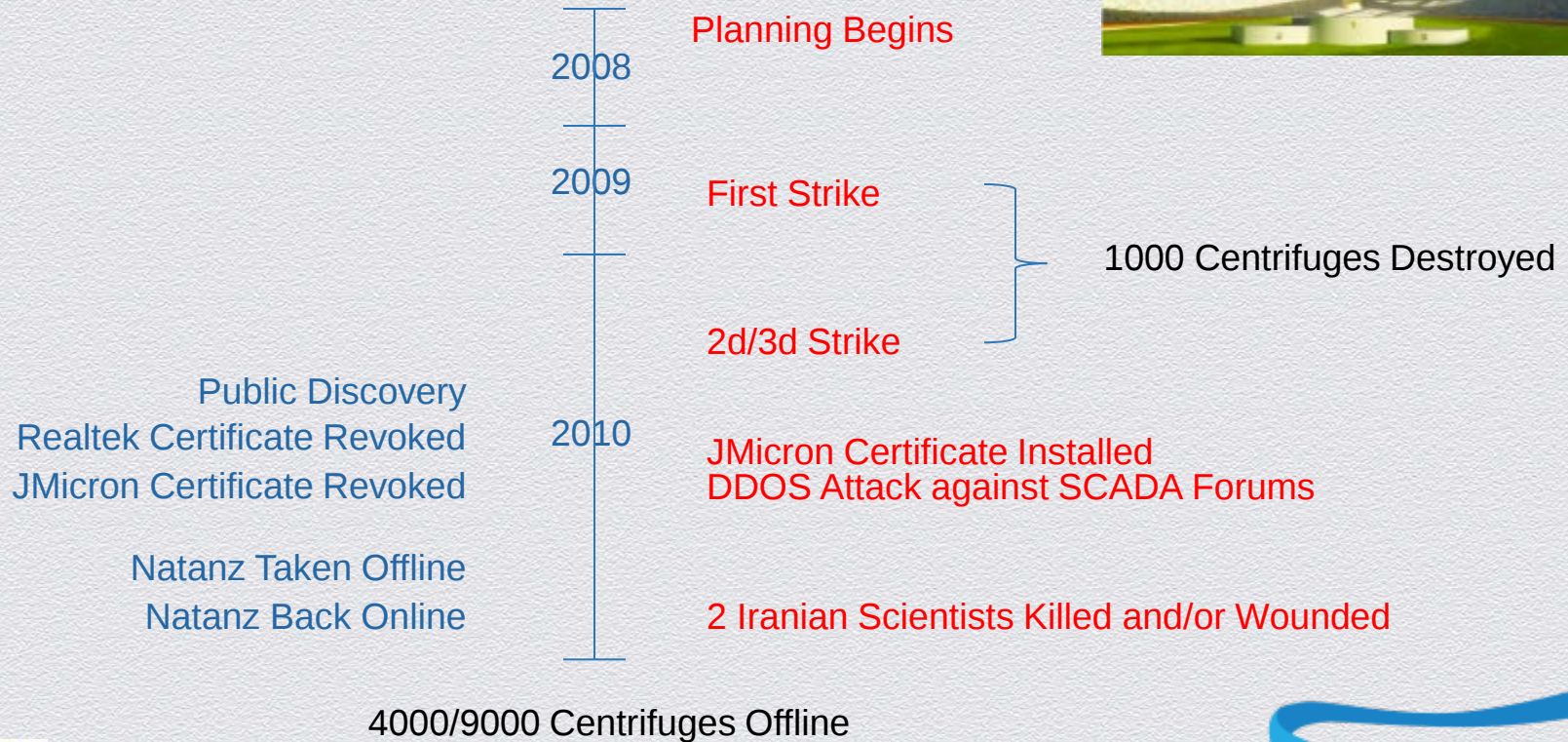


**Mostafa
Ahmadi-
Roshan**
Assassinated
January 2012



Ardeshir Hosseinpour
Assassinated
February 2007

Olympic Games: The Campaign Plan



Olympic Games: Assessment



Nuclear Program Delayed until 2015

No Affect



September 28 2012



Olympic Games: Conclusion

Olympic Games: Conclusion



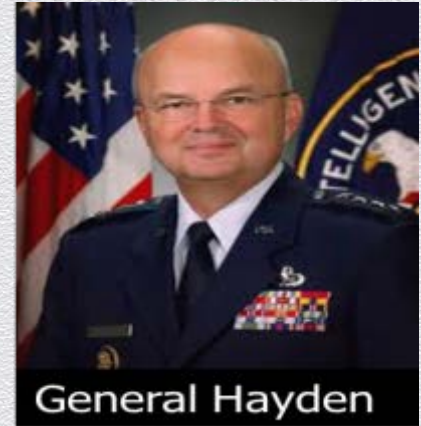
New US Foreign Policy

Olympic Games: Conclusion



New US Foreign Policy

“We Have Crossed the Rubicon ...”



Olympic Games: Conclusion



Olympic Games: Conclusion



Olympic Games: Conclusion



Cyber Warfare involves one or more nation states destroying each other's national treasure to achieve some political purpose.

Olympic Games: Conclusion



Olympic Games: Conclusion



½ of all 9,000 Centrifuges are idle

Olympic Games: Conclusion



½ of all 9,000 Centrifuges are idle

Olympic Games: Conclusion

It is just a matter of time now



$\frac{1}{2}$ of all 9,000 Centrifuges are idle

To Participate

For Further Discussion



twitter: @raceBannon99

email: rhoward@paloaltonetworks.com

Reviews of the Books on My List



<http://researchcenter.paloaltonetworks.com/>



<http://terebrate.blogspot.com/>

To Vote



https://www.surveymonkey.com/s/2014_Cyber_Security_Canon_Survey



RSACONFERENCE**2014**

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

