

# Verisign® iDefense® Cyber Security Trends

Rick Howard, iDefense General Manager  
June 22, 2011



VERISIGN™

# How Technical Are You?



## **Operation Aurora Impact**

## **Stuxnet Impact**

## **Cyber Security Disruptors**

# Learning Points



CYBER ESPIONAGE



CYBER WARFARE



HACKTIVISM



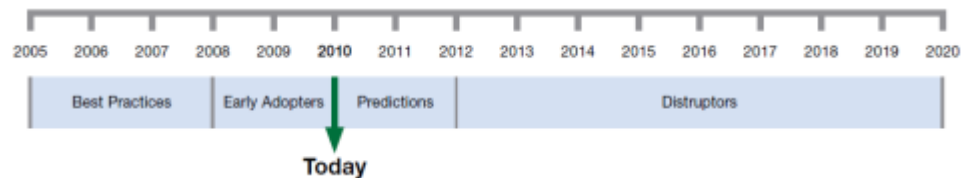
DISRUPTOR

## Game Changer

Theory **Fact**



## DATA LOSS PREVENTION SYSTEMS

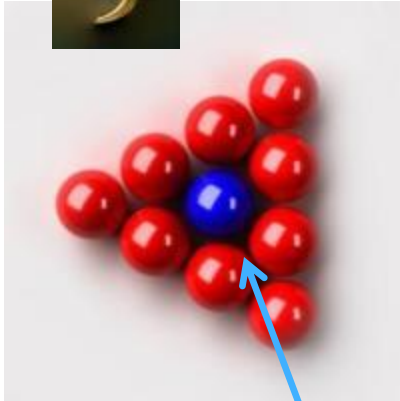


# Operation Aurora Impact

# The Aurora Attacks – 5 Unprecedented Changes



5



# The Aurora Attacks – 5 Unprecedented Changes

1

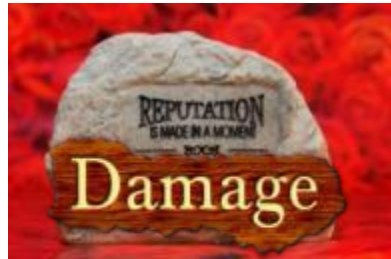
Public Disclosure



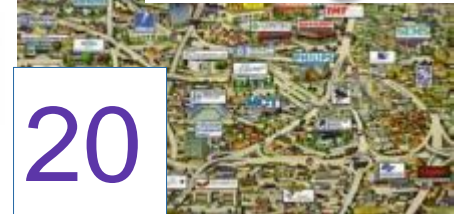
Google™



# The Aurora Attacks – 5 Unprecedented Changes



Public Disclosure



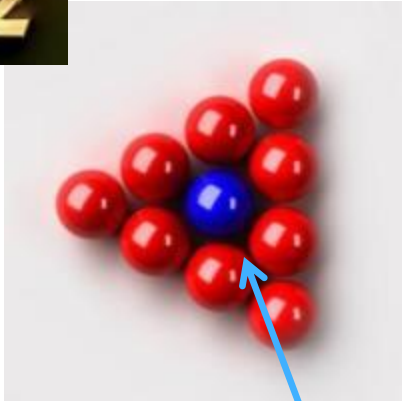


# The Aurora Attacks – 5 Unprecedented Changes



# The Aurora Attacks – 5 Unprecedented Changes

2



# The Aurora Attacks – 5 Unprecedented Changes



# The Aurora Attacks – 5 Unprecedented Changes

"We have been briefed by Google on these allegations, which raise very serious concerns and questions," she said. **We look** to the **Chinese government** for an explanation."

Source: Network World: 13 Jan 2010

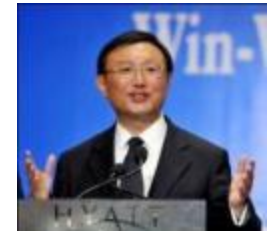


**"We look** to **Chinese authorities** to conduct a thorough investigation of the cyber intrusions that led Google to make this announcement. We also look for that investigation and its results to be transparent."

Source: Washington Times: 21 Jan 2010

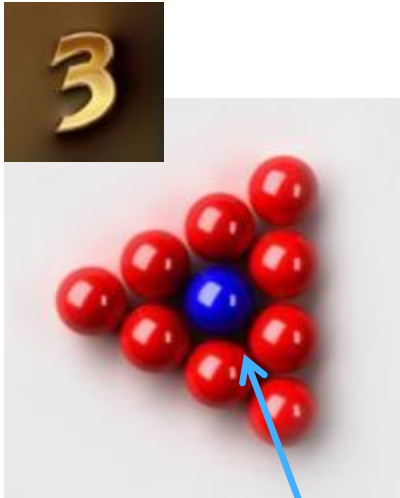
"It was a **very open and candid conversation**. We agreed we would continue this conversation in the context of our ongoing dialogue."

Source: France 24: 28 Jan 2010



**Foreign Minister Yang Jiechi**

# The Aurora Attacks – 5 Unprecedented Changes



# The Aurora Attacks – 5 Unprecedented Changes





# The Aurora Attacks – 5 Unprecedented Changes



# Raytheon

\$100,000,000

Vulnerability Assessment

Capabilities Research

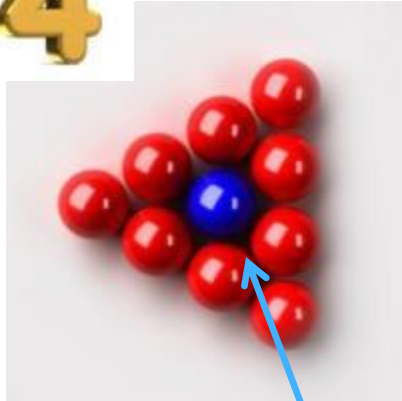


Google

PERFECT CITIZEN

# The Aurora Attacks – 5 Unprecedented Changes

4





# The Aurora Attacks – 5 Unprecedented Changes



Moonlight Maze



Byzantine Hades



Titan Rain



# The Aurora Attacks – 5 Unprecedented Changes

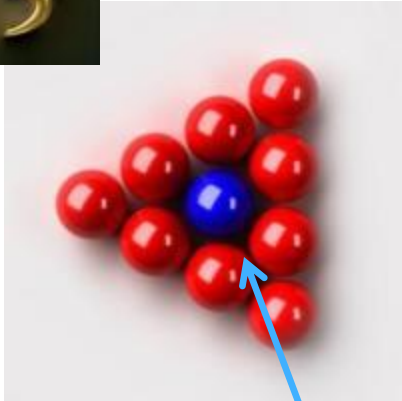


2010 Top Security Concerns



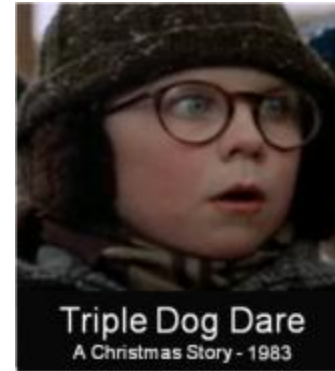
# The Aurora Attacks – 5 Unprecedented Changes

5



# The Aurora Attacks – 5 Unprecedented Changes

**CONFIDENCE IS HIGH**



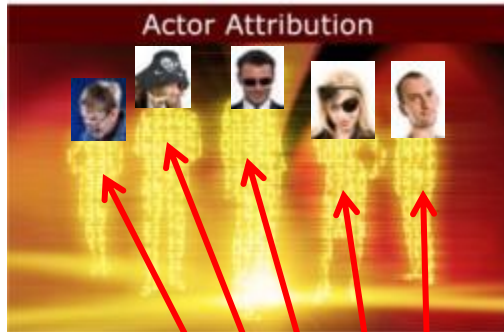
Is Hard ...

But not Impossible



# The Aurora Attacks – 5 Unprecedented Changes

**CONFIDENCE IS HIGH**



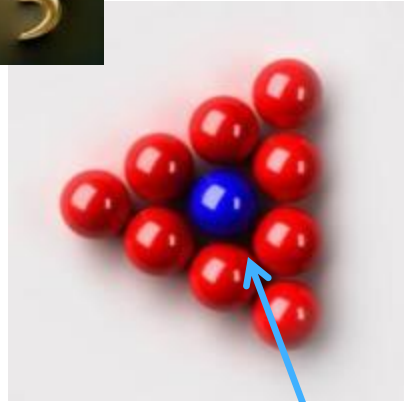
Is Hard ...

But not Impossible



# The Aurora Attacks – 5 Unprecedented Changes

5



1



## Game Changer

2

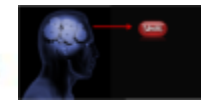


3



PERFECT CITIZEN

4



CYBER ESPIONAGE



## Operation Aurora

5



VERISIGN

# Stuxnet Impact



# The Stuxnet Attacks



# SIEMENS

Industrial Control Systems (ICS)



Supervisory Control and Data Acquisition

SCADA ATTACK

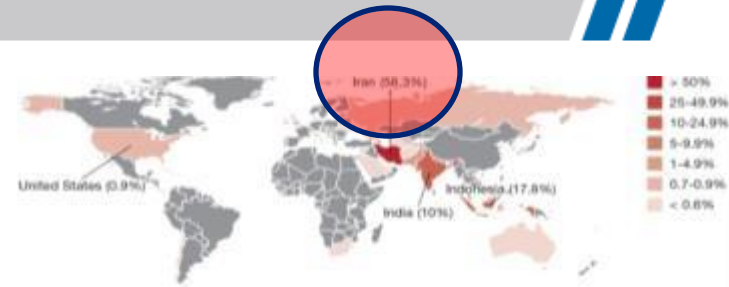




# The Stuxnet Attacks



# The Stuxnet Attacks



Data from W 32.Stuxnet Dossier





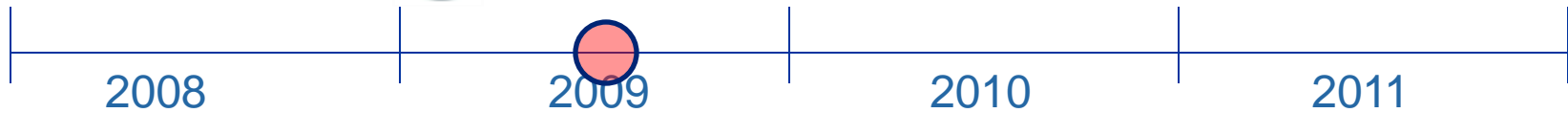
# Stuxnet Timeline



**NATANZ, IRAN – SITE OVERVIEW**  
INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY      Source: CNN, Associated Press  
Date of Issue: 06 Feb 2011  
THE NATANZ SITE IS A POTENTIAL URANIUM ENRICHMENT FACILITY, POSSIBLY A GAS CENTRIFUGE SITE. IT IS LOCATED APPROXIMATELY 100 KILOMETERS SOUTH OF TEHRAN.



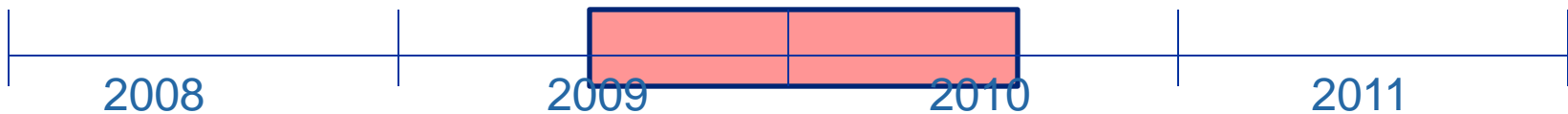
First Strike



# Stuxnet Timeline



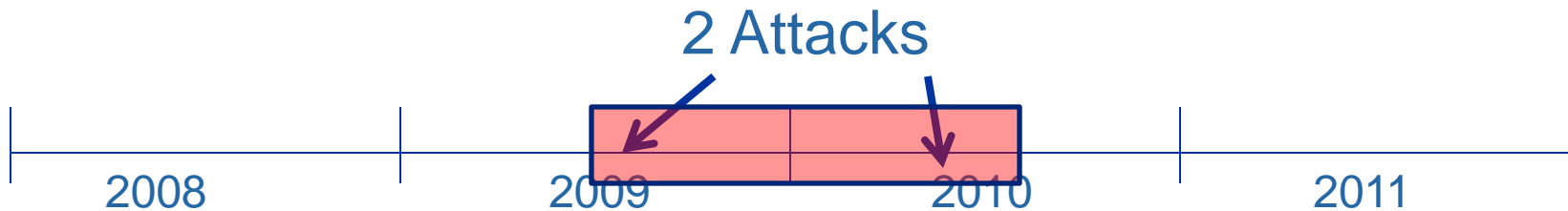
## 1000 Centrifuges Dismantled



# Stuxnet Timeline



## 1000 Centrifuges Dismantled



# The Stuxnet Attacks



Speculation

Theory

Proof of Concept

2007



2008



# The Stuxnet Attacks



CYBER  
WARFARE

## Speculation

## Theory

## Proof of Concept

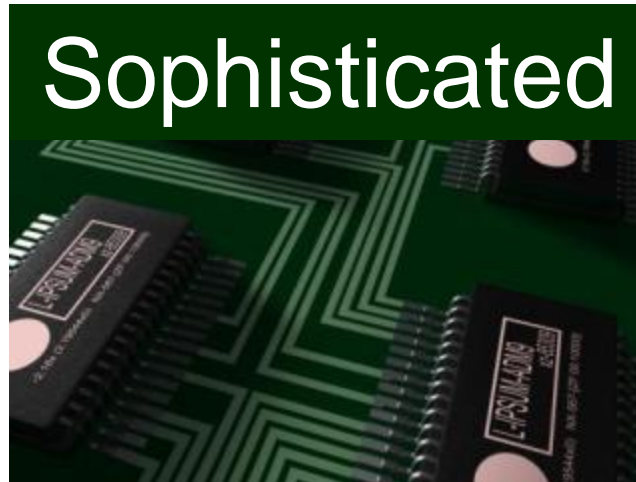
2007



# The Stuxnet Attacks



CYBER  
WARFARE



**Real**

**Compared to What?**

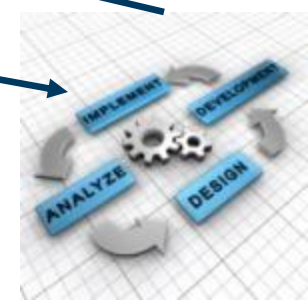
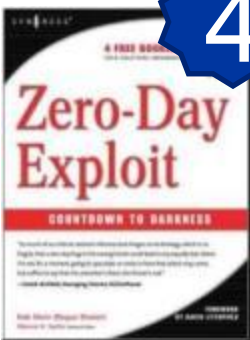




# The Stuxnet Attacks – Why Sophisticated?

1

4



\$400K – \$1.5 MIL



Well Financed



# The Stuxnet Attacks – Why Sophisticated?

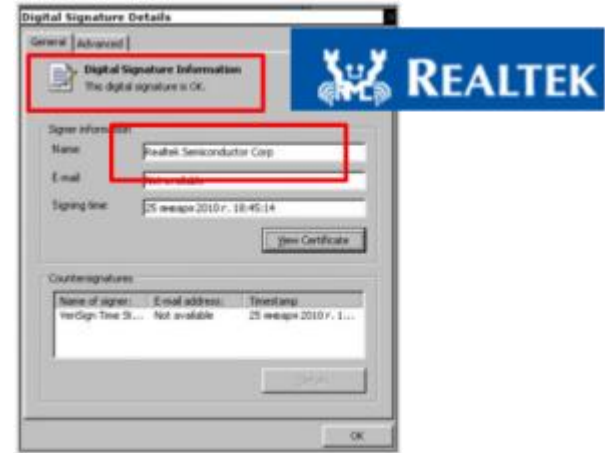
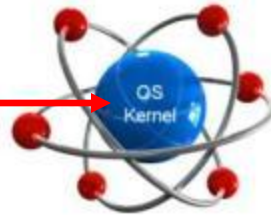
2

Windows Server 2008

Driver Signing

Windows Vista

T  
R  
U  
S  
T



Source: Dennis Fisher - Kaspersky, July 2010



# The Stuxnet Attacks – Why Sophisticated?

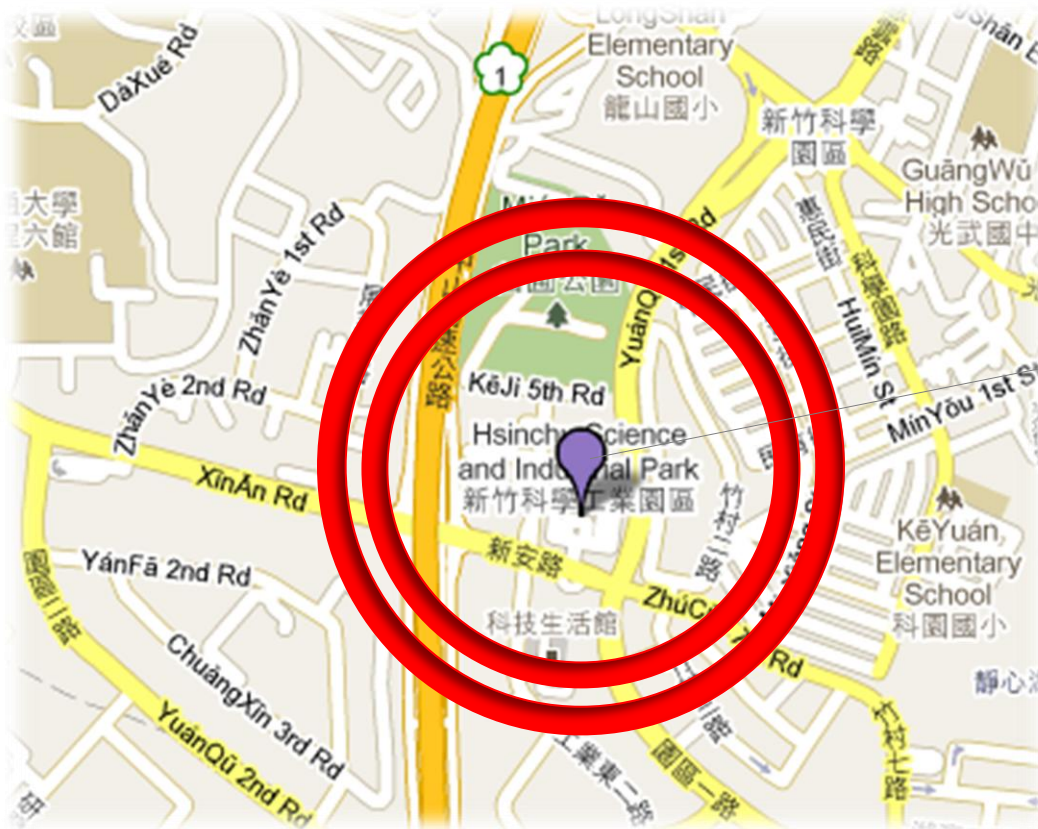
Realtek Semiconductor Corp. (瑞昱半導體股份有限公司)



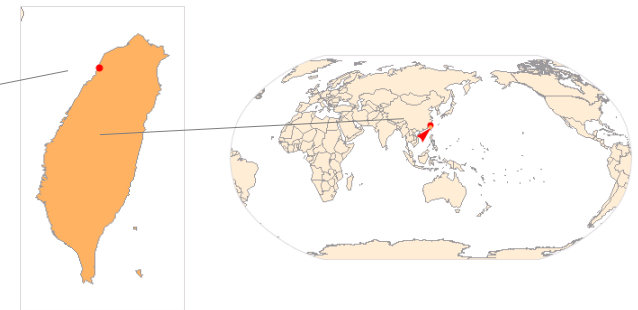
JMicron (智微有限公司)



Innovation Road, Hsinchu Science Park, Hsinchu, Taiwan



Source: Google Maps



Source: Wolfram Alpha

# The Stuxnet Attacks – Why Sophisticated?

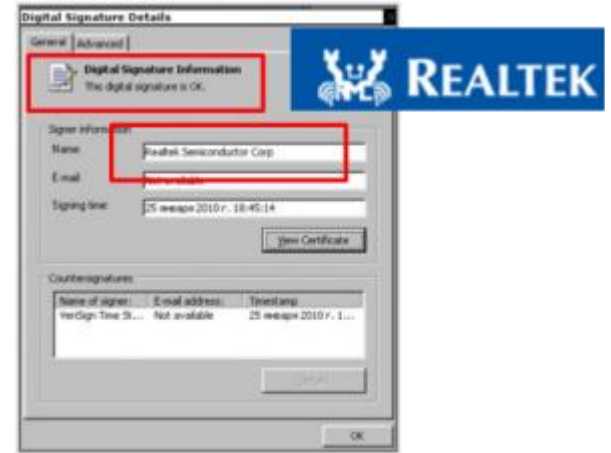
2



Microsoft

VeriSign

CANCELLED



Source: [Dennis Fisher](#) - Kaspersky, July 2010



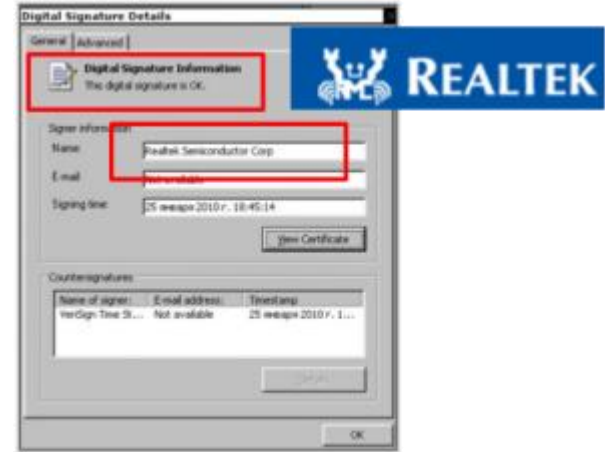
Source: [Costin Raiu](#) - Kaspersky, July 2010



# The Stuxnet Attacks – Why Sophisticated?

2

New Trend in 2010



Source: [Dennis Fisher](#) - Kaspersky, July 2010



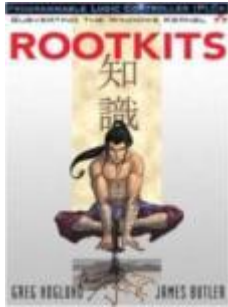
Source: [Costin Raiu](#) - Kaspersky, July 2010





# The Stuxnet Attacks – Why Sophisticated?

3



Enriched



Centrifuge

807 Hz and 1210 Hz



90%



# SIEMENS

Industrial Control Systems (ICS)



# The Stuxnet Attacks – Why Sophisticated?

3



1400 Hz



Centrifuge



2 Hz

807 Hz and 1210 Hz



# SIEMENS

Industrial Control Systems (ICS)



# The Stuxnet Attacks – Why Sophisticated?

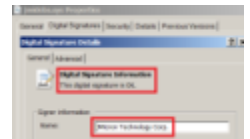


1



2

Driver Signing



3



SCADA ATTACK





# Stuxnet Timeline



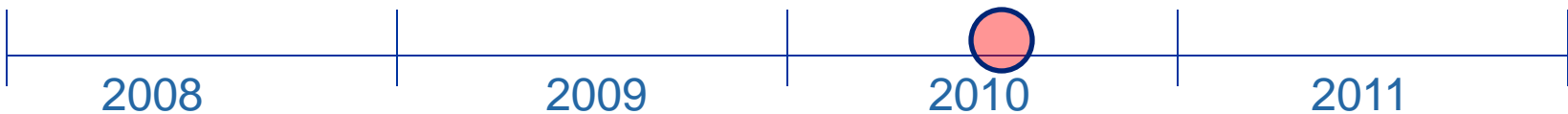
# SIEMENS

Industrial Control Systems (ICS)



SCADA ATTACK

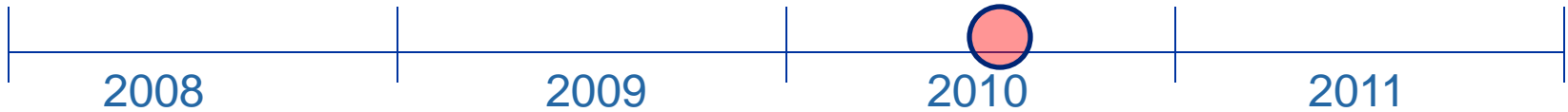
Supervisory Control  
and Data Acquisition



# Stuxnet Timeline



Source: Dennis Fisher - Kaspersky, July 2010



# Stuxnet Timeline



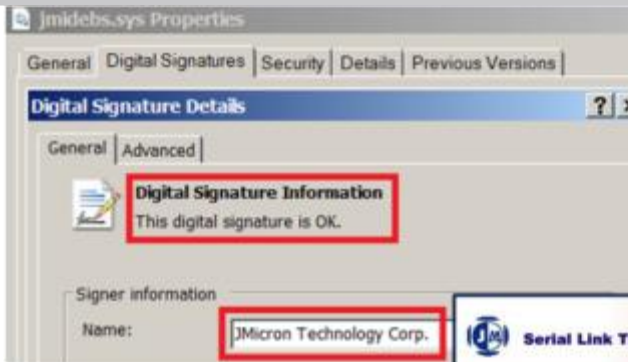
Installs



# Stuxnet Timeline



# Stuxnet Timeline



Source: Costin Raiu - Kaspersky, July 2010



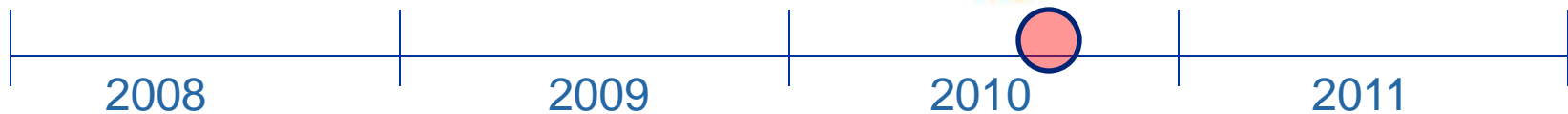
# Stuxnet Timeline



30,000 Iranian Computers infected

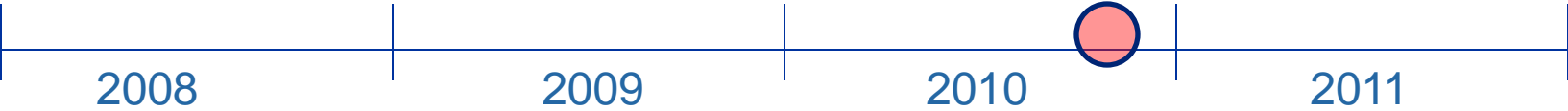


1/2 of all Centrifuges are idle



# Stuxnet Timeline

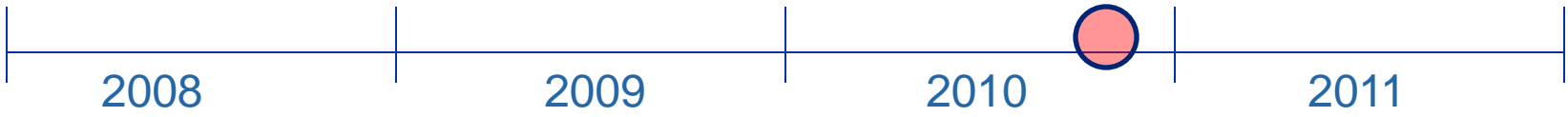
Enriched





# Stuxnet Timeline

Enriched





# Stuxnet Timeline

## Assassinated



Source: Crethi Plethi Blog

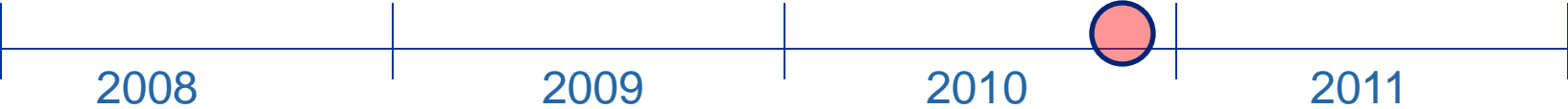
<http://www.crethi-plethi.com/abandoned4-buses-were-and-trial-for-assassination-of-iranian-academic-hijack-computer-virus-stuxnet-iran-islamic-courtesy2010>



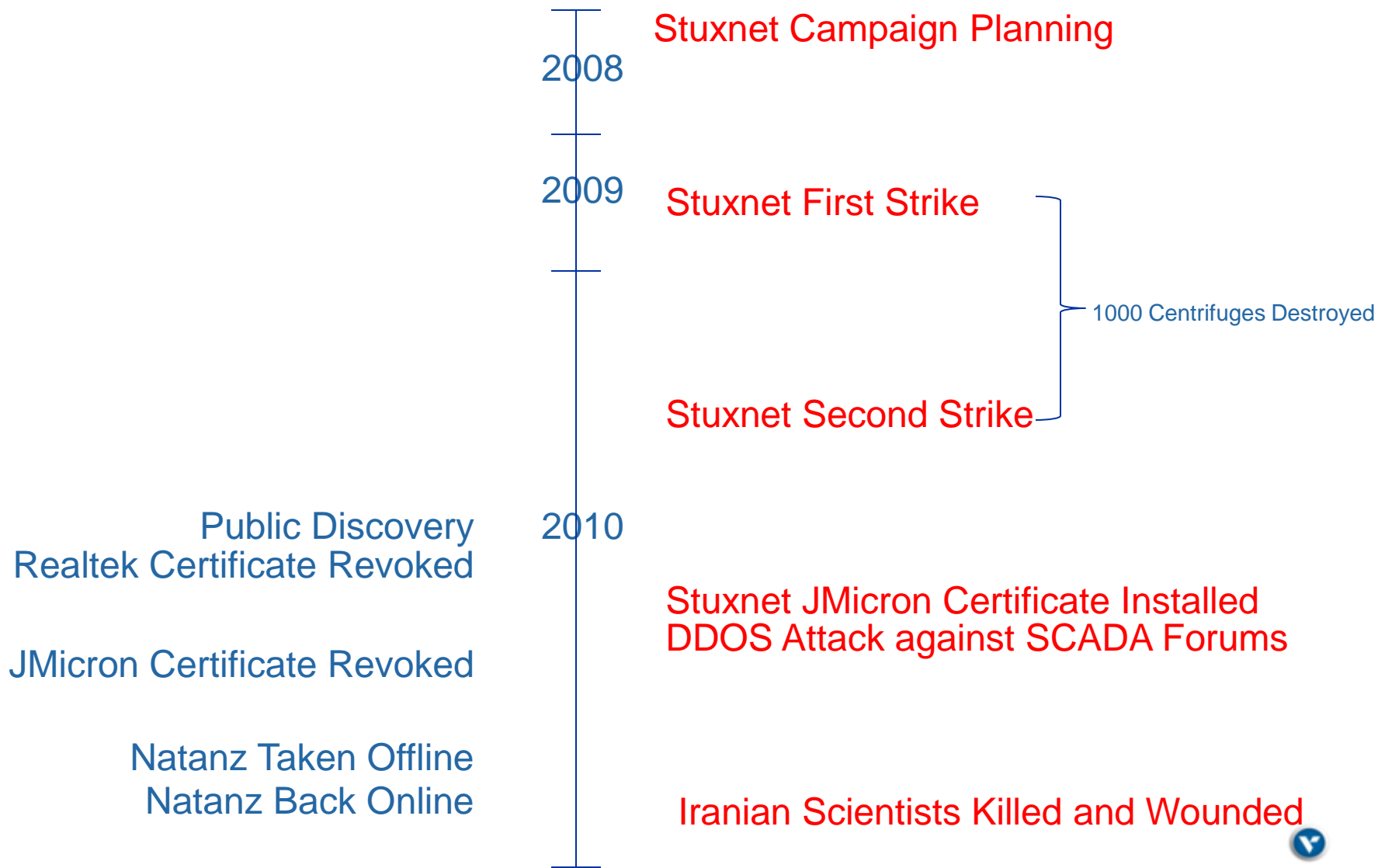
## Assassination Attempt

Source: CNN

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



# Stuxnet Campaign



VERISIGN

# Stuxnet Assessment



US Sec of State  
Mrs. Hillary Clinton



Meir Dagan  
Israeli Retired Chief  
Mossad Intelligence Service

## Nuclear Program Delayed until 2015



No Affect

 **ISIS** INSTITUTE FOR SCIENCE AND  
INTERNATIONAL SECURITY

# The Stuxnet Attacks – What about Them?



**CYBER  
WARFARE**

Theory **Fact**



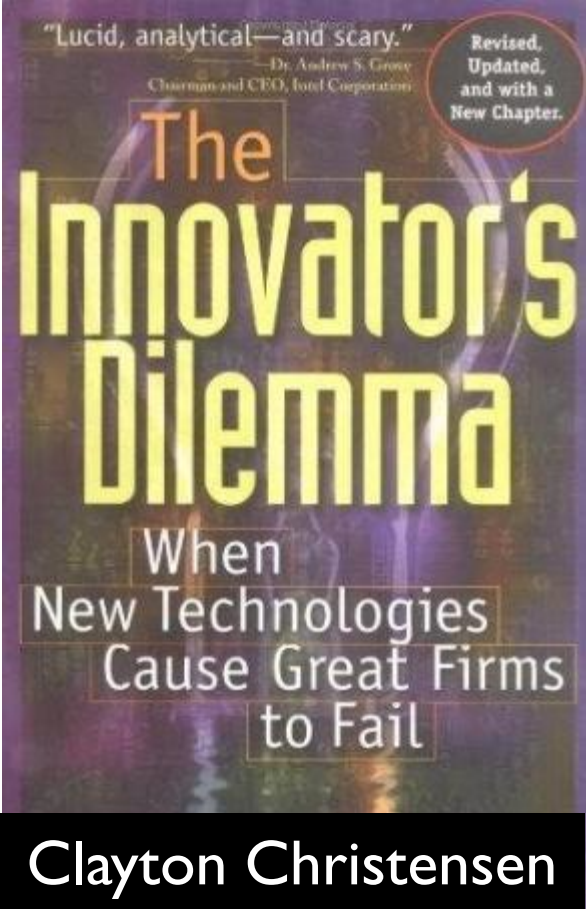
**SCADA ATTACK**



**REFRESHING**

# Cyber Security Disruptors

# What is a Cyber Security Disruptor?



1997

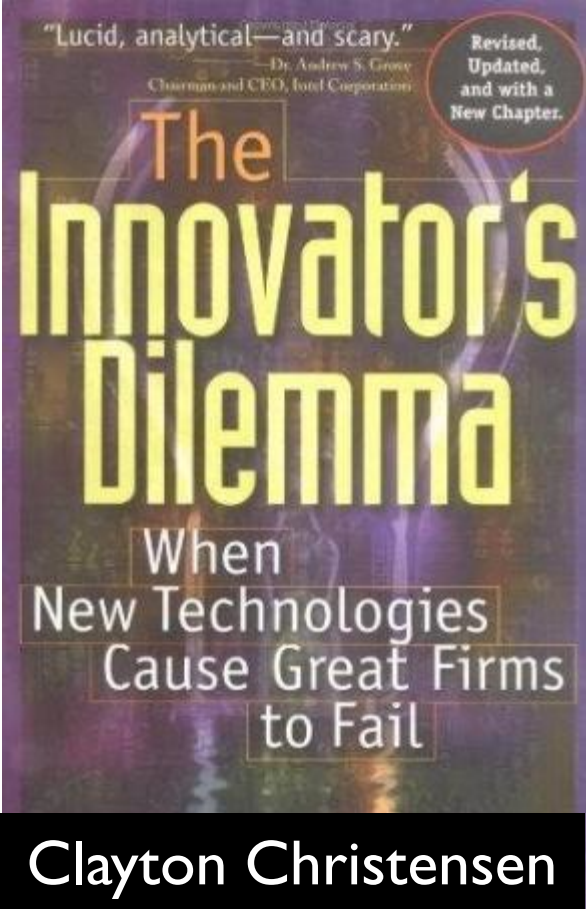


Theory





# What is a Cyber Security Disruptor?



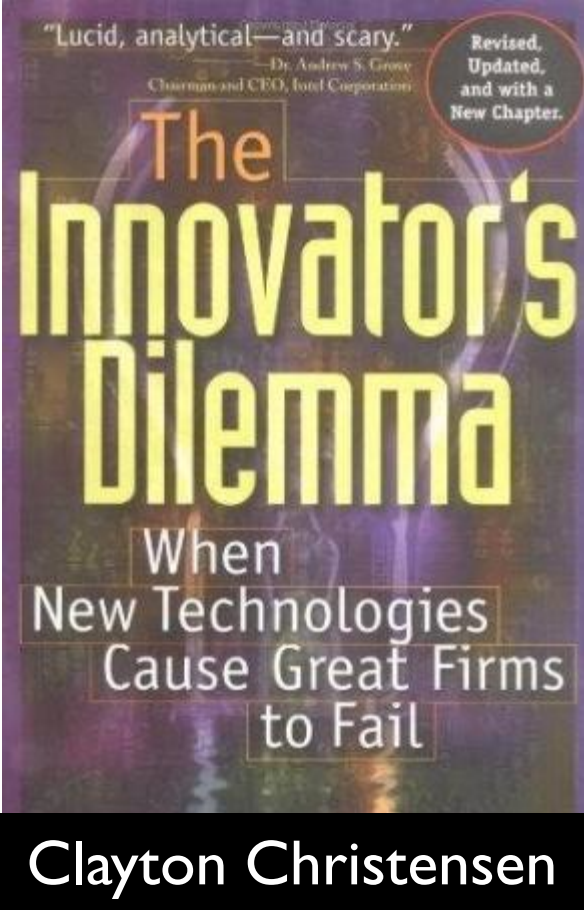
Innovation



Business Failure



# What is a Cyber Security Disruptor?



Innovation

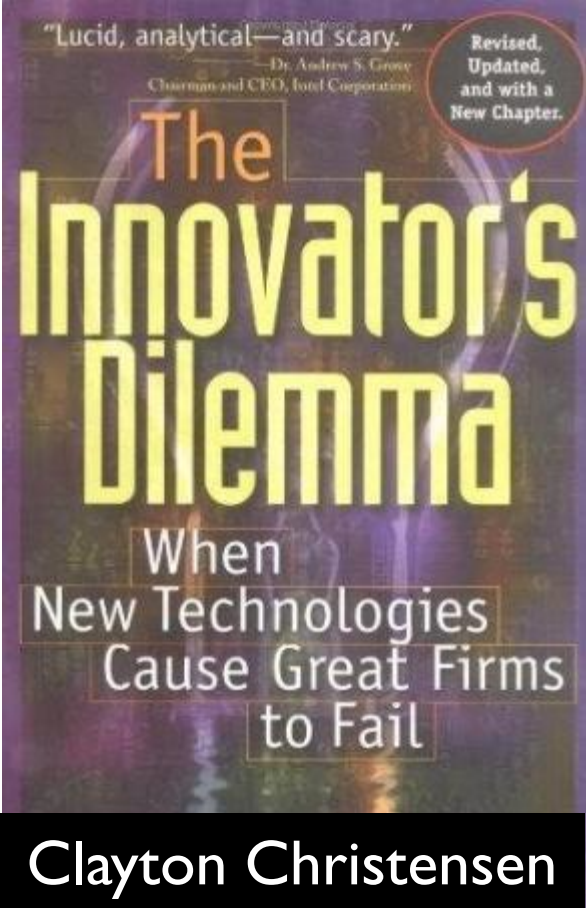


Catalysts

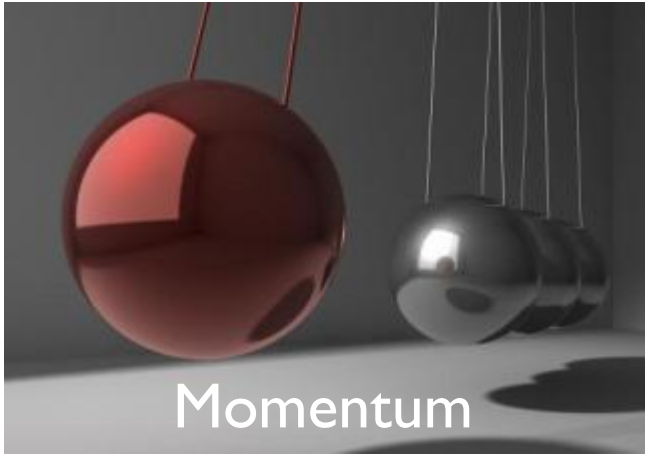




# What is a Cyber Security Disruptor?

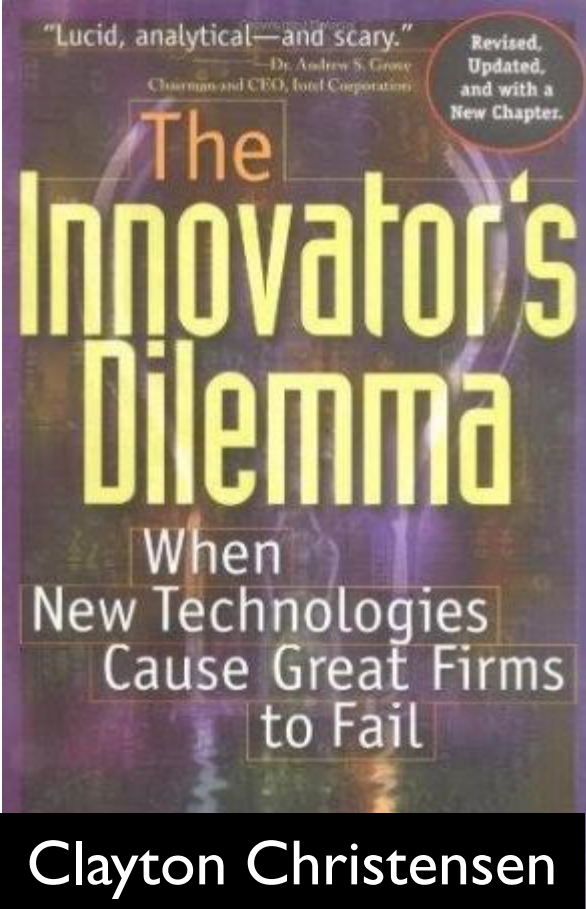


Innovation



Momentum

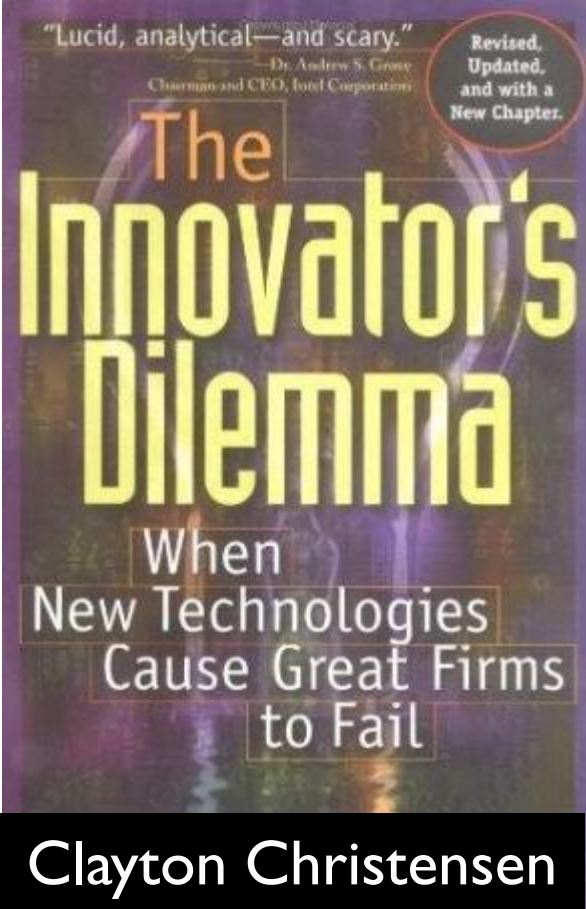
# What is a Cyber Security Disruptor?



Innovation

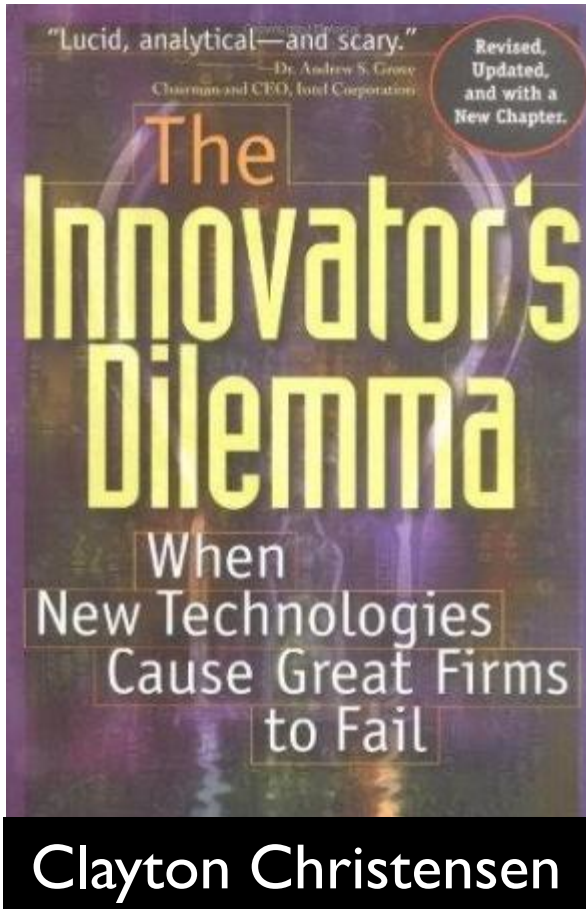


# What is a Cyber Security Disruptor?



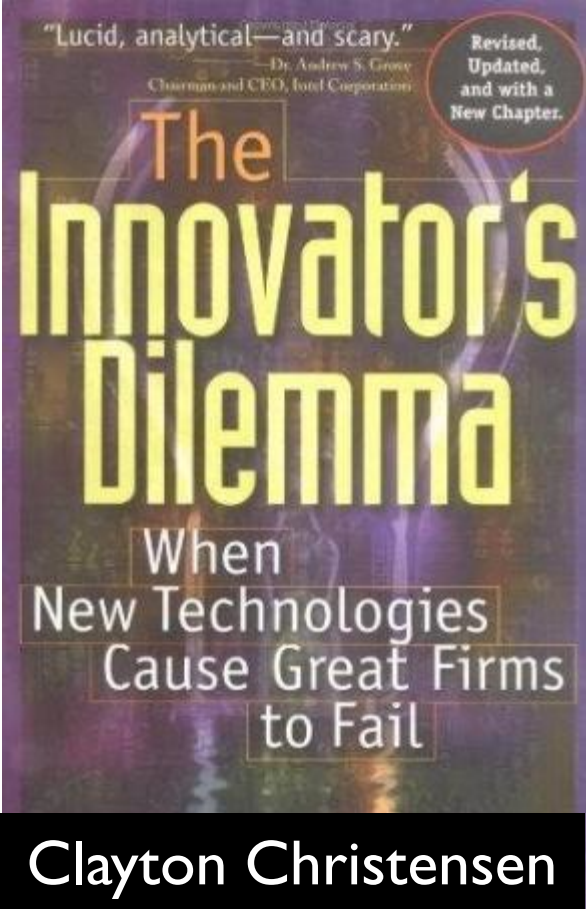
1990s

# What is a Cyber Security Disruptor?





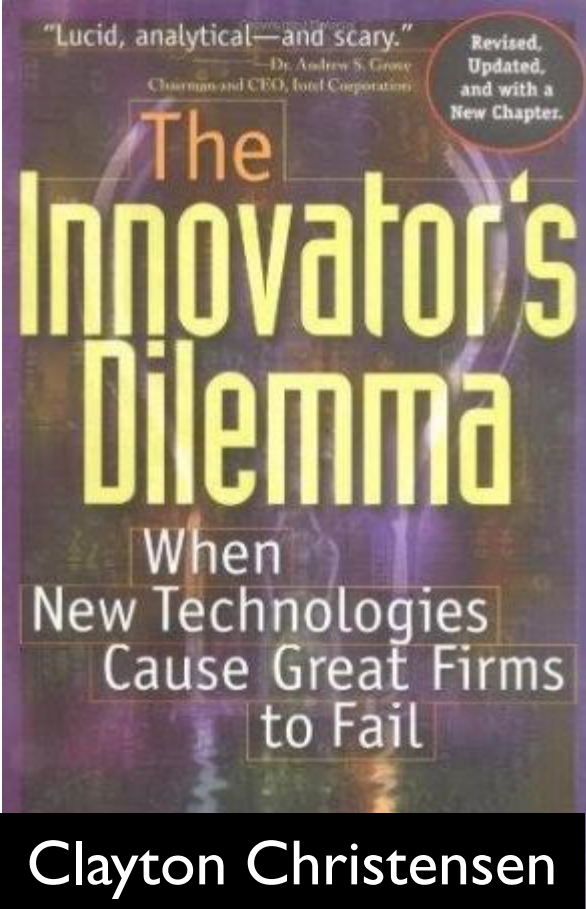
# What is a Cyber Security Disruptor?



**THE LITTLE TRAMP**



# What is a Cyber Security Disruptor?



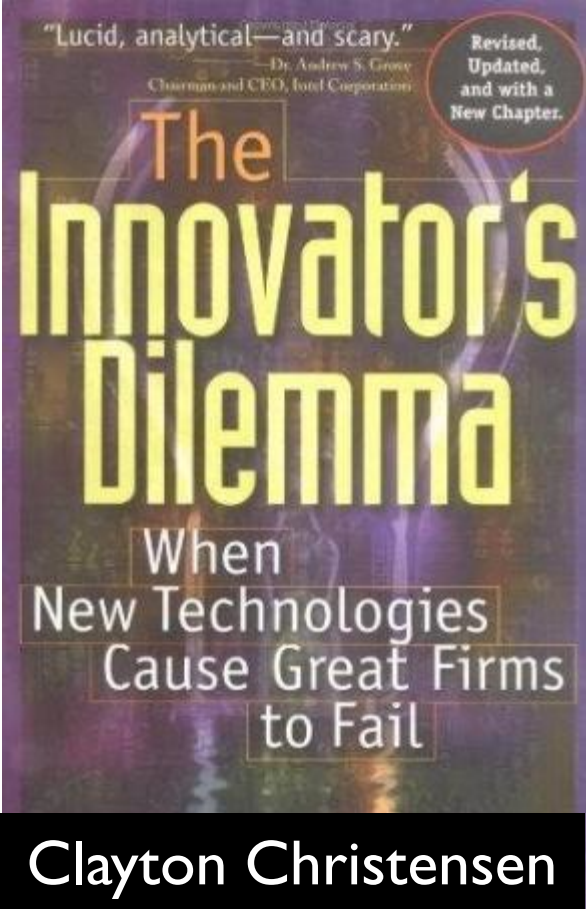
**DOMINANT**



High End



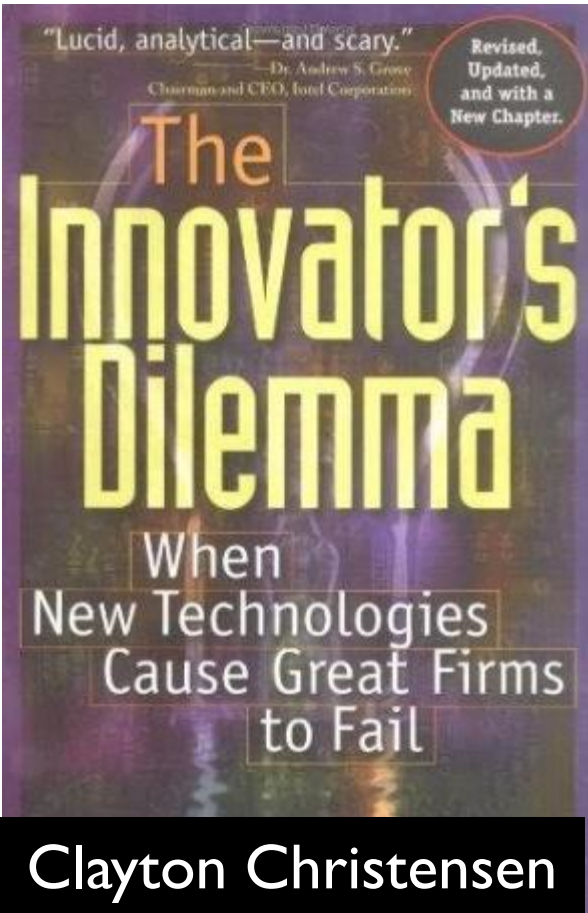
# What is a Cyber Security Disruptor?



Commercial-off-the-shelf



# What is a Cyber Security Disruptor?

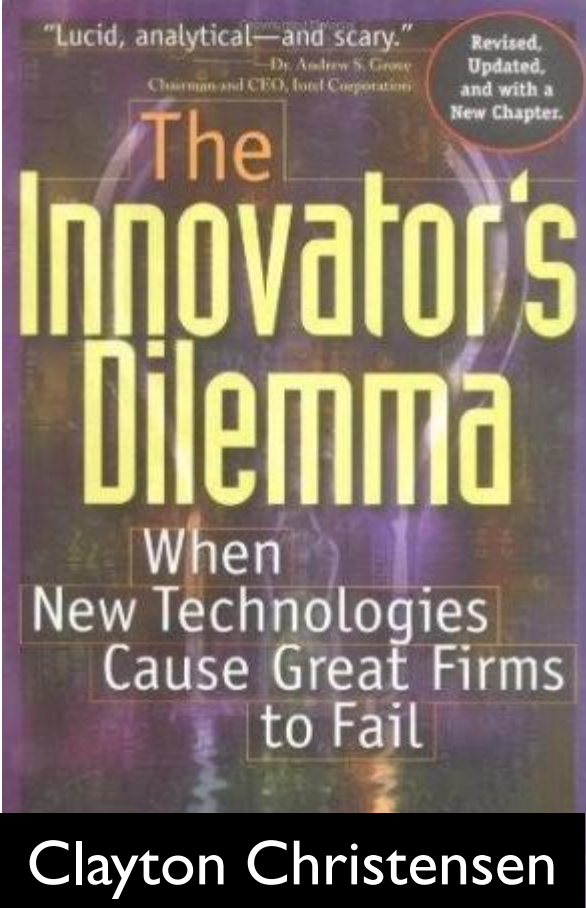


- Shugart Associates
- Micropolis
- Priam
- Quantum



ANTICIPATED DEMAND

# What is a Cyber Security Disruptor?

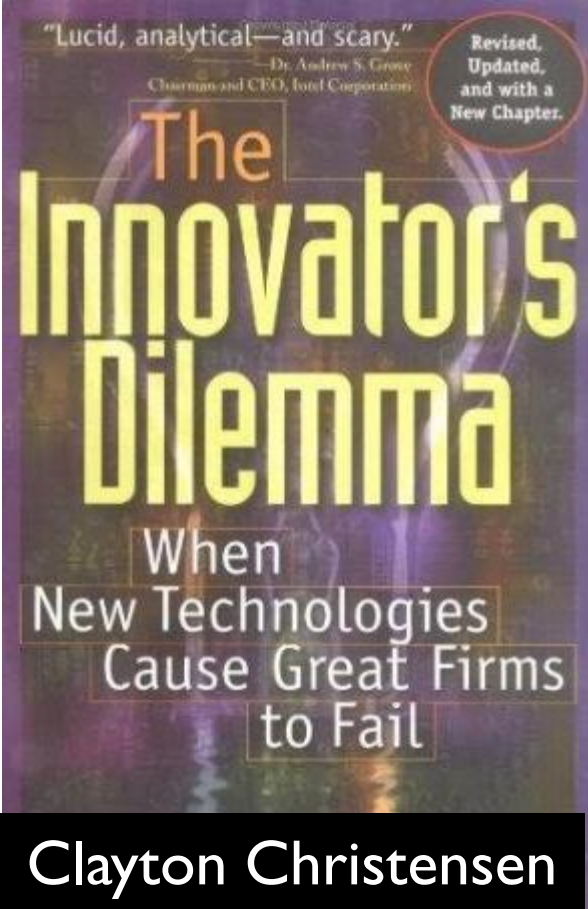


Micropolis



ANTICIPATED DEMAND

# What is a Cyber Security Disruptor?



Innovation







# What is a Cyber Security Disruptor?



→ 5-10 Years

<p>Cyber Security</p>  <p>Disruptor</p>	 <p>Catalysts</p>
---	--



... adopted for the s  
expediency, facili  
**pol-i-cy** - a cours  
adopted and pur  
government, rul  
... action of



# 10 Cyber Security Disruptors



DOMAIN NAME SYSTEM  
SECURITY EXTENSIONS



IPv6



MOBILE PLATFORM



SCADA ATTACK



CLOUD COMPUTING



APT



DEVELOPING NATIONS



CYBER TERRORISM



METaverse



TOP-LEVEL DOMAIN  
EXTENSIONS



INTERNATIONALIZED  
DOMAINS



APPLICATION STORE

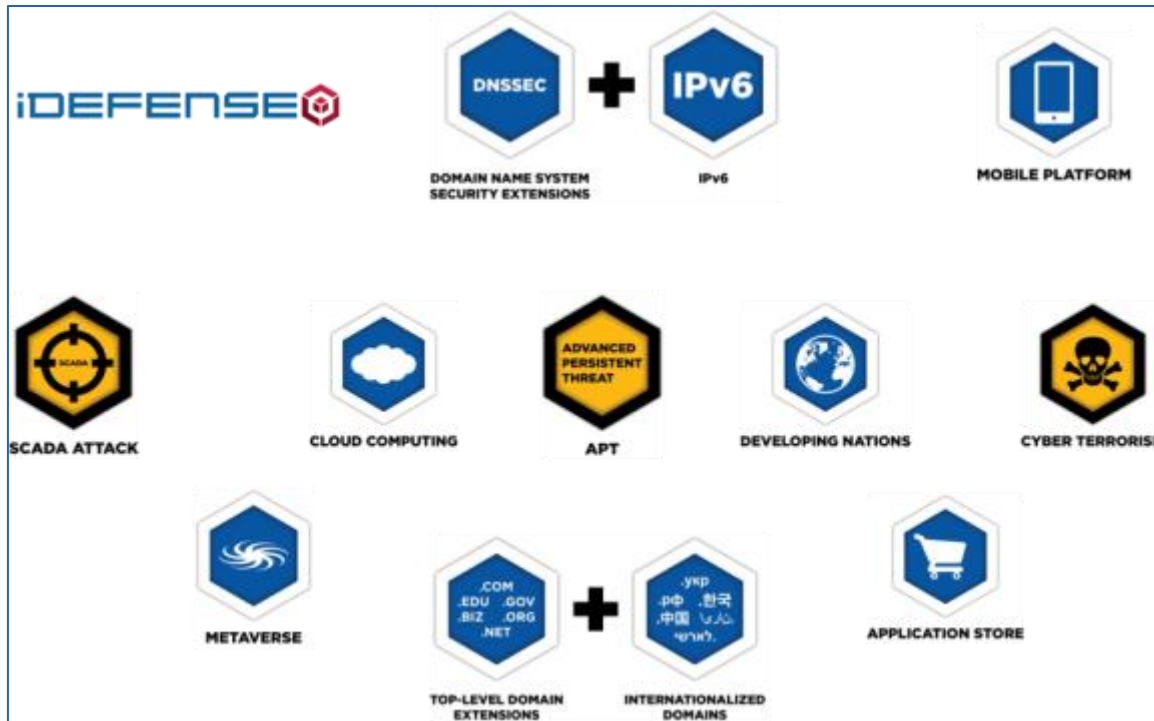




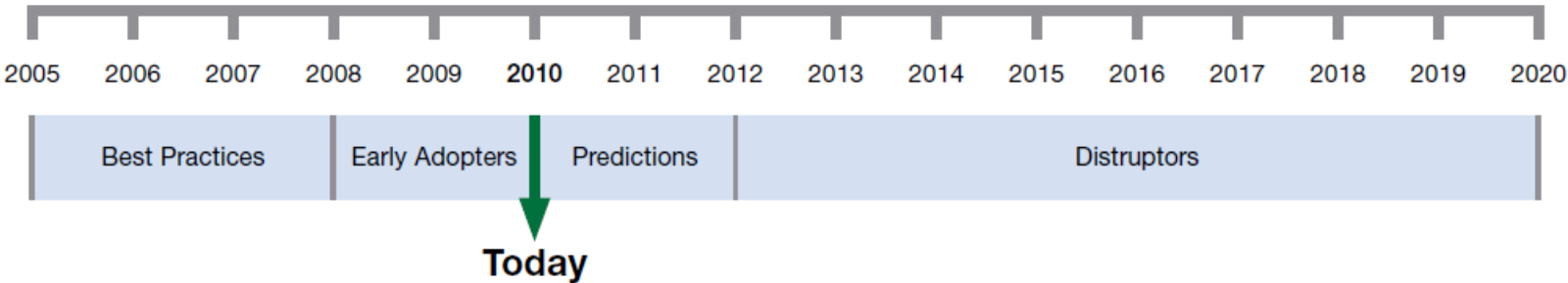
# Cyber Security Disruptor



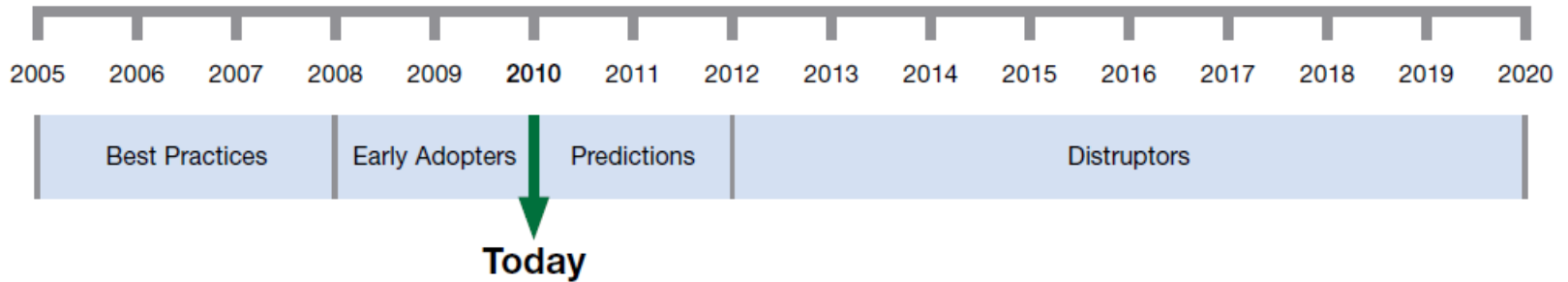
# Cyber Security Disruptor



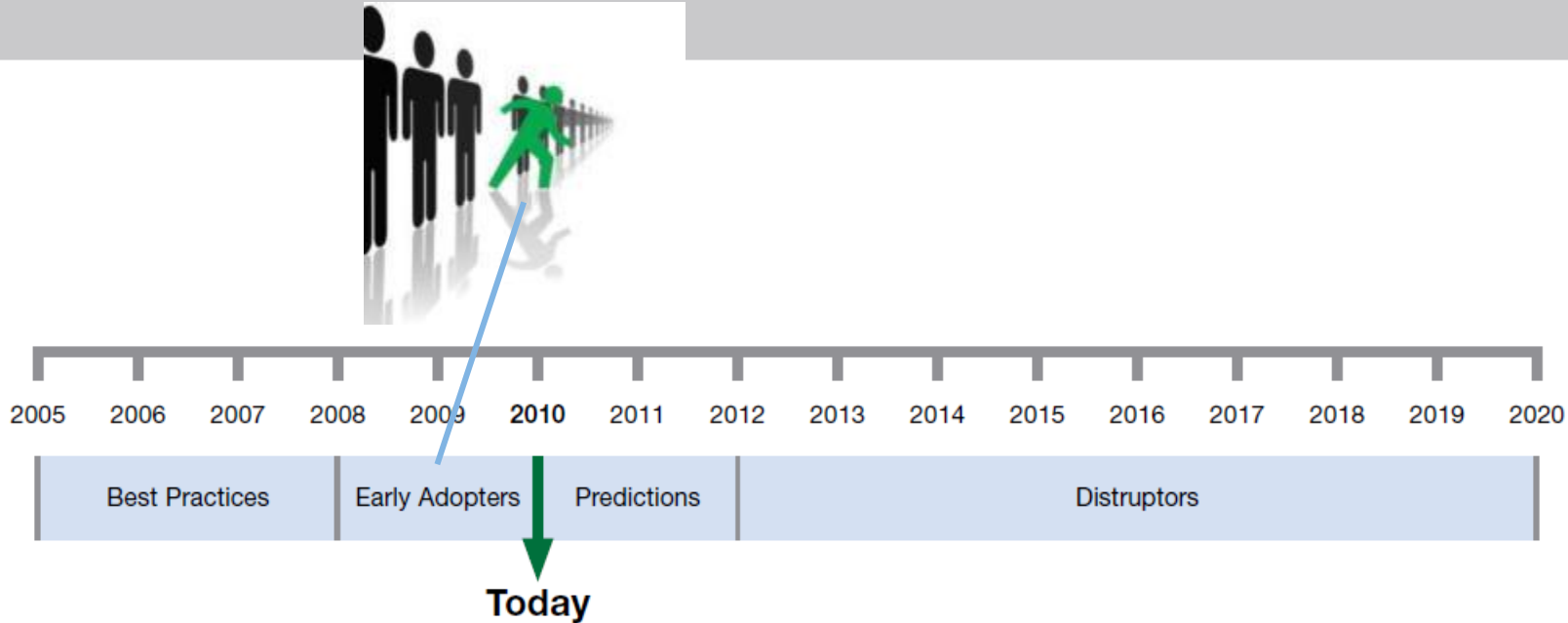
# Cyber Security Disruptors Timeline



# Cyber Security Disruptors Timeline

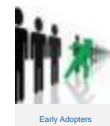


# Cyber Security Disruptors Timeline



~~Prime Time~~

# Cyber Security Disruptors Review



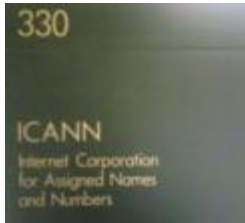


# Disruptor: TLDS & IDNS



2015

2010



Concept



Impact

Blacklists become unmanageable at the Enterprise level



# Disruptors: DNSSEC & IPv6

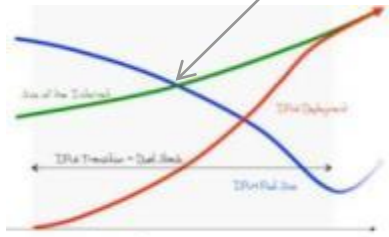


2013



2010

2-5 Years



Size of Internet  
IPv6 deployment  
IPv4 Pool

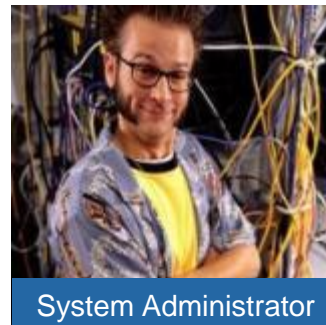


Concept



Impact

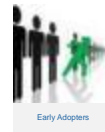
## IP Management just became very complex



System Administrator



# Disruptors: APT



2013

2010



CYBER ESPIONAGE



APT

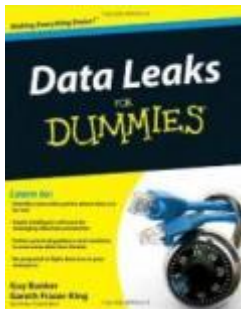


Concept

Intellectual Property is seriously at risk.



Impact



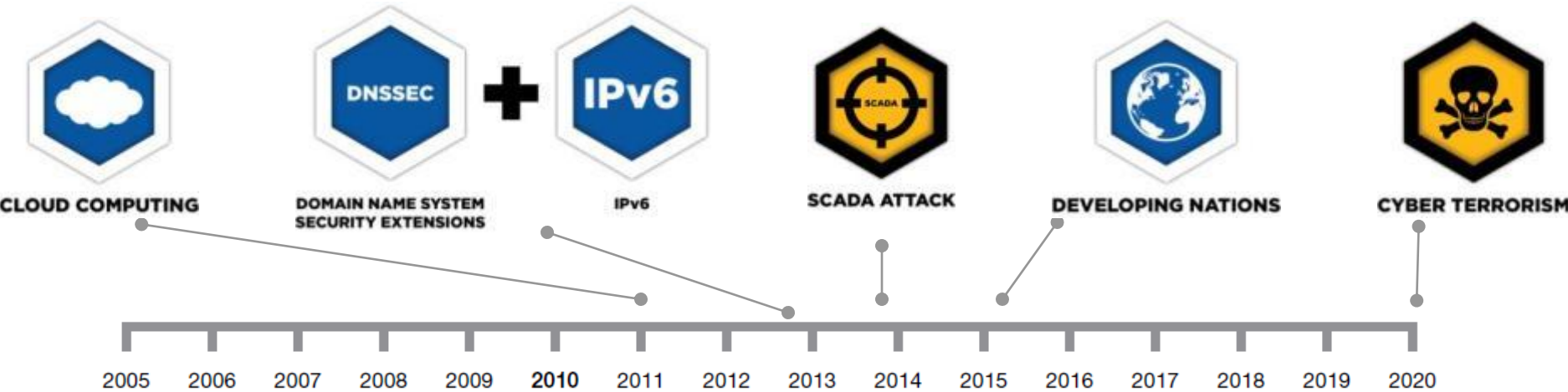
DATA LOSS PREVENTION SYSTEMS



Enterprise



# Cyber Security Disruptors Timeline



Today



MOBILE PLATFORM

APT

APPLICATION STORE

TOP-LEVEL DOMAIN EXTENSIONS

INTERNATIONALIZED DOMAINS

METAVESE

# Cyber Security Disruptors Early Adopters



CLOUD COMPUTING



DOMAIN NAME SYSTEM  
SECURITY EXTENSIONS



IPv6



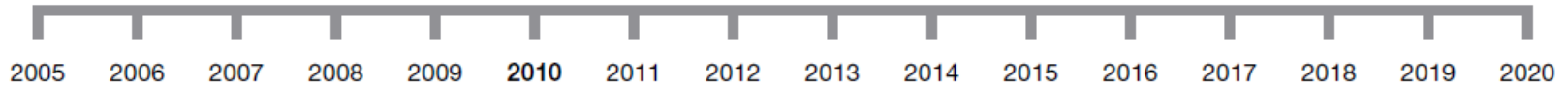
SCADA ATTACK



DEVELOPING NATIONS



CYBER TERRORISM



Today



MOBILE PLATFORM



APT



APPLICATION STORE



TOP-LEVEL DOMAIN  
EXTENSIONS



INTERNATIONALIZED  
DOMAINS



METVERSE



# Cyber Security Disruptor



... adopted for the s  
 expediency, facili  
pol·i·cy - a cours  
 adopted and pur  
 government, rul  
 ... action of





# Conclusion



**CYBER ESPIONAGE**

**Operation Aurora Impact**



**HACKTIVISM**

**Stuxnet Impact**

**Wikileaks Impact**



**CYBER WARFARE**

**Cyber Security Disruptors**



**DISRUPTOR**

# Recap

## iDEFENSE

### iDefense Security Intelligence Organization



Malware Analyst's Cookbook



Cyber Fraud

Cyber Security Essentials



2011 Cyber Threats and Trends

