# Intro Cyber Security/IA

J. Farricker – UW i310, Jan 2016

# *Cyber Security/IA*: Level Setting & Situational Awareness

# *Cyber Security*: Level Setting & Situational Awareness

- **Wiki: Definition of Cybersecurity**

**Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term *security* implies Cybersecurity**

# *Cyber Security*: Level Setting & Situational Awareness

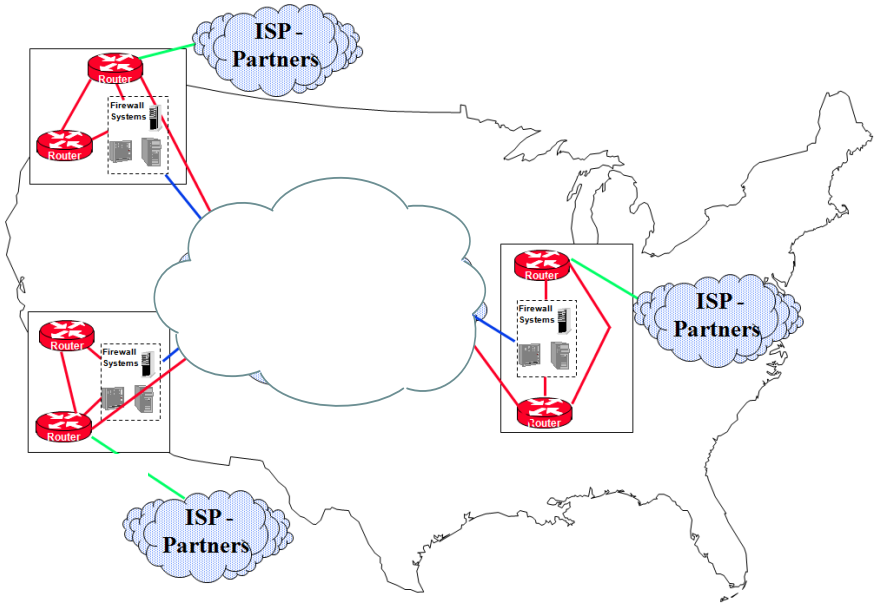
- **Wiki: Definition of Information Assurance**

**Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.**

# *Cyber Security/IA*: Level Setting & Situational Awareness

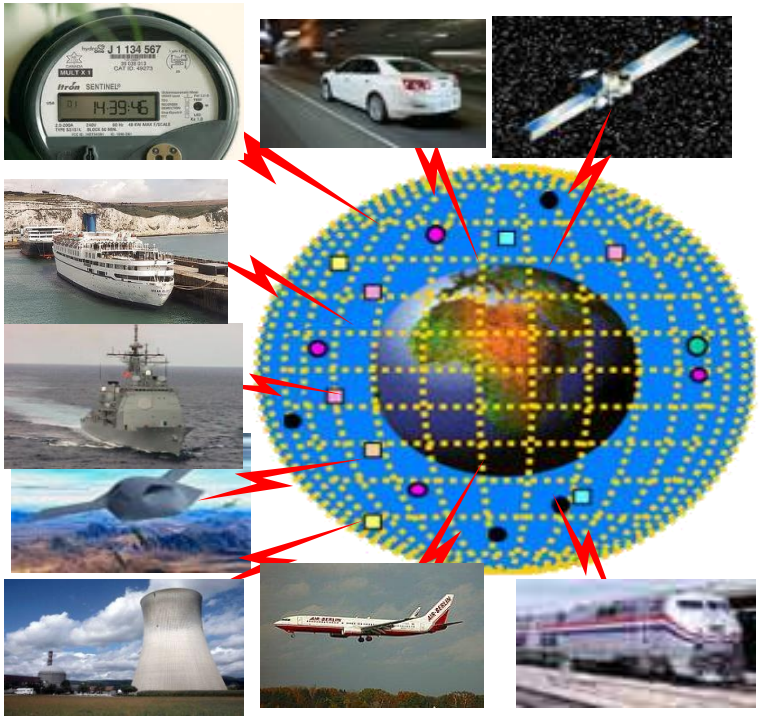
## Quick Summary

***Enterprise/Infrastructure Protect/Monitor***




**Cyber Security**

***Platforms/Products/Services***

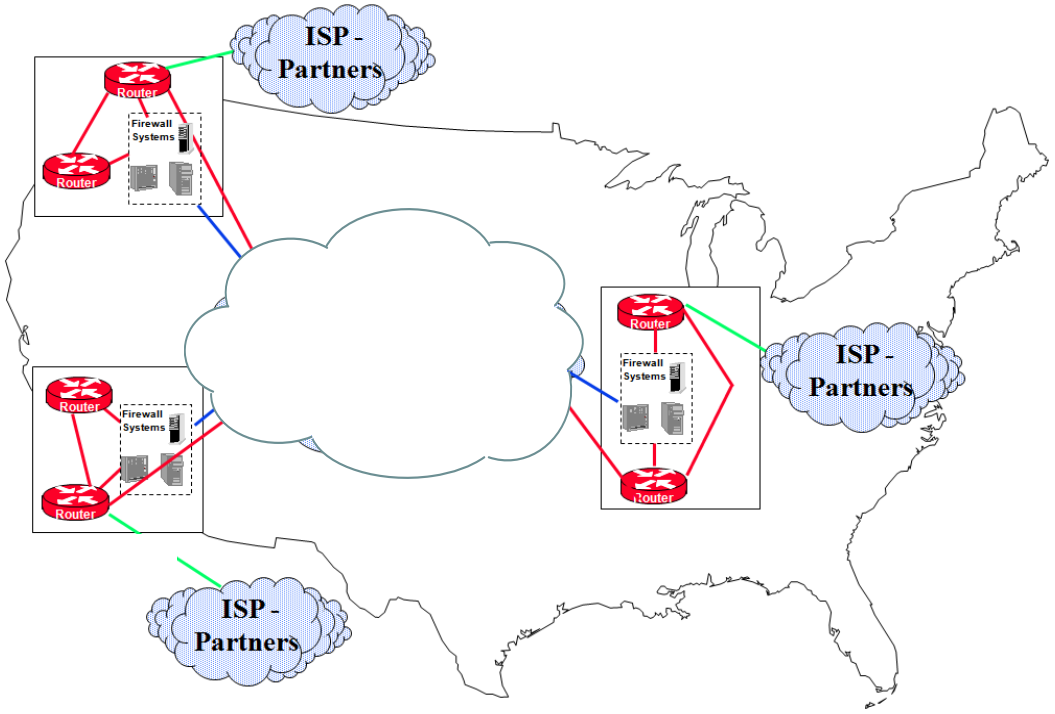


**Info Assurance**

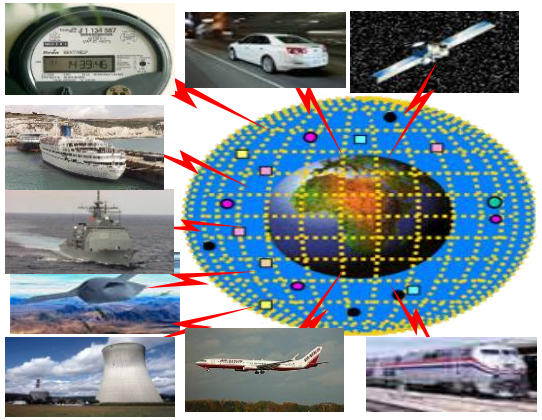
# *Cyber Security/IA*: Level Setting & Situational Awareness

## Quick Summary

***Enterprise/Infrastructure Protect/Monitor***



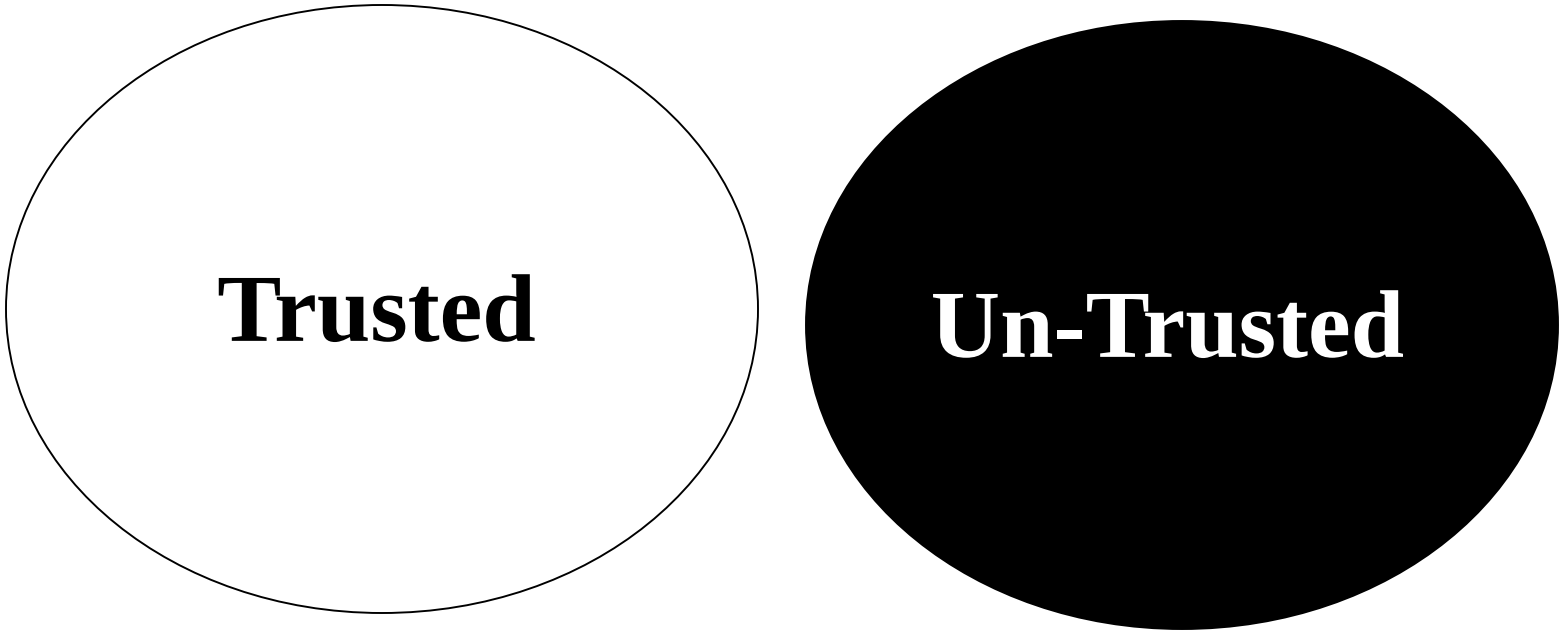

***Platforms/Products/Services***



**Cyber Security**

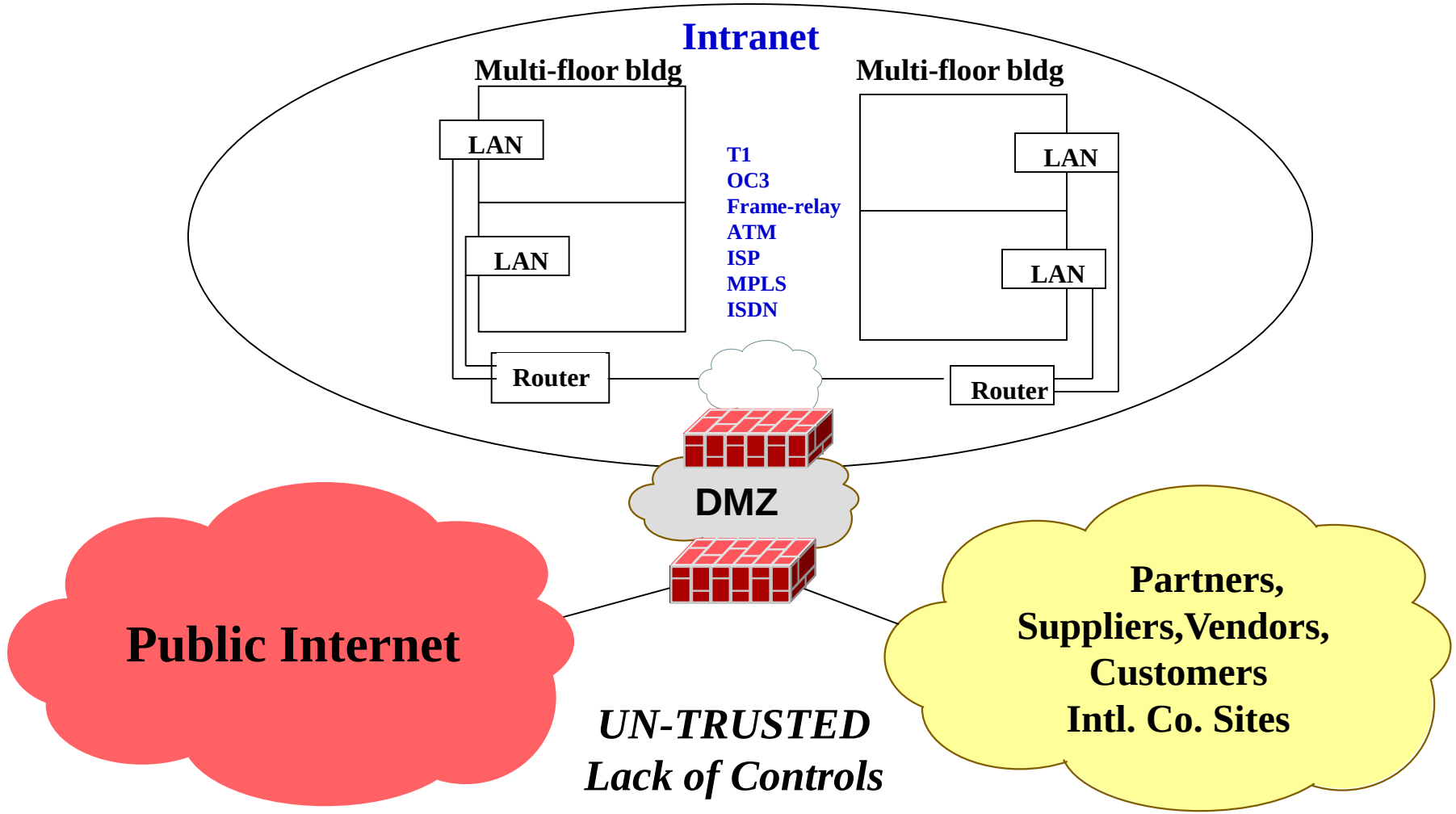
**Info Assurance**

# Network Security (Basically Two Types of Networks)



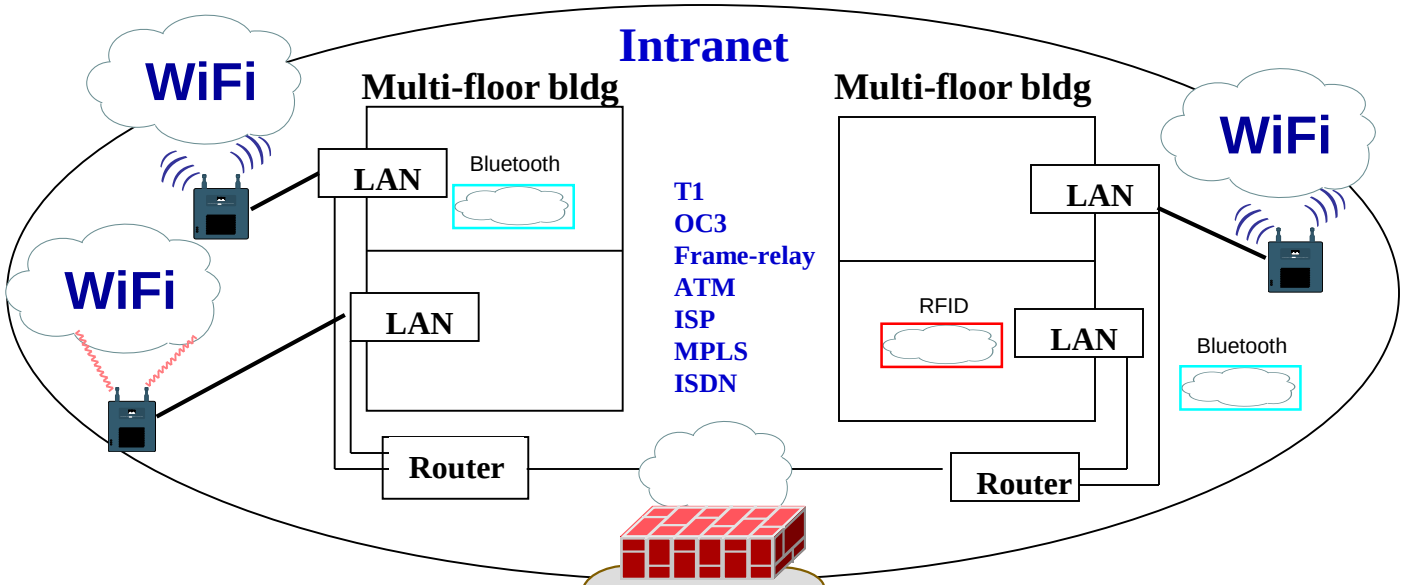
# TRUSTED

**Co. Owned/Leased Bldg. (Fenced)**
**Badge/Physical Access Controls**
**Locked Data Closets**
**Multi-factor Authentication**



# *TRUSTED ??*

**Co. Owned/Leased Bldg. (Fenced)**
**Badge/Physical Access Controls**
**Locked Data Closets**
**Multi-factor Authentication**

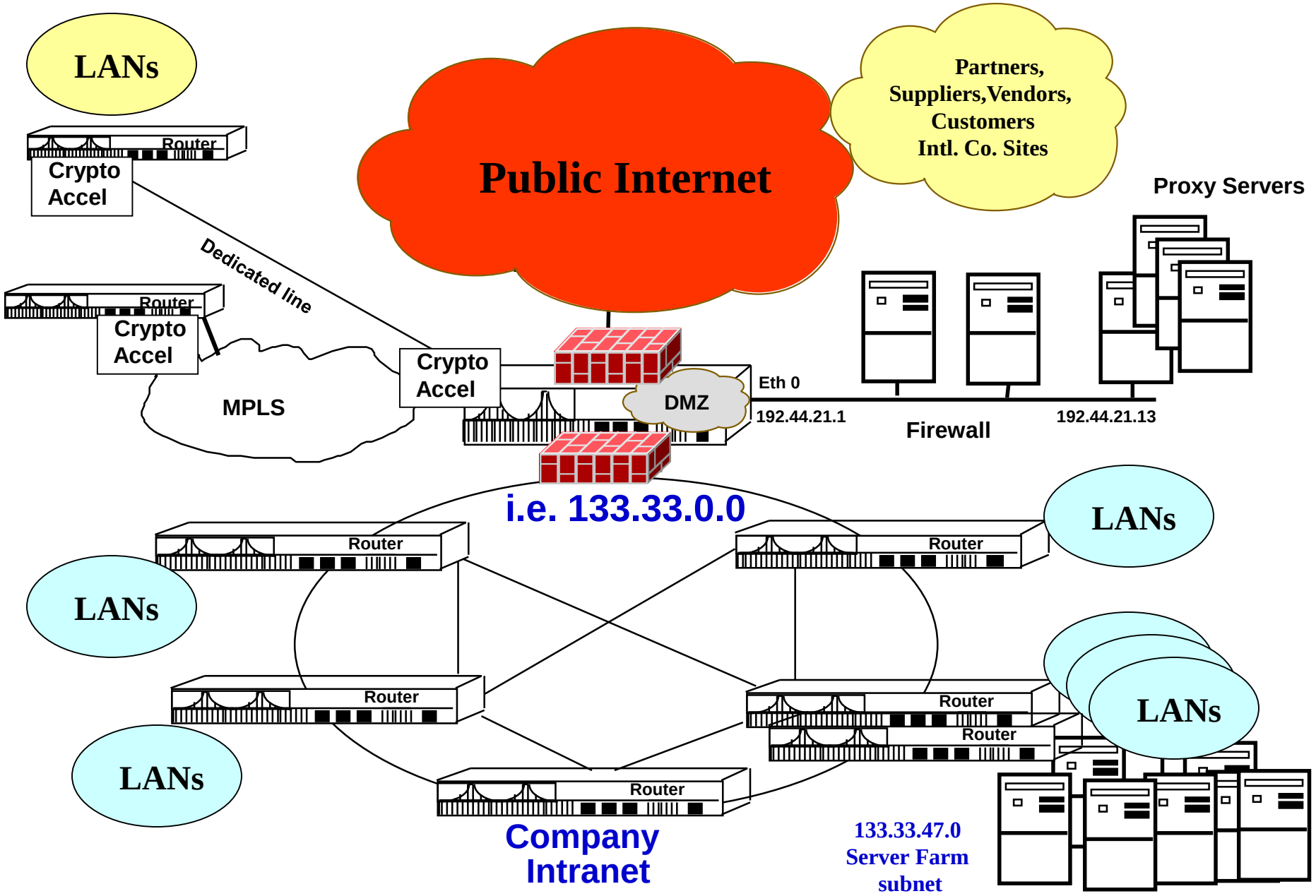



**Public Internet**

**Partners,**
**Suppliers,Vendors,**
**Customers**
**Intl. Co. Sites**

***UN-TRUSTED***
***Lack of Controls***

# Security Perimeters/DMZ's: 2000s



# Game/Industry Changers

***What changed ??***

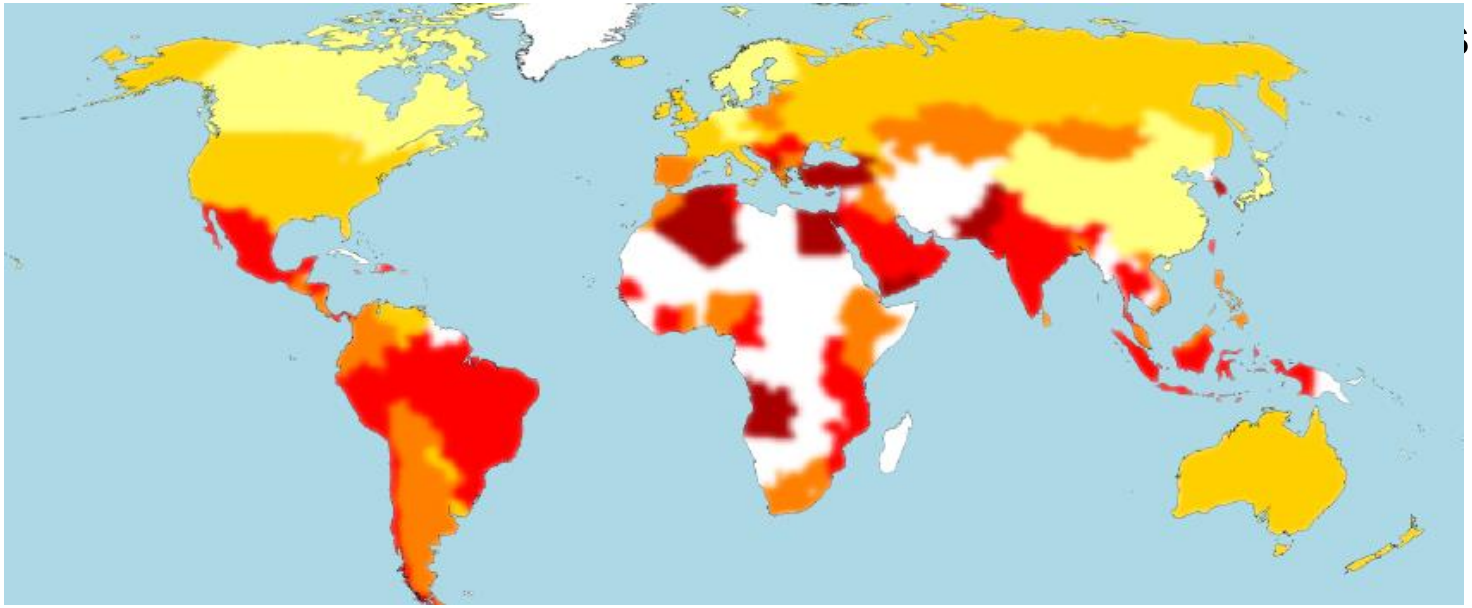
***How long has "hacking" been around ??***

***What doesn't the DMZ on prev page protect against ??***

***Relying on Network Centric Protection mechanisms only - akin to playing "Whack-a-Mole"***

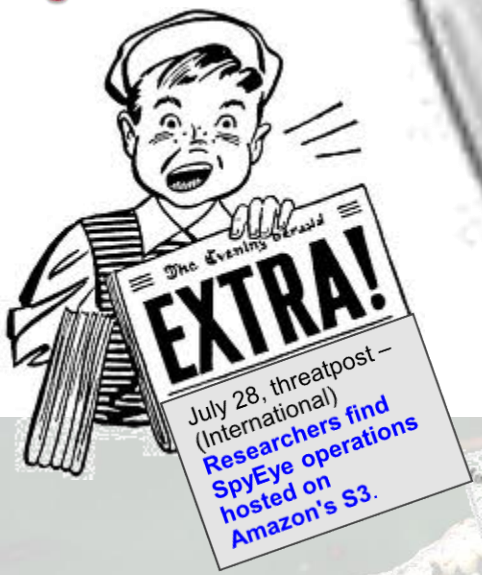
# What is APT

- **APT (Advanced Persistent Threat)**
  - **Term coined by the Air Force**
  - **Often over-used and misrepresented by media and vendors**
  - **These attacks often have political or economic motivation**
  - **Generally target defense industry technologies**



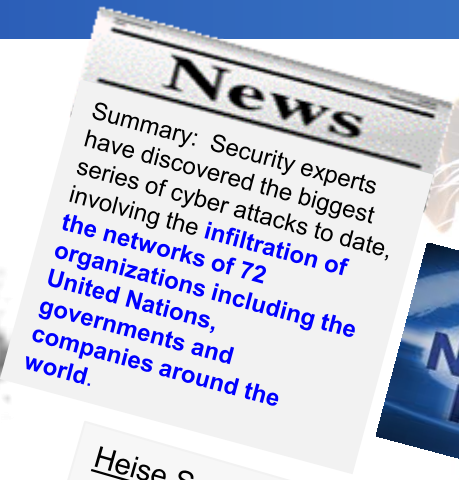
# APT Changing Landscape of Business and Defense Industry

**It's:**
**Big News**
**Big Business**
**Big Risk!**




July 28, threatpost – (International) **Researchers find SpyEye operations hosted on Amazon's S3.**


July 22, Dark Reading – (International) **New targeted attack campaign against defense contractors under way.** The U.S. defense industry is under siege by cyber spies in an attack that provides a link to a rigged spreadsheet **containing a real list of high-level defense industry execs…**




Summary: Security experts have discovered the biggest series of cyber attacks to date, involving the **infiltration of the networks of 72 organizations including the United Nations, governments and companies around the world.**


Heise Security, 1 Aug 2011: The recently discovered iFrame injection campaign rages on… **Mass iFrame injection attack now counts millions of compromised web pages.**

CNN Money Tech, 28 Jul 2011: On April 8, 2010, **traffic to about 15% of the world's websites was rerouted to China.** State-owned Internet company China Telecom tricked relays from around the world into routing traffic through its servers for about 18 minutes.

THE WALL STREET JOURNAL.

**"Regarding current state of Advanced Persistent Threat in Corporate America: There are are two types of Fortune 500 Companies, those that have been hacked and those that don't know they've been hacked…**

## NEWS

**A unique malware file is created every ½ second**

Heise Security, 1 Aug 2011: Sophos has released its Mid-Year 2011 Security Threat Report, which reveals that since the beginning of 2011, the company has identified an average of 150,000 malware samples every day.


PC World, 1 Aug 2011 - **Malicious software is leaping from PCs to cell phones…**

New Threats are Discovered Every Day

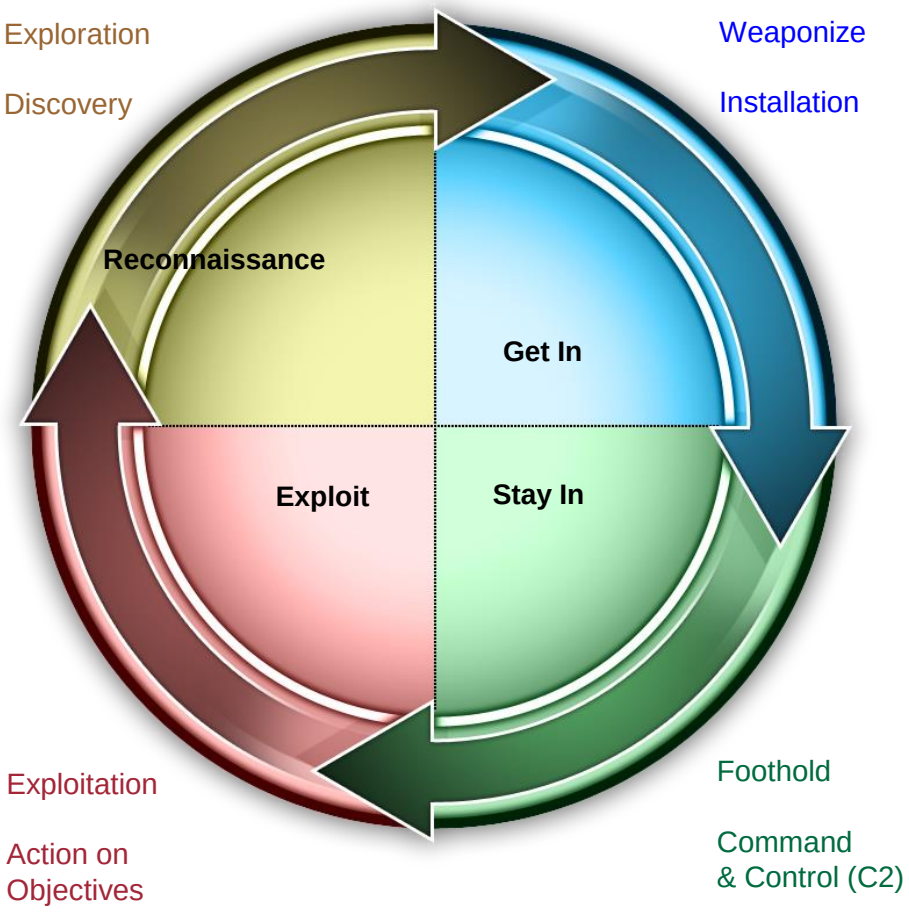
# APT Intentions

- **Developing nations share technology attained through espionage to advance their industrial base**

- **How countries benefit from APT**
  - ***Low entry cost to establish APT program***
  - ***Attain industrial competitive advantage***
  - ***Identify DoD capability or system vulnerability***
  - ***Replicate key DoD capability***
  - ***Gain access to new or restricted technology***
  - ***Save billions of dollars in research and development***

**The US DoD has indicated some governments, in addition to employing thousands of its own hackers, manages massive teams of experts from academia and industry in "cyber militias" that act in national interests with unclear amounts of support and direction.**

# APT Approach




The Department of Defense calls these attacks Advanced Persistent Threats or APT

Very Sophisticated:

**Advanced** – Attacks are well-funded and use highly skilled operators

**Persistent** – Attacks are hard to detect and remove; they keep coming back

**Threats** – The attackers are exfiltrating – or copying out – large amounts of information

Others call it: Determined Human Adversary

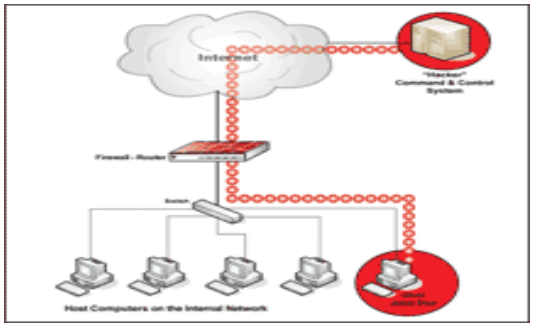
**No matter what you call it - it's real !**

# *Cyber Security*: Level Setting & Situational Awareness

## APT Approach

**Reconnaissance**

- Social Networking
- Mailing Lists
- Conference Proceedings
- Press Releases
- Web Search

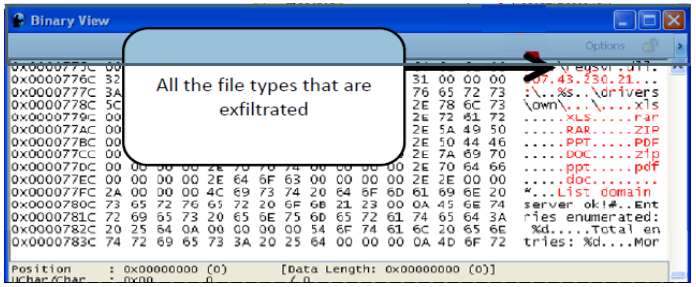


**C2 (Command and Control)**

- Backdoor “calls home”
- Gives the adversary the ability to execute commands on the infected host
- Will “beacon” on some form of interval
- Could beacon to web pages etc.

**Weaponization – “Trojan horse” Malware**

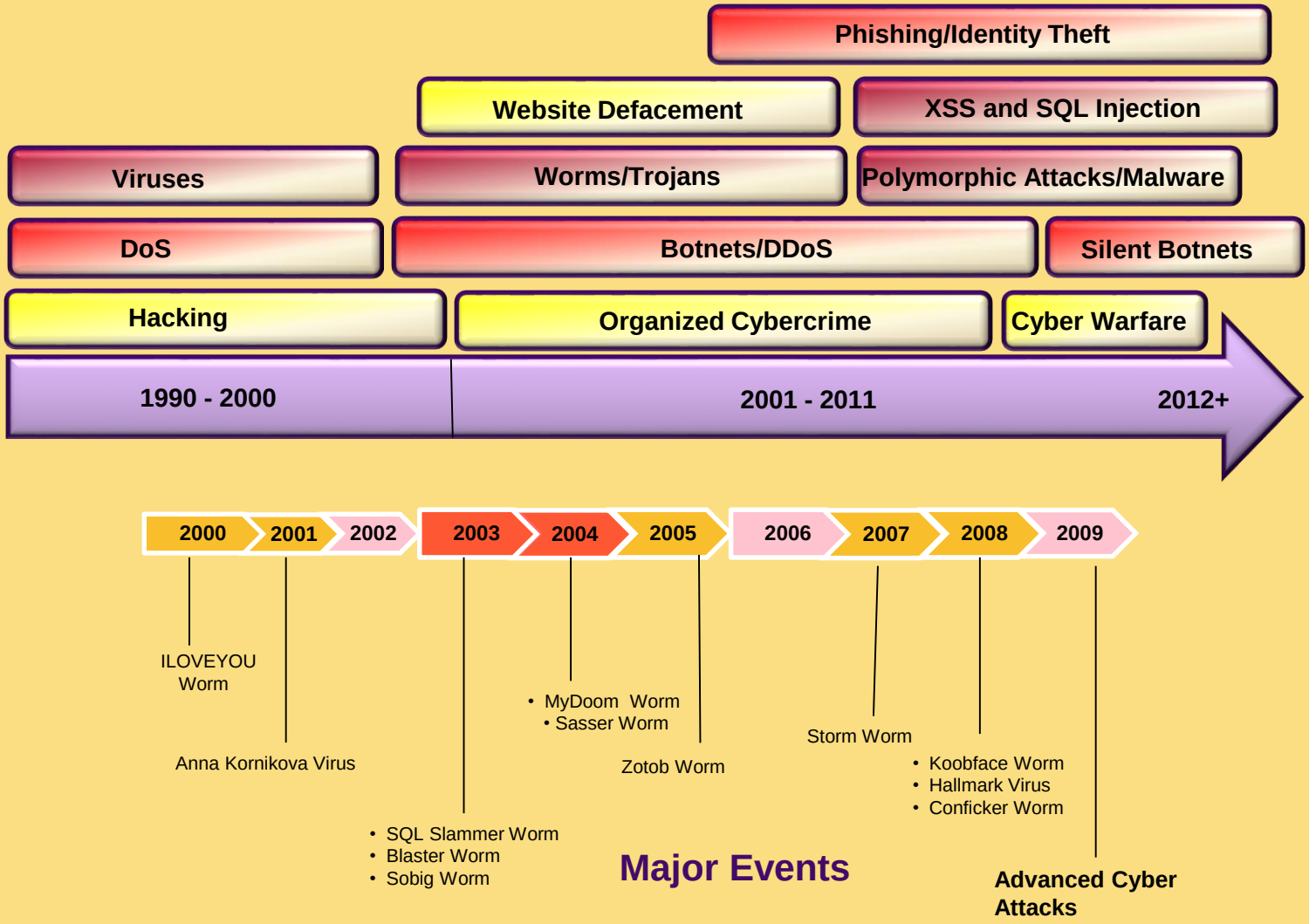
- Coupling an exploit with a backdoor
- Can be hidden inside of a PDF, Excel, Java, DOC, web page, etc.


**Exploit/Installation**

- Zero-day Vulnerabilities
- Almost always tested against all Anti-Virus technologies before deployment
- Installation is usually disguised as a legitimate process

# The Threat



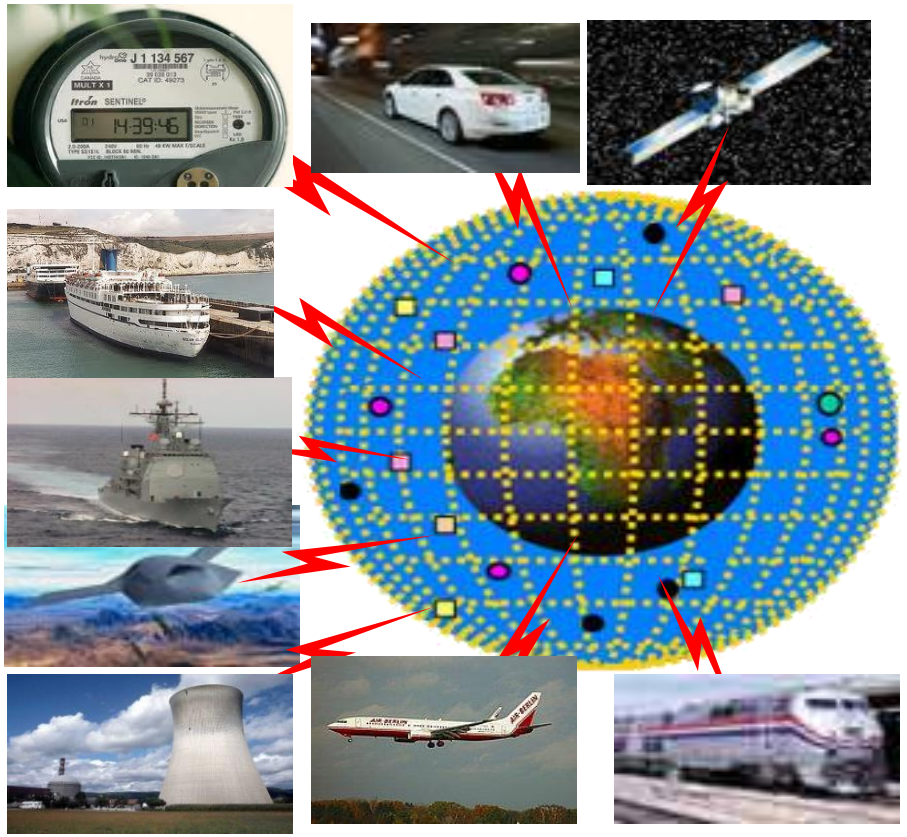
# Joel Brenner, former head of counterintelligence, NSA

**We've taken an open system based on anonymity and meant for a small, trusted community of government officials and university scientists, and we've turned it into the backbone of our national commerce and much of our national and military communications.**

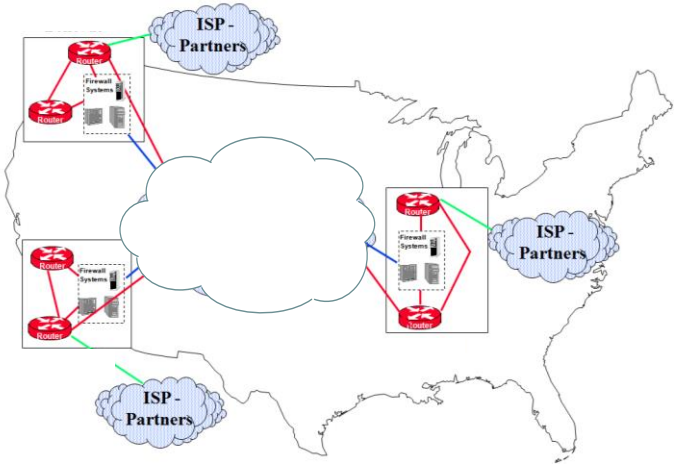
**Few people, even among business and government leaders, realize how gravely vulnerable this situation makes us.**

# Platform Cyber Security/IA

## Platforms/Products/Services



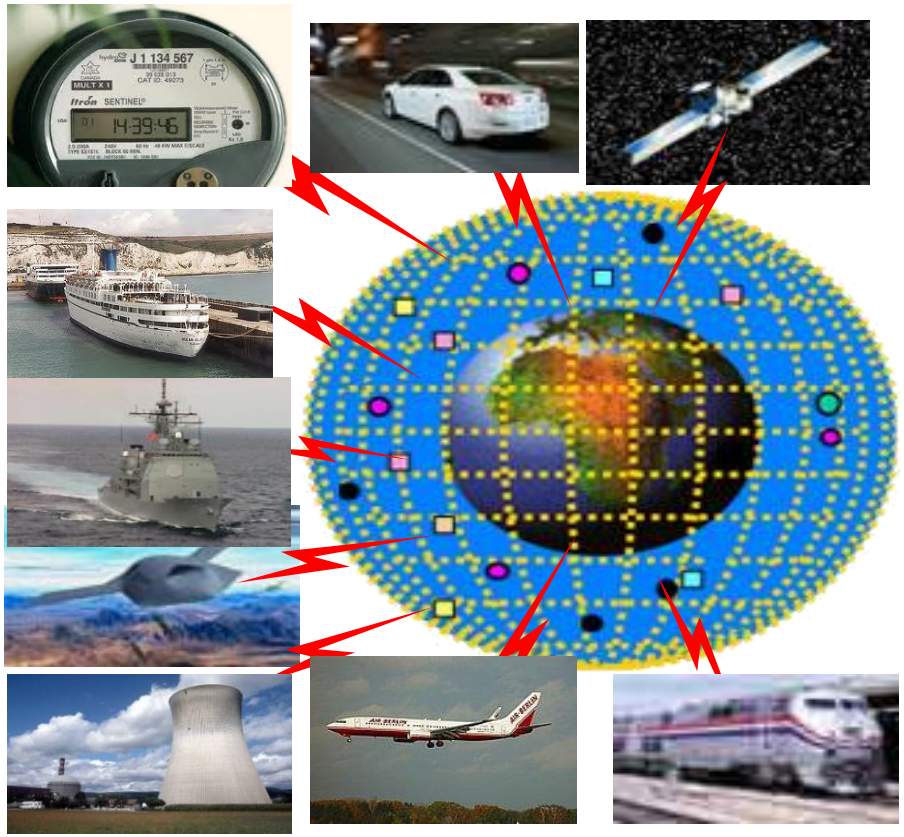
**Enterprise/Infrastructure Protect/Monitor**




**Cyber Security** ⟷ **Info Assurance**

# Platform Cyber Security/IA

## Platforms/Products/Services



## Why important ?

*(Why should you care ???)*

## Info Assurance

# Pillars of Information Assurance

***Pillars of IA (Information Assurance)*** **describe the fundamental properties that must be maintained. IA (Information Assurance) is the practice of managing risks while maintaining these properties. Malicious human threats are not the only kind IA considers — a hungry squirrel might gnaw through a cable and bring down a server. Protecting against this is IA, though not really cyber security.**

***Per the security-related aspects of IA.***

**Confidentiality: Assurance info not disclosed to unauthorized individuals, processes, or devices.“**

**Integrity: no unauthorized modification or destruction of information.**

**Availability: Timely, reliable access to data and information services for authorized users.**

**Non-repudiation: Assurance sender of data is provided w/proof of delivery & recipient provided w/proof of sender's identity**

**Authentication: Security measure designed to establish the validity of a transmission, message, or originator, and/or means of verifying individual's authorization to receive specific categories of info.**

# *Platform Cyber Security/IA*: Engineering Perspective

## *Key Considerations*

**Secure Op System**

**Secure RF Comm**

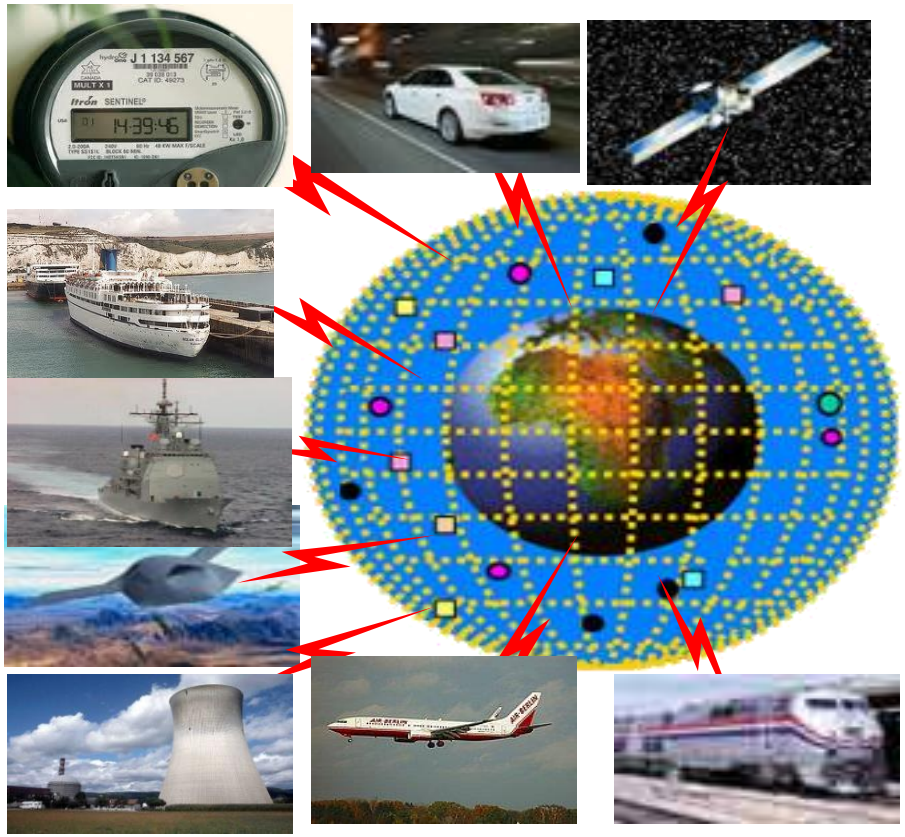
**Software (inspect,VA)**

**Maint Link/Integration**

**End to End solutions**

***(SupplyChain, Maint/Logistics, Net Mgmt/Admin, Bus Continuity, VulnAnalysis, Eng/Factory Integration)***

## Platforms/Products/Services



**Info Assurance**

# *Platform Cyber Security/IA*: Program Observations


**Supplier Software**

**COTS Components (cost driven)**

**Software Loading/Maintenance laptops/test tools**

**Earlier engagement w/accreditation TWG/Orgs**

# Key Take-away

***Security designed in, not bolted on !***