



# Evolution and Revolution of Cyber Threat Intelligence

March 20, 2013

**PROPRIETARY INFORMATION**

Copyright 2013 FS-ISAC, Inc.  
Unauthorized distribution is prohibited.

# Agenda

- **FS-ISAC Overview**
- **Cyber Threat Landscape**
- **Intelligence Primer**
- **Cyber Threat Intelligence**
- **Capability Development**
- **Intelligence Products**
- **Come the Revolution**





# FS-ISAC OVERVIEW

# FS-ISAC Background

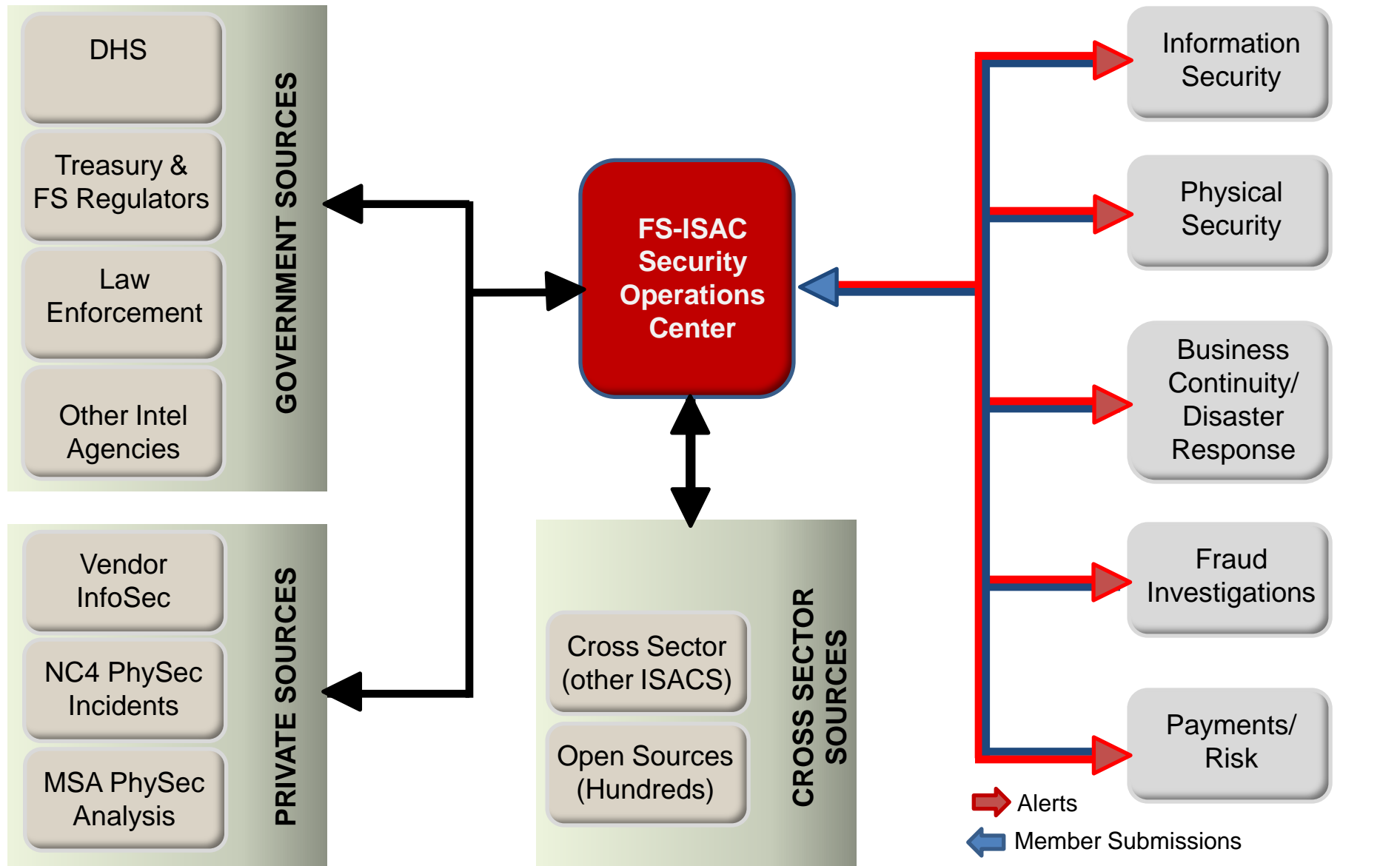
- ❑ Formed in 1999 in response to PDD-63 with a cyber security mission. Updated in 2003 under HSPD-7 to include physical security and disaster recovery missions.
- ❑ Member owned, not-for-profit incorporated association open for membership to all US federally regulated financial institutions and utilities.
- ❑ Currently has over 4200 direct and indirect (via association) owner/operator members with:
  - 20 trade associations
  - 85% of the card processor volume
  - All major card brands
  - All payment system operators
  - All major exchanges and clearinghouses.
- ❑ Operational arm of the Financial Services Sector Coordinating Council (FSSCC).



# Information Flows

## Information Sources

## Member Communications





# CYBER THREAT LANDSCAPE

# Threats Actors

- ☐ **Can generally characterize actors targeting sector in the following affiliations/motivations:**
  - Nation State/Military
  - Covert State Sponsored/Affiliated
  - Terrorist
  - Criminal
  - Commercial Industrial Espionage
  - Activist/Issue Motivated
  - Insiders
  - Opportunistic
  - Other
- ☐ **They are not necessarily as separate as we would like.....**
- ☐ **Some question the reasons for attribution, but hopefully that will become clear, although attribution is obviously not necessary in all cases.**



# Militarization of Cyber Space

## ❑ Rapid expansion of national espionage and offensive military capabilities into cyber space:

- Since early 2012 there has been substantial media reporting of the advancement of military cyber operations programs in Israel, Iran, North Korea, South Korea, India and Taiwan.
- In Aug 15th 2012 a blogger released a reported copy of Israel's alleged military strike plans against Iran's nuclear facilities which included employment of substantial cyber offensive capability in support of conventional military activities.

## ❑ Many larger organizations operate in a global context so even potential regional cyber conflicts can be of significant business concern, eg, China/Taiwan, India/Pakistan, Israel/Iran, Iran/Saudi Arabia.



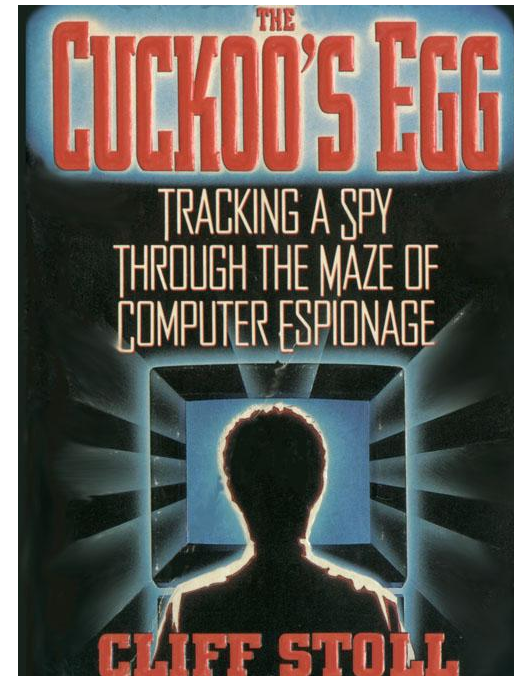
<http://www.threatgeek.com/threattoons/>





# The First Known Cyber Espionage Event

- ❑ Year: **1986**
- ❑ Location: Lawrence Berkeley Laboratory
- ❑ Actor: Soviet Union – KGB  
through German hacker  
Markus Hess
- ❑ Collection Objectives:  
Strategic Defense Initiative (SDI) aka Star Wars Ballistic Missile Defense, nuclear technology materials
- ❑ Technologies:  
VAX VMS, UNIX, Login Trojans, ARPANET, Dialup Modem



Images belong to their Copyright Holders



# Moonlight Maze

- ❑ Timeline: **March 1998 – 2003  
at least**
- ❑ Location: US DOD, NASA, US  
DOE, universities,  
and National  
Research Labs
- ❑ Actor: Believed Russia –  
Likely FSB/FAPSI
- ❑ Collection Objectives: Unknown  
but likely military and nuclear  
technology related



Courtesy: Threatpost.com



Images belong to their Copyright Holders



# State Sponsored/Affiliated

- ❑ **Advanced Persistent Threat (APT)** – We are well aware APT is a who, not a what.
- ❑ **Cyber Espionage**, is the more general term we apply to intellectual property theft related activities.
- ❑ We have also found that that the term “**State sponsored**” does not necessarily mean “**state executed.**” It may mean “**State Condoned**” or “**State Endorsed.**”
- ❑ There are lots of contracting and affiliate relationships making attribution more complex.





# INTELLIGENCE PRIMER



# Intelligence

- There is no globally accepted definition of Intelligence, even in the US Intelligence Community (IC).
- **Military Intelligence** exploits information collection and analysis approaches to provide guidance and direction to commanders in support of their decisions.
- Achieved by assessing all available data from all sources, directed towards the entities' mission requirements or responding to focused questions as part of a planning activity.
- To provide informed analysis, the information requirements are first identified.
- A 360 degree review of the operational environment, including friendly information, is carried out.

[http://en.wikipedia.org/wiki/Military\\_intelligence](http://en.wikipedia.org/wiki/Military_intelligence)

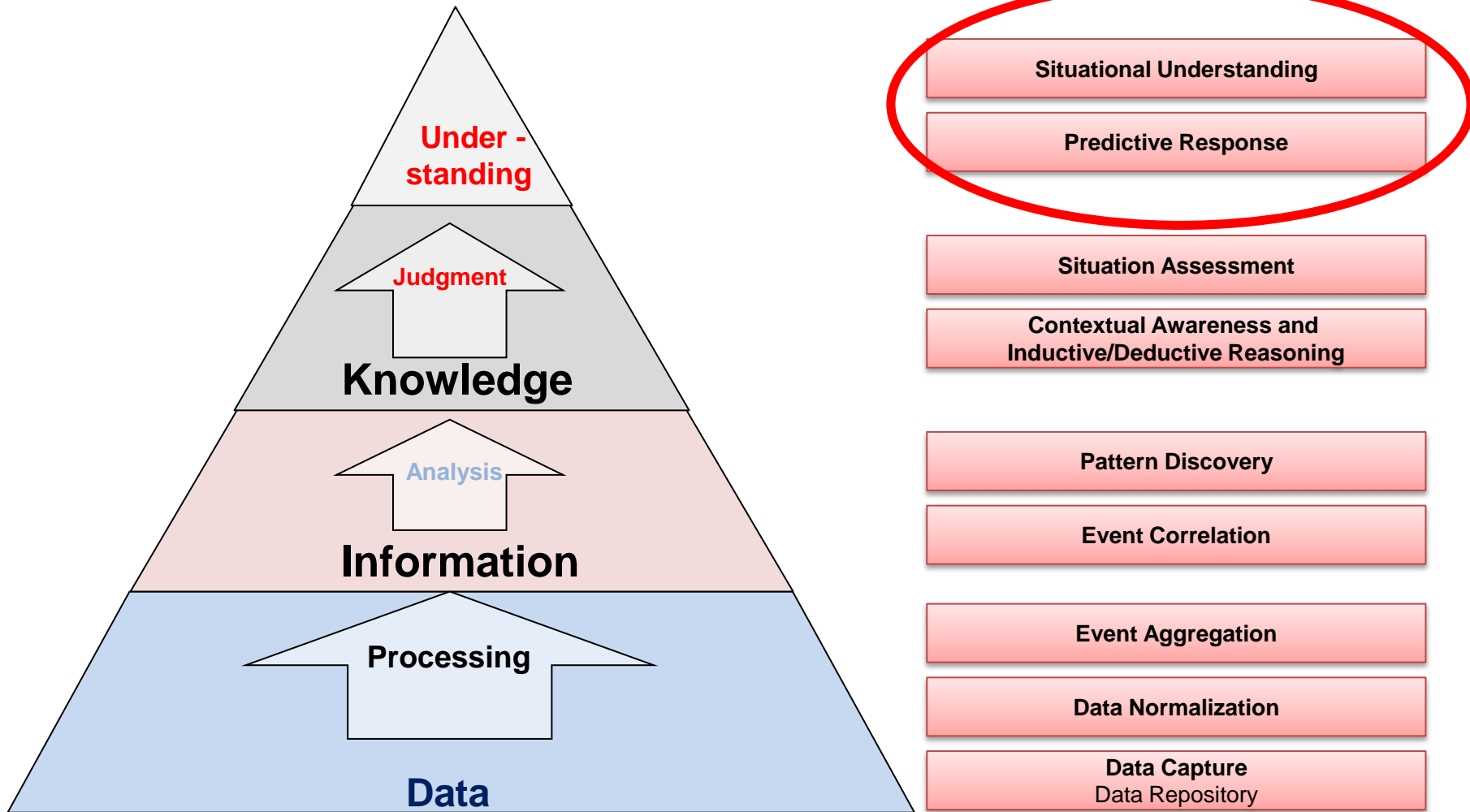


# Levels of Intelligence

- Intelligence operations are carried out throughout the hierarchy of political and military activity:
  - **Strategic Intelligence** is concerned with broad issues such as capabilities and intentions of adversaries at all levels, economics, political assessments. In a corporate business and technology sense, it can include activities such as examining the cyber threat environment in a country or region where you are opening a new office.  
Temporally it is a longer term activity
  - **Operational intelligence** is focused on support to operational activities in the medium term. Continuing the new office example, it would be identifying sources and methods associated with the new office location, particularly where there are language, cultural and other issues. It might be implementing a new control (eg. Blocking of zips in web download) due to high order analysis of a set of threat activity
  - **Tactical intelligence** is focused on low level engagements at a threat realization level. It is focused on the protective, detective and reactive controls for specific threats, as part of a specific attack.



# What we seek to achieve!



Based on US Army Operations Processes for Leadership, Command and Control





# Intelligence Cycle

(Courtesy FBI Directorate of Intelligence)



Images belong to their Copyright Holders

<http://www.fbi.gov/about-us/intelligence/intelligence-cycle>





# It's Not Just Adversaries

- True comprehensive intelligence involves understanding the total environmental context including:
  - **Geopolitical factors** such as global/regional/local office locations and threat drivers in those locations.
  - **Socio-cultural issues** that may drive certain threats and responses. For example in the Middle East, there is “an eye for eye” mentality that drives both Israel and Arab/Iranian actors at all levels.
  - **Business Drivers** so that there is understanding of the environment that your organization is currently active in, or intends to get active in. For example, what factors do you need to consider if you are going to open an office in Sao Paulo or Moscow or Beijing.
  - **Understanding your critical assets** is key to identifying threats to them. Assets may include personnel, services, systems, data and reputation.
  - **Personal Drivers** particularly in high risk countries where there is potential for subversion, corruption or increased likelihood for insider risk.
  - **Technology Footprint** of your organization so you can determine relevance of technical threat.
  - **Controls and mitigation** offset threat and risk and need to be well understood to provide an accurate assessment or forecast.





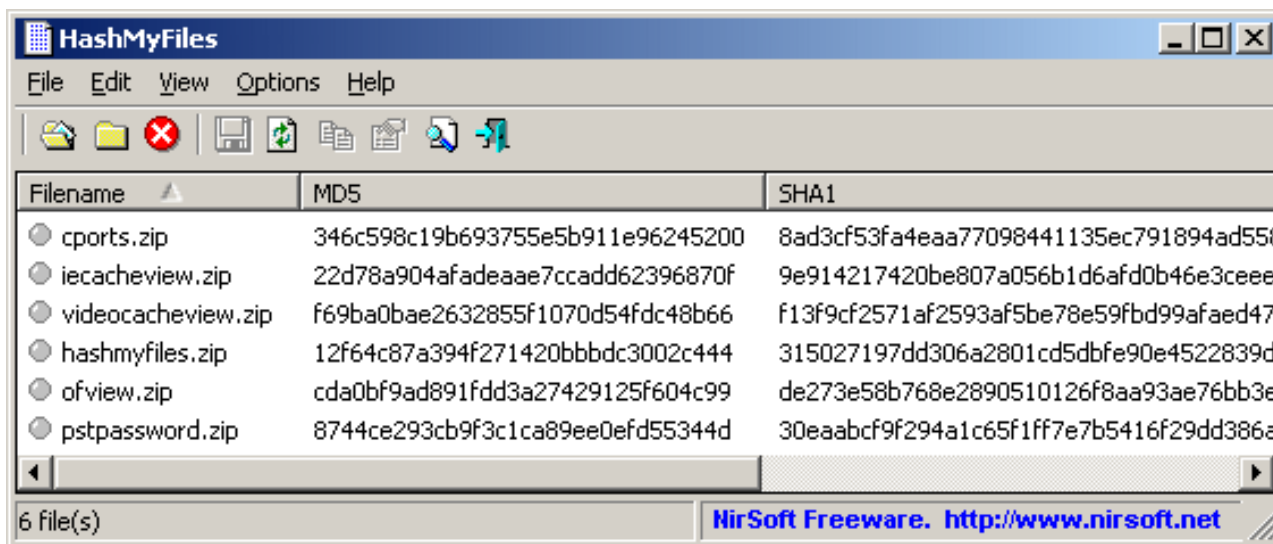
# CYBER THREAT INTELLIGENCE

# Definitions – What's in a Name?

- **Cyber Squared** in April of 2011 defined CTI as “an emerging information security discipline that **seeks to recognize and understand sophisticated cyber adversaries, specifically why and how they threaten data, networks, and business processes.** With enhanced knowledge of the threat develop better protective measures against them.”
- **Cyber Intelligence Sharing and Protection Act (CISPA)** describes CTI as “**information** in the possession of an element of the intelligence community **directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity,** including information pertaining to the protection of a system or network from either 'efforts to degrade, disrupt, or destroy such system or network'; or 'theft or misappropriation of private or government information, intellectual property, or personally identifiable information.”
- **The Software Engineering Institute Innovation Center of CMU**, defines Cyber Intelligence as **the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.**



# Cyber Threat Intelligence is not (only)...



The screenshot shows the HashMyFiles application window. It has a menu bar with File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for file operations. The main area is a table with three columns: Filename, MD5, and SHA1. The table lists six files: cports.zip, iecacheview.zip, videocacheview.zip, hashmyfiles.zip, ofview.zip, and pstpassword.zip. The status bar at the bottom indicates '6 file(s)' and provides the NirSoft Freeware website URL.

Filename	MD5	SHA1
cports.zip	346c598c19b693755e5b911e96245200	8ad3cf53fa4eaa77098441135ec791894ad558
iecacheview.zip	22d78a904afadeaae7ccadd62396870f	9e914217420be807a056b1d6afd0b46e3ceee
videocacheview.zip	f69ba0bae2632855f1070d54fdc48b66	f13f9cf2571af2593af5be78e59fbd99afaed47
hashmyfiles.zip	12f64c87a394f271420bbbd3002c444	315027197dd306a2801cd5dbfe90e4522839d
ofview.zip	cda0bf9ad891fdd3a27429125f604c99	de273e58b768e2890510126f8aa93ae76bb3e
pstpassword.zip	8744ce293cb9f3c1ca89ee0efd55344d	30eaabcf9f294a1c65f1ff7e7b5416f29dd386a

- A MANDIANT Indicator of Compromise (IOC)..
- An MD5 of a new piece of Malware...
- The Fully Qualified Domain Name of a Command and Control (C2) Server....





# CAPABILITY DEVELOPMENT

# Cyber Intelligence Tradecraft Project Overview

- ❑ SEI studying the state of cyber intelligence across government, industry, and academia in study, known as the Cyber Intelligence Tradecraft Project (CITP).
- ❑ Seeking to advance capabilities of organizations performing cyber intelligence by elaborating on best practices and prototyping solutions to shared challenges.
- ❑ From June 2012, six government agencies and 20 organizations from industry and academia provided information on their cyber intelligence methodologies, technologies, processes, and training.
- ❑ Baseline data was benchmarked against a cyber intelligence analytic framework consisting of five intelligence functions:
  - Environment
  - Data gathering,
  - functional analysis,
  - strategic analysis, and
  - stakeholder reporting and feedback.



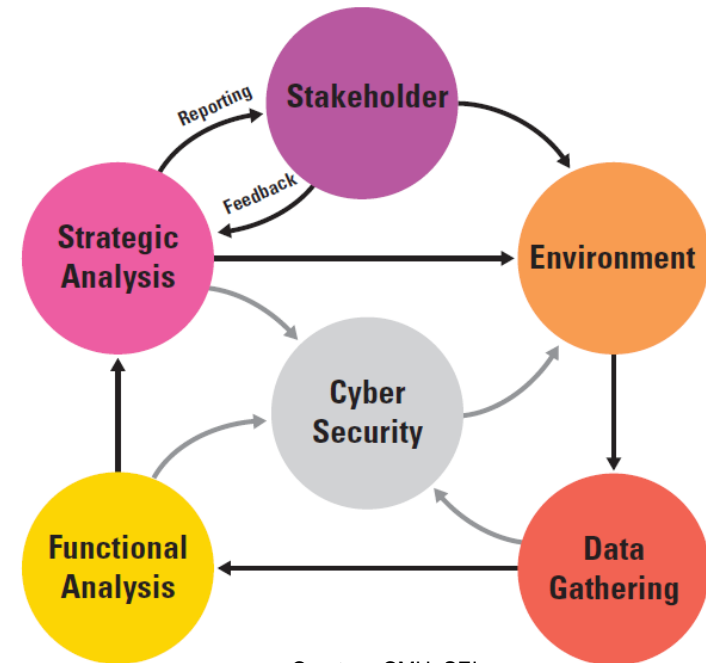
**Software Engineering Institute**  
Carnegie Mellon



[http://www.sei.cmu.edu/library/abstracts/whitepapers/CITP-Summary.cfm?wt.mc\\_id=goto50](http://www.sei.cmu.edu/library/abstracts/whitepapers/CITP-Summary.cfm?wt.mc_id=goto50)

# Cyber Intelligence Tradecraft Project Overview

- **Environment:** Top-sight on cyber footprint; cyber intelligence distinction with cyber security; role alignment; personnel to support cyber intelligence; organizational structure; workflow utilization; prioritization of threats; organizational situational awareness; cyber intelligence functional and strategic analysis; scope of past, present, and future analysis; insider threat and cyber intelligence relationship.
- **Data Gathering:** Collection requirements and sources relationship; information sharing; meeting analytical needs; technology facilitating data gathering; indexing and archiving of data; validation of sources.
- **Functional Analysis:** Workflow exists; timeliness in producing analysis; diversity with incorporating multiple technical disciplines; skills, knowledge, and abilities; tools utilized.
- **Strategic Analysis:** Distinguished from functional analysis; workflow exists; diversity with incorporating multiple technical disciplines; skills, knowledge, and abilities; tools utilized.
- **Stakeholder Reporting and Feedback:** Report types generated; reporting mechanism for actionable and predictive analysis; leadership influences format and production timelines; cyber intelligence influences decision making; feedback mechanisms exist; feedback influences data gathering and analysis; satisfying intelligence consumers; capturing return on investment.



Courtesy CMU SEI

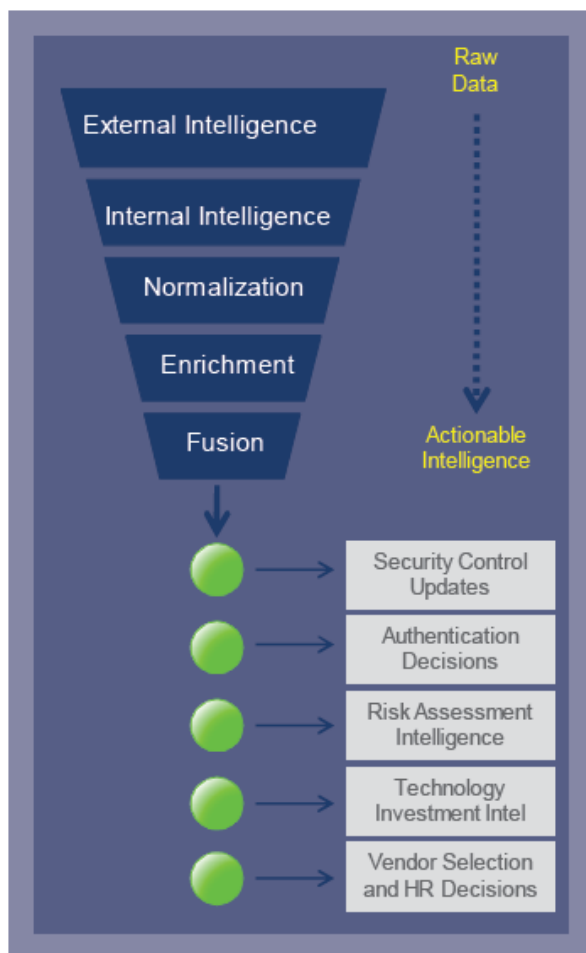


# Deloitte's View on CTI



*Predict, Prepare, Prevent  
Respond, Investigate*

## The New Approach for Cyber Security – Proactive



Draft – For Discussion Purposes Only



### A Forward Looking Cyber Threat Intelligence Capability

1. Conduct emerging threat research
2. Establish partnerships to share intelligence
3. Assign threat focus areas
4. Establish live, dynamic intelligence feeds
5. Implement a holistic approach to cyber threat identification
6. Actively track the cyber criminal element
7. Perform daily emerging threat reviews
8. Maintain awareness of the changing technology and business environment
9. Patch operating system, network, process, and application vulnerabilities
10. Deploy and maintain signature **and** behavioral based controls
11. Produce metrics and trending data for multiple key threat indicators
12. Continuously improve automation capabilities

- 5 -

Copyright © 2010 Deloitte Development LLC. All rights reserved.





# Deloitte's View on CTI



*Predict, Prepare, Prevent  
Respond, Investigate*

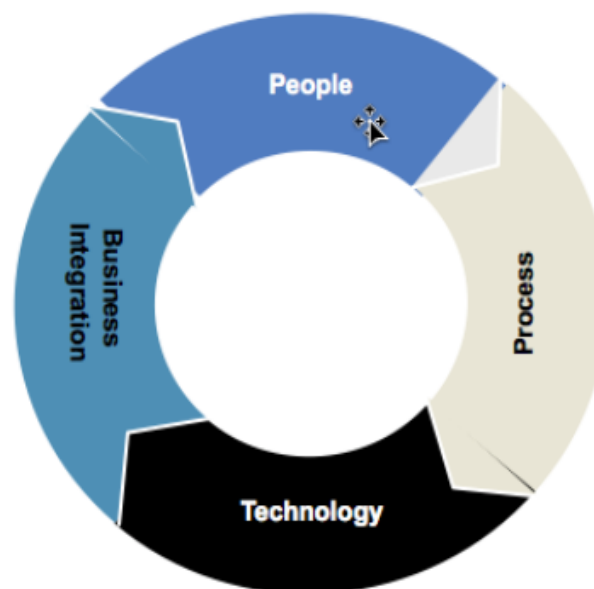
## Cyber Threat Intelligence Program Requirements Gathering Methodology

### Discussion Topics

- 1 **Discuss Mission and Mandate of Organization**
  - Responsibilities
  - Goals
  - Key Metrics
- 2 **Discuss Key Initiatives and Active Projects**
  - Regulatory
  - Audit Driven
  - Discretionary
  - Strategic Initiatives
- 3 **Discuss Areas that Require Attention and Prioritization**
  - Organization
  - Process
  - Technology
- 4 **Discuss Current State of Functions in Scope Using Diagnostic Framework**
  - Strengths
  - Maturity Level
  - Measurements
- 5 **Discuss Desired State Concepts and Strategies**
  - Internal Opportunities
  - External Opportunities

### Key Focus Areas

The scope of the discussion will focus on 4 measurement areas and will use a diagnostic framework for understanding current capabilities



*Draft – For Discussion Purposes Only*

- 6 -

Copyright © 2010 Deloitte Development LLC. All rights reserved.



# Deloitte's View on CTI



*Predict, Prepare, Prevent  
Respond, Investigate*

## Sample Leading Practices for a Cyber Threat Intelligence Function

### — 1. Organization —

- Resources dedicated toward- reviewing and analyzing emerging threats.
- Annual budget for security control upgrades, new detection tools, and intelligence sources.
- Cyber command center

### — 3. Malware Forensic Capability —

- Ability to rapidly collect and review forensic information from devices that are suspect.

### — 5. All Source Intel Fusion —

- Automated, monitored, incremental feeds with aging algorithm.
- Two-way, cross-industry intelligence sharing.
- Contingency plans for loss of intelligence sources.

### — 7. Threat Modeling —

- Capability to model and analyze the likelihood that an emerging threat will impact an organization and identify where the weaknesses are that will be exposed.

### — 9. Research and Development —

- Threat intelligence teams should work in conjunction with internal security teams to identify new strategies and solutions for testing and improving the security posture of customer devices and banking applications.

### — 2. Process —

- Daily regimen to review and communicate emerging threat data.
- Threat matrix
- Scenario planning

### — 4. Perimeter Monitoring —

- Network extrusion monitoring
- Network conversation recording and reconstruction

### — 6. Metrics and Reporting —

- Regular cyber bulletin updates.
- Threat briefings by line of business / delivery channel
- Automated custom alerting based on thresholds

### — 8. Threat Lifecycle Management —

- Case management tools to coordinate cyber incidents across multiple business areas and support organizations.

### — 10. Supporting Capabilities —

- Patch management
- Configuration management
- Vulnerability management
- Security event management
- Incident Response

Draft – For Discussion Purposes Only

- 8 -

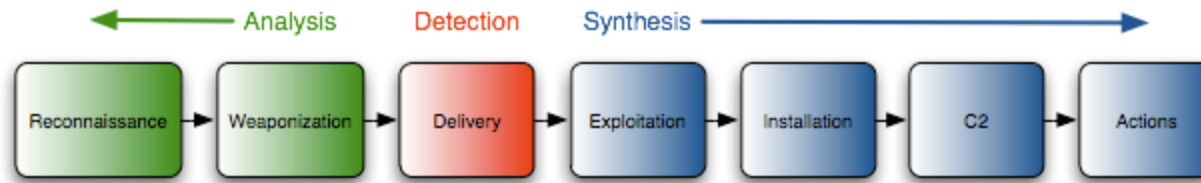
Copyright © 2010 Deloitte Development LLC. All rights reserved.





# INTELLIGENCE PRODUCTS

# Kill Chain Analysis



- Groundbreaking work by the Lockheed Martin Cyber Intel team on building a progressive model of the phases of an APT attack and mapping threat events and controls to it.
- Allows mapping of individual attacks to Campaigns and potentially actor attribution with enough data.





# COME THE REVOLUTION

# Marcus Sachs - 2006

## ❑ SRI Cyber Threat Analytics presentation:

### ❑ Next Generation Threat Management capabilities:

- Must support highly automated threat diagnosis and prioritization
- Must scale to alert volumes and data sources covering millions of IP addresses
- Must be able to rapidly distribute actionable information back to user communities
- Must be able to fuse data from multiple sources, most of which are not related
- Must also be sensitive to data privacy and anonymity concerns



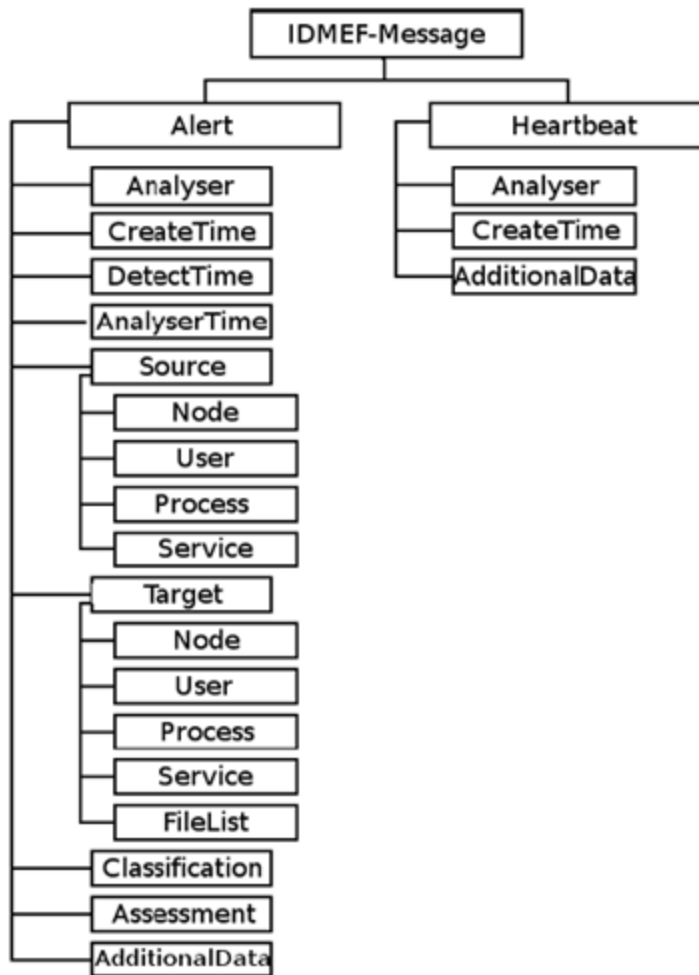
# Marcus Sachs - 2006

## ❑ Need to adopt innovative techniques such as

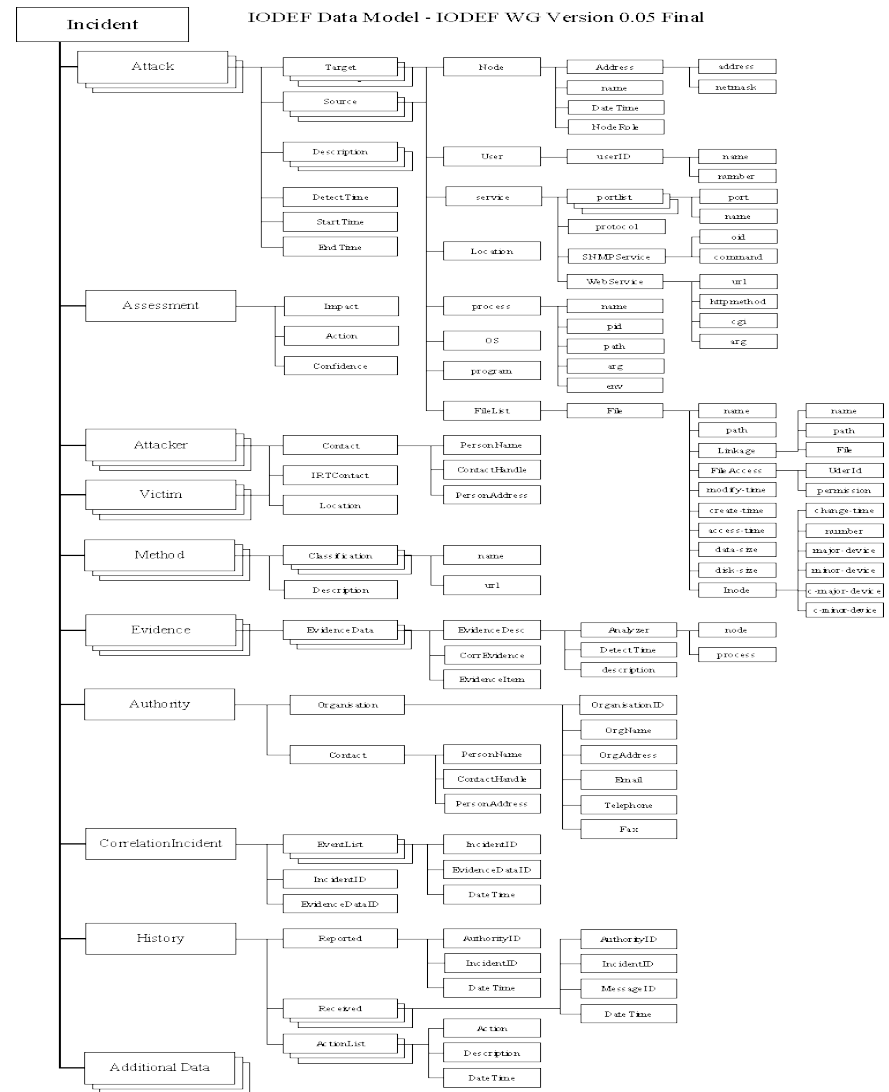
- Sensor meta-data sharing and analysis
- Publishing consensus-based signatures
- Sharing honeynet and malware collections
- Sharing botnet command and control data
- Dynamic updates to firewalls and IPSs
- Detecting changes to DNS, BGP, and other mechanisms
- Using application crash analysis tools for early detection of zero-day attacks



# Standards – Out with the Old...



[http://www.isoc.org/seinit/portal/images/stories/architecture/idmef\\_class.png](http://www.isoc.org/seinit/portal/images/stories/architecture/idmef_class.png)

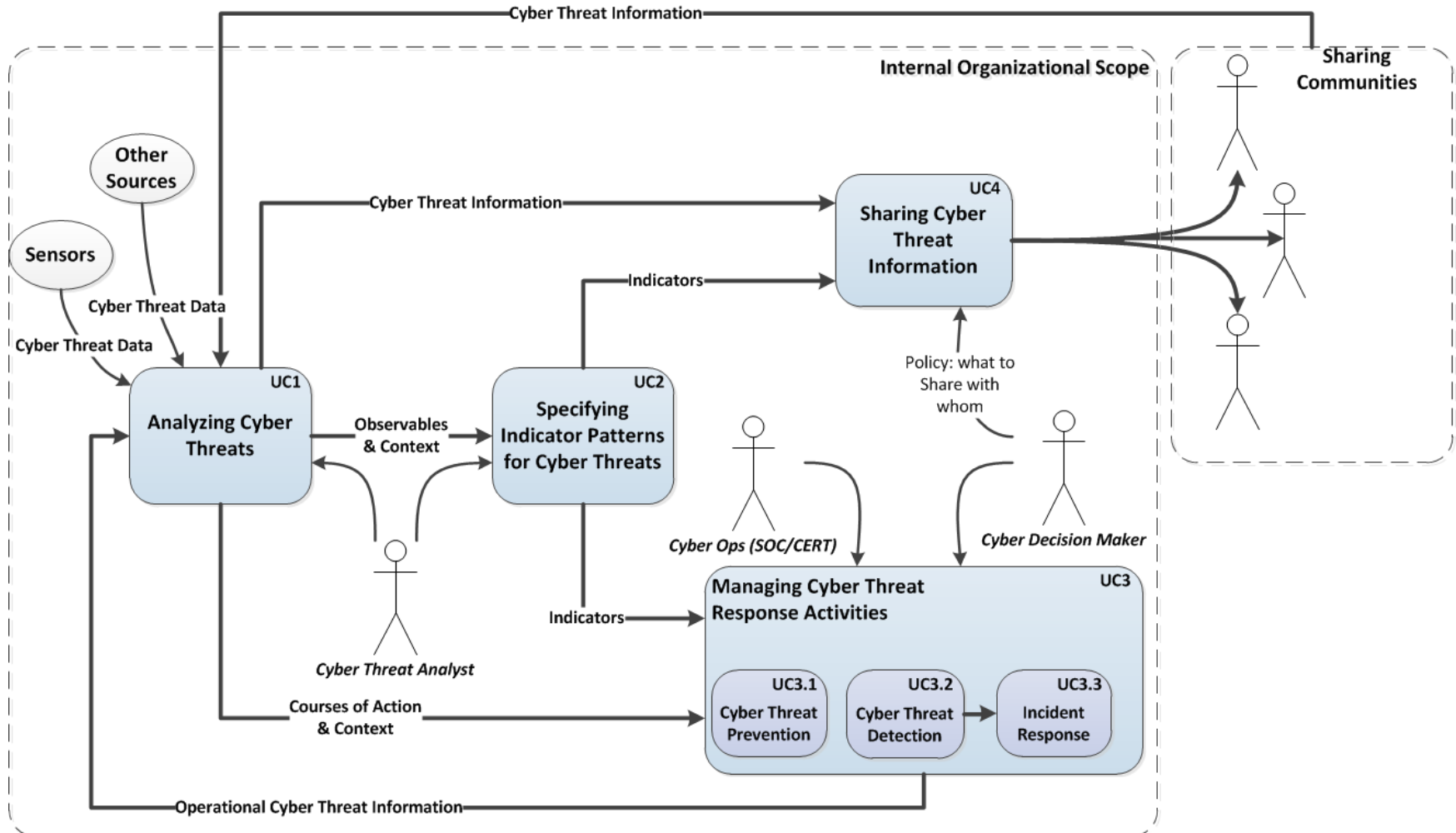


<http://www.terena.org/activities/tf-csirt/iodef/docs/iodef-datamodel-draft-005-final.html>





# Standards – In with the New...



**STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.**



# Crowdsourcing Intelligence

- ❑ Crowdsourcing aims to use the “wisdom of crowds” and was popularised by projects like Wikipedia.
- ❑ Applied Research Associates actually started the project last year with another website called [Forecasting Ace](#), which had over 2,000 registered contributors making predictions on everything from the future of space exploration to political elections.
- ❑ On the new website, [Global Crowd Intelligence](#), the company hopes that number will grow substantially by making forecasting more like a game of spy versus spy.

CODE RED | 10 October 2012

## Intelligence agencies turn to crowdsourcing



▼ Sharon Weinberger

Technology

Crowdsourcing

Data

Military

Science & Environment

Share f t p



(Copyright: Columbia Pictures)

US intelligence agencies hope the “wisdom of the crowd” can help them predict the future.

Courtesy BBC

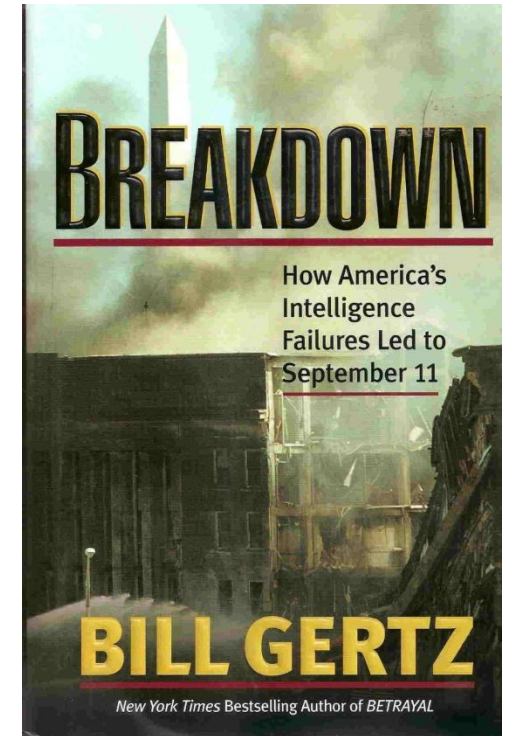
<http://www.bbc.com/future/story/20121009-for-all-of-our-eyes-only>

Images belong to their Copyright Holders



# CrowdSourcing in a Cyber Context

- ❑ Experience is, no one person or organization, including the Intelligence Community, has all the information or the correct analysis.
- ❑ Leveraging social media platforms, email distribution lists, trust groups like the FS-ISAC, to bounce information and analysis off
- ❑ Analytical rigor:
  - Peer review, test and defend your hypothesis and analysis



# Summary

## **We are in a revolutionary phase of intelligence driven cyber defense:**

- There are substantial intelligence capabilities in house and out on the street. Identify them and engage them as your program requires.
- Cyber Threat Intelligence informs comprehensive risk assessment and should be used to drive and prioritize both your intelligence and technology risk programs
- Cyber Threat Intelligence is not just tactical threat indicators, but a more comprehensive view of those actors who may impact you, their capabilities and motives and more tactically the things they will throw at you.
- Take a holistic view, and work from the inside of your organization to the outside.



# QUESTIONS



# Some References

- <http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf>
- <http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/>
- <http://makingsecuritymeasurable.mitre.org/docs/STIX-Whitepaper.pdf>
- <http://www.nedrix.com/presentation/0312/Evolving%20Cyber%20Threat%20Landscape-Rich%20Baich.pdf>
- <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf>

