



# Can Game Theory Save Us From Cyber Armageddon?



Barry Kouns, CEO  
Risk Based Security  
[barry@riskbasedsecurity.com](mailto:barry@riskbasedsecurity.com)

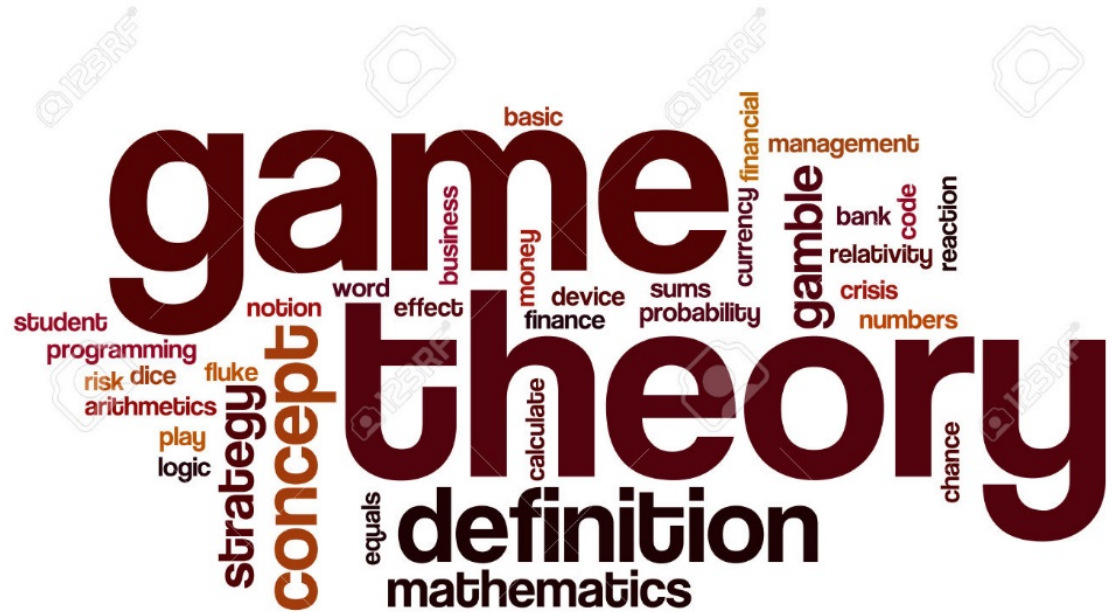


# Overview

- Game Theory Basics
- Mutually Assured Destruction (MAD)
- Current State of Cyber Threats
- Mutually Assured Cyber Destruction (MACD)
- Lessons for the Office

# Quick Poll #1

- How many of you have been exposed to using game theory?
- Did you use it to predict an outcome?
- Any game theory experts with us?
- How many of you know about MAD?



# Game Theory

- Models conflict and cooperation between rational decision makers.
- Assumes non-emotional behavior.
- Predicts events as people act in their own best interests.



# Game Theory, In Essence ...



- A computer model that considers the options open to the 'players', determines their likely course of action, evaluates their ability to influence others and predicts the course of events.

# The Most Popular Game Theory Exercise?

- The “Prisoners' Dilemma” is the most used example of game theory.
- How many of you heard of it?
- Anyone recognize the movie this picture is from?



# Prisoners' Dilemma

- Two persons were picked up on a suspicion of committing a crime. (They are both equally guilty, but the police have no proof).
- Both are moved to separate holding areas and questioned. Both are offered deals to reduce their jail time if they confess and rat on the other.
- Here's the game with the numbers representing years in prison.

		 Red	
		Quiet	Confess/Rat
 Blue	Quiet	Go Free Go Free	1 year 5 years
	Confess/Rat	5 years 1 year	2 years 2 years



# Prisoners' Dilemma

- Both prisoners would be better off if they both kept quiet.
- Human nature seems to drive us to not trust the other and think “better to get 2 years than 5” and both confess/rat instead.





# Poll #2

- If Red and Blue were related would the result be different?
- What if they were married?
- Seems like knowledge of or trusting the other person is key.

		 Red	
		Quiet	Confess/Rat
 Blue	Quiet	Go Free Go Free	1 year 5 years
	Confess/Rat	5 years 1 year	2 years 2 years



Forget the Prisoners, we had a  
Nuclear dilemma.



MAD

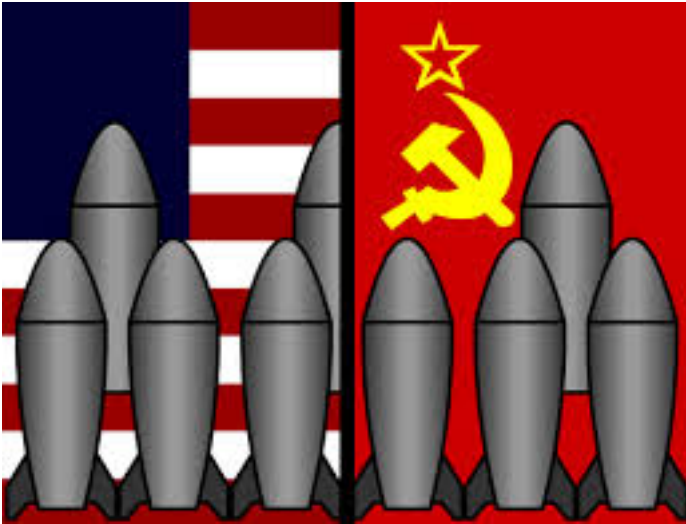
Mutually Assured Destruction

# Threat from USSR Army Neutralized



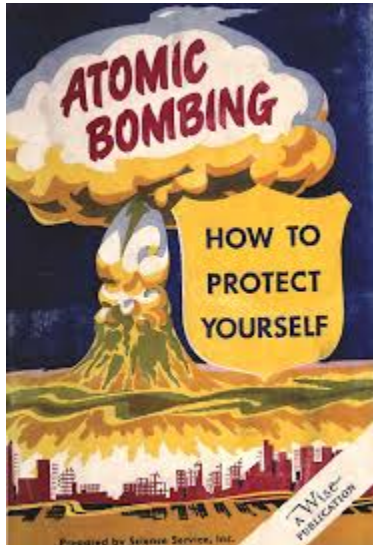
- After World War II tensions between the USA and the USSR escalated as the USSR realized the Atom bomb had neutralized the might of their vast army.

# Nuclear Arsenal Build-up



- The USSR soon had an Atom bomb of its own and both sides began a build-up of nuclear weapons, (Cold War).

# Fear of a Nuclear Attack .. No Doctrine



- With suspicions growing and as fear of a nuclear exchange (Armageddon) gripped both sides, both nations struggled to develop a strategic nuclear doctrine.

# The Doctrine



- The eventual doctrine, developed by Game Theory experts at the RAND corporation, was named MAD, Mutually Assured Destruction.



# Nuclear War Avoided

## The Evolution of Deterrence

The McNamara Years



- MAD is largely attributed with preventing any full-scale conflicts between the United States and the USSR.

# MAD

- Game Theory was used to examine nuclear strategy during the Cold War.
- MAD was based on the **Prisoner's Dilemma**.

			
		No Action	First Strike
	No Action	0 Loss 0 Loss	90% Loss from Retaliation 90% Loss
	First Strike	90% Loss 90% Loss from Retaliation	Annihilation Annihilation

# MAD

A STRANGE GAME.  
THE ONLY WINNING MOVE IS  
NOT TO PLAY.

*Joshua from "War  
Games"*

# US Mutual Deterrence Doctrine



# Assumptions Behind MAD ...

- Each side has enough weaponry to destroy the other side.
- Each side if attacked, could and would retaliate with equal or greater force.
- Each side believed there was no possibility of camouflaging a launch.
- Each side believed no rogue states will develop nuclear weapons.



# MAD Assumptions ...

- Each side could not defend itself against the other's nuclear attack.
- Each side had to believe that once initiated a retaliatory strike could not be stopped.
- Each side must have perfect detection equipment.
- Each side must show their commitment to MAD.



- Each side had the ability for perfect attribution of the launch.





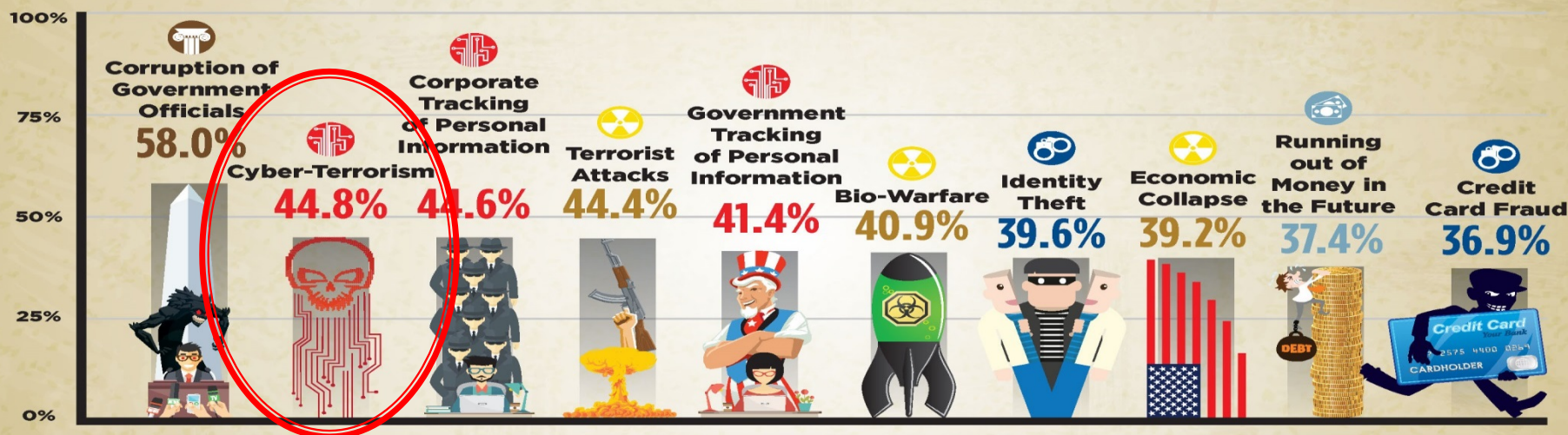
# Poll #3

- Anyone know when the Cold War ended?
- Has the Cold War ended?
- Has the risk of nuclear war diminished since the Cold War?
- Has the fear of nuclear war been replaced with worrying about cyber war?



# Nuclear War Not in Top 10 Fears – Cyber #2

## Top 10 Fears of 2015



Above are the 10 fears for which the highest percentage of Americans reported being “Afraid,” or “Very Afraid.”

Government Technology Man-made Disasters Crime Personal Future

The Chapman University Survey of American Fears 2015

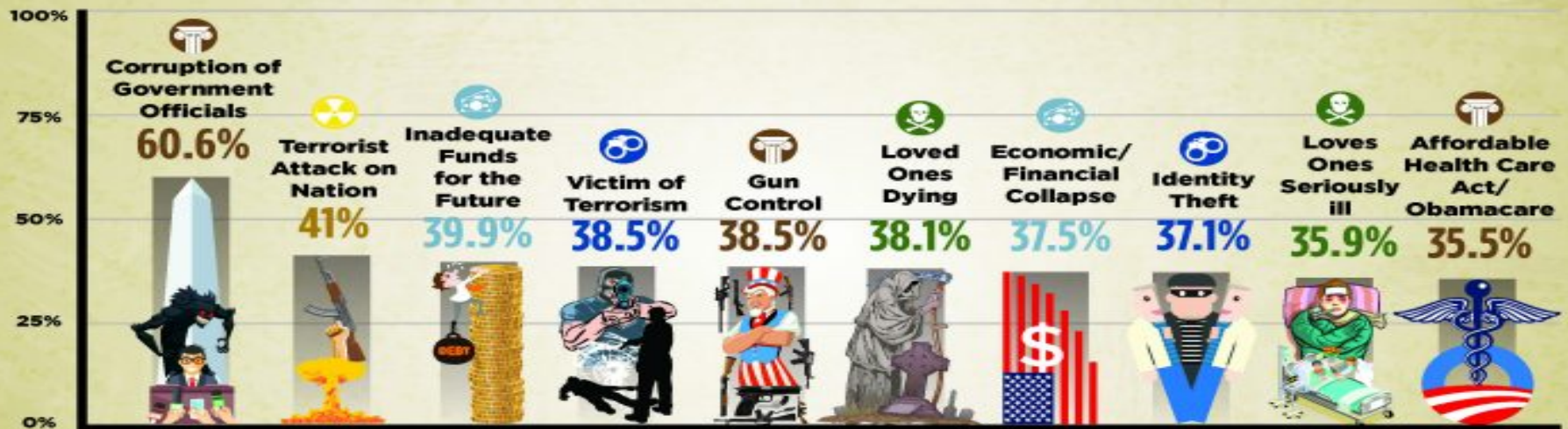


CHAPMAN UNIVERSITY  
ORANGE, CALIFORNIA



# Neither Nuclear or Cyber War in Top 10 Fears

## Top 10 Fears of 2016



Above are the 10 fears for which the highest percentage of Americans reported being "Afraid," or "Very Afraid."

 Government  Illness and Death  Man-made Disasters  Crime  Economic

The Chapman University Survey of American Fears 2016



CHAPMAN UNIVERSITY  
ORANGE, CALIFORNIA

# And Yet ...

**North Korea on 'inevitable' path to nuclear ICBM:**  
*US DIA chief says if left unchecked, it's only a matter of time before Pyongyang can strike the US with a nuclear missile.*



Ballistic missile were paraded through Kim Il Sung Square last month. (Wong Maye-E/AP Photo)



# And Yet ...

Russia declares  
US relations in  
'worst period'  
since the Cold  
War.

Alexey Eremenko, Alastair  
Jamieson & Abigail  
Williams  
Tuesday, 11 Apr 2017 |  
10:32 AM ETNBC NEWS

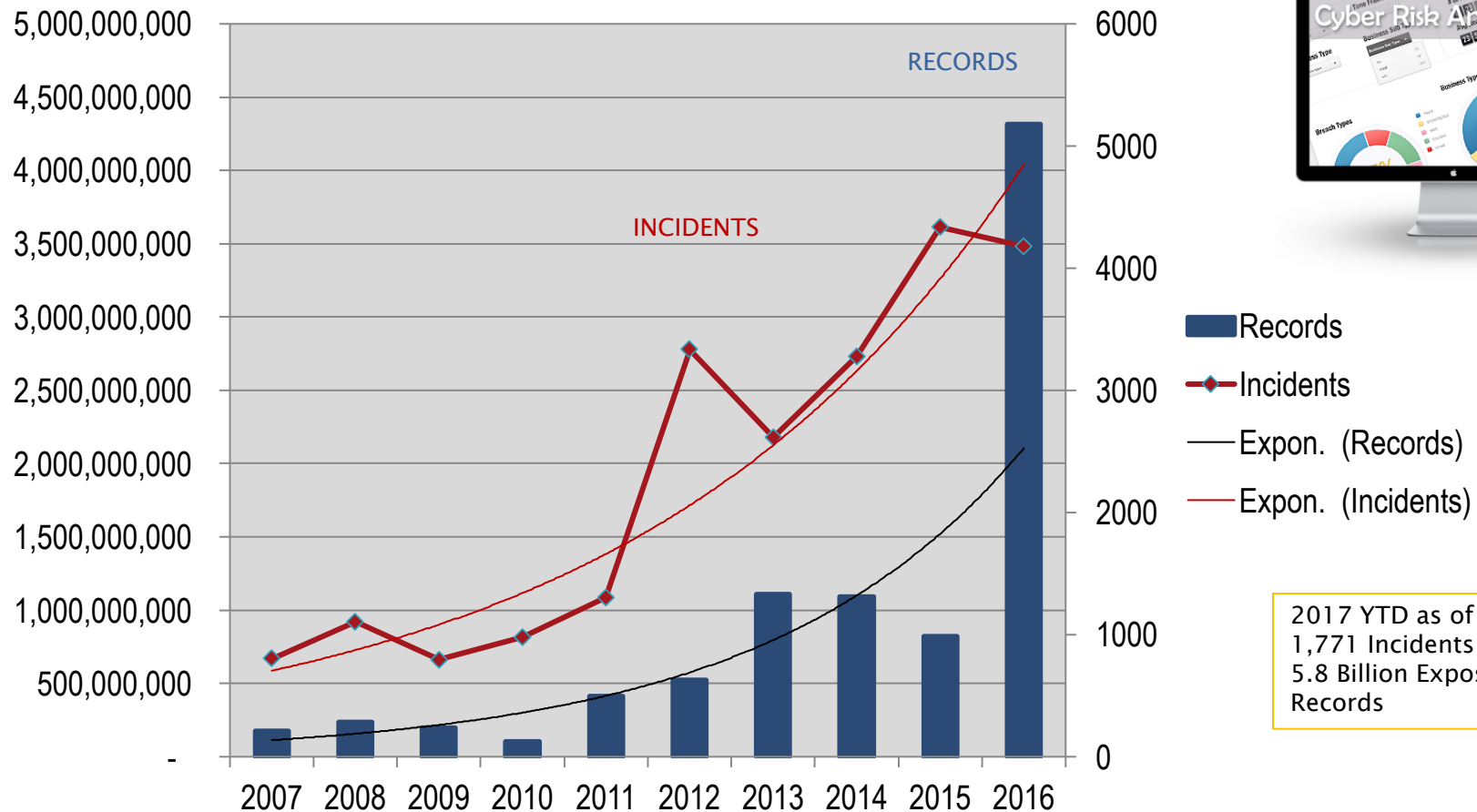




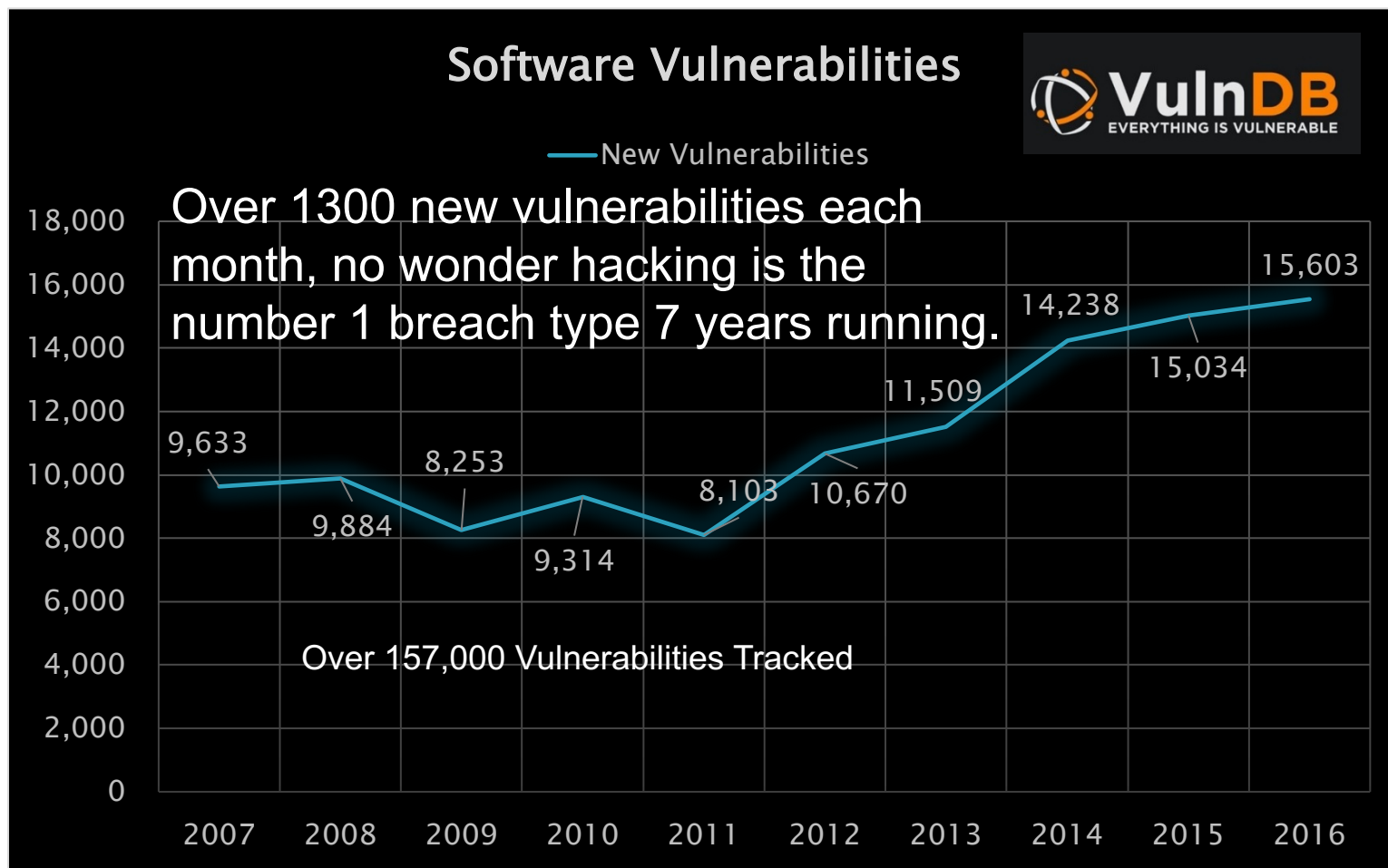
But, should we fear Cyber Armageddon?



# The Number of Data Breaches Point to Yes



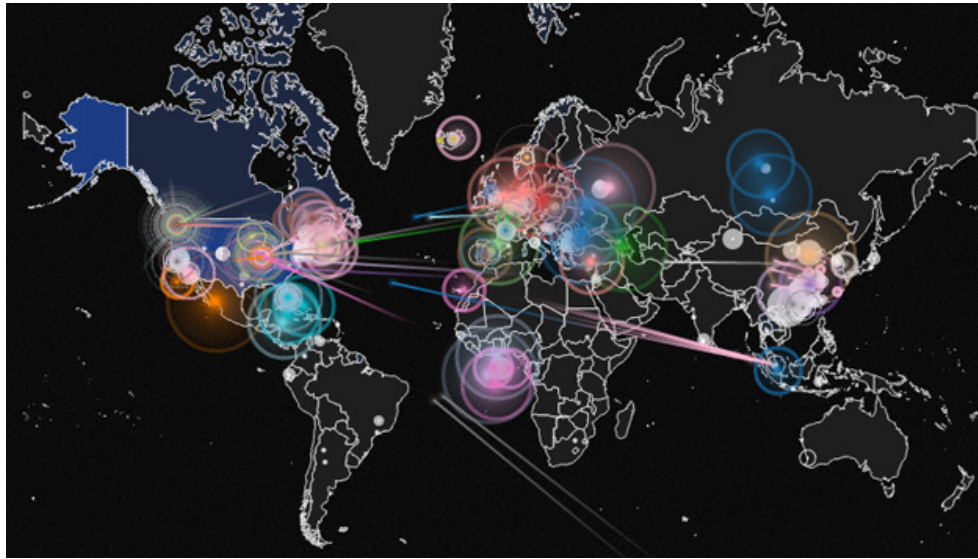
# Number of New Vulnerabilities Points to Yes



# Staggering Numbers

## Cyber Attacks Light Up the Map

Nearly 1  
million new  
malware  
threats  
released  
every day  
[Money.cnn.com](http://Money.cnn.com)

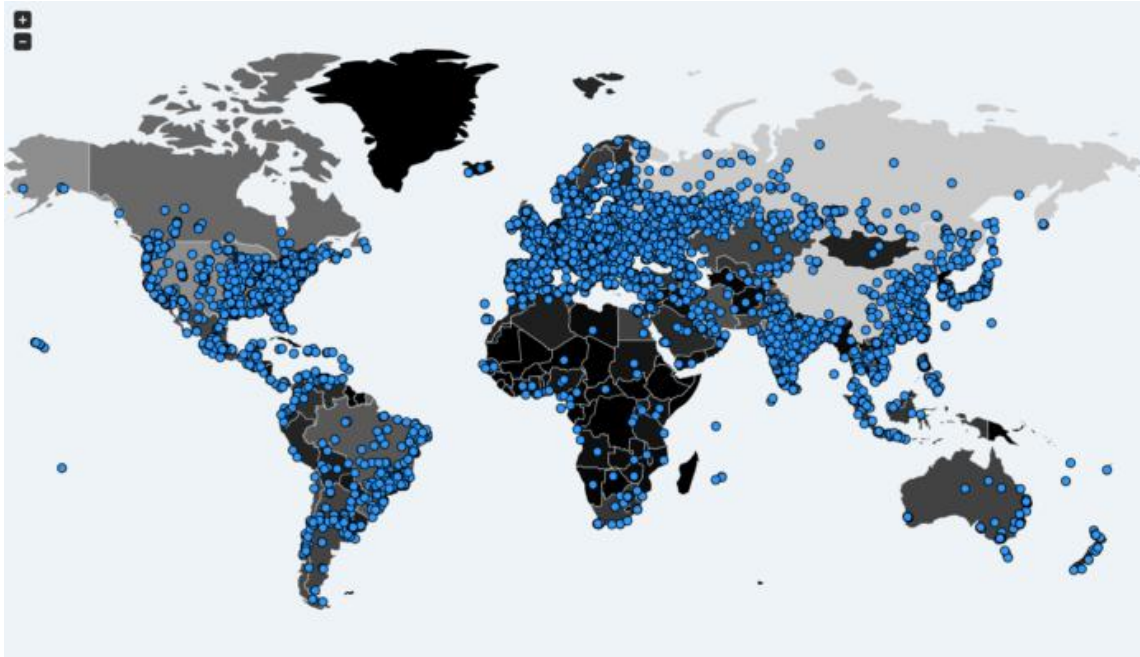


NSA Data  
Center  
Experiencing  
300 Million  
Hacking  
Attempts Per  
Day  
[The Hacker News](http://The Hacker News)

UK businesses were hit 230,000 times each by cyber-attacks in 2016  
[cnbc.com](http://cnbc.com)

Russia tops list of 100 countries that could launch cyberattacks on US  
Mike Levine, May 18, 2017, 11:54 AM ET

# Most Recent Global Cyber Attack?



WannaCry infects more than 200,000 systems in over 150 countries around the world.

# Poll #3 continued

- Have you heard of the term [“Fire Sale?”](#)



# Fire Sale

*Matt Farrell:* Man! It's a fire sale.

*John McClane:* What?

*Matt Farrell:* It's a fire sale.

*Deputy Director Bowman:* Hey! We don't know that yet.

*Taylor:* Yeah, it's a myth anyway. It can't be done.

*Matt Farrell:* Oh, it's a myth? Really? Please tell me she's only here for show and she's actually not in charge of anything.

*John McClane:* Hey, what's a fire sale?

*Matt Farrell:* It's a three-step... it's a three-step systematic attack on the entire national infrastructure. Okay, ...

- Step one: Take out all the transportation
- Step two: Take out the financial base and telecoms.
- Step three: You get rid of all the utilities. Gas, water, electric, nuclear. Pretty much anything that's run by computers which... which today is almost everything.
- So that's why they call it a fire sale, because everything must go.





# Government Actions

France has a  
'fourth army' of  
young hackers  
for cyber warfare

Business Insider-Apr 5, 2017



# Government Actions

UK will enact legislation to adopt the Network & Information Security Directive (NIS) and the General Data Protection Regulation (GDPR) will also come into force.



# Government Actions

## China Restructures Military, Enhances Cyber-Warfare Capabilities

Breitbart News-Apr 19, 2017



# Government Actions

THE WHITE HOUSE,  
May 11, 2017.

## Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure



# Government Actions

Germany  
activates  
new cyber  
warfare unit

World Socialist  
Web Site-Apr 7,  
2017





# Government Actions

The US Army  
Wants to Call  
in Cyber Attacks  
Like Artillery Fire  
The Drive-Apr 18, 2017





# Poll #4

- Do you think Cyber warfare is in our future?
- Do you think nuclear retaliation for a cyber attack is possible?
- Can the same Game Theory be used to save us from Cybergeddon?



# Mutually Assured Cyber Destruction (MACD)

# Do the same MAD assumptions hold-up?

## MAD Assumption: Each Side ...

1. Has enough weaponry to destroy the other side
2. If attacked for any reason by the other, could and would retaliate with equal or greater force
3. Believes there is no possibility of camouflaging a launch
4. Believes no rogue states will develop nuclear weapons (or, if they do, they will adopt the logic of MAD)
5. Cannot defend itself against the other's attack

## MACD



# Do the same MAD assumptions hold-up?







## MAD Assumption: Each Side ...

6. Believes that once initiated a retaliatory strike could not be stopped
7. Has perfect detection equipment with no false positives
8. Will demonstrate its commitment to MAD
9. Has the ability for perfect attribution of an attack

## MACD



# Prisoners' Dilemma Work Here?

										<b>50+ Others</b>	
		No Action	First Strike	No Action	First Strike	No Action	First Strike	No Action	First Strike	No Action	First Strike
	No Action	0 Loss 0 Loss	80% Loss from Retaliation 90% Loss	0 Loss 0 Loss	80% Loss from Retaliation 90% Loss	0 Loss 0 Loss	80% Loss from Retaliation 90% Loss	0 Loss 0 Loss	80% Loss from Retaliation 90% Loss	0 Loss 0 Loss	80% Loss from Retaliation 90% Loss
	First Strike	90% Loss 90% Loss from Retaliation	Annihilation Annihilation	90% Loss 90% Loss from Retaliation	Annihilation Annihilation	90% Loss 90% Loss from Retaliation	Annihilation Annihilation	90% Loss 90% Loss from Retaliation	Annihilation Annihilation	90% Loss 90% Loss from Retaliation	Annihilation Annihilation

What game theory exercise would be better?

# Assumptions Guiding a MACD Doctrine

- Cyber war is a “game” with multiple moves with many players exchanging attacks.



- There are five cyber warfare super powers plus as many as 100 others that could wage an attack.





# Assumptions Guiding a MACD Doctrine



- The proliferation of cyber weapons is impossible to control.



- All governments are working to improve cyber capabilities.

# Assumptions Guiding a MACD Doctrine

- All Cyber-attacks are not acts of war.
- Less technologically developed nations are not equally vulnerable to cyber-attacks compared to the US or European nations.



# Assumptions Guiding a MACD Doctrine



- Assured Destruction from a cyber-attack is not a guarantee.



- Attribution for an attack could take days/weeks/months.

# Attribution – Not an Exact Science



- Deterrence is highly dependent on the ability to distinguish the source of the attack (attribution) and the motivation of the attacker.

<http://www.secmeme.com/2017/05/copy-attribution-for-copy-cyber-threat.html>

# Proposed MACD Tenants

1. Publish what is considered an act of cyber warfare. (Draw the Line)
2. Be recognized as a cyber super power. (Carry a big stick)
3. Obtain perfect attribution capability. (Let them know that we will know)
4. Publish a Retaliatory Response Plan. (Define the pain they can expect in return)
5. Ensure resiliency. (Deny them the hope of victory)
6. Build a global coalition of Cyber-Nations. (Attack one you attack us all)
7. Muster the will to execute the plan. (Demonstrate resolve)



# Poll #5

1. What type of cyber-attack would you consider an act of war?
2. Do NATO member obligations extend into cyber warfare?
3. Can a doctrine of MACD work to deter Cybergeddon?
4. What, if anything, can we learn from preparing for Cybergeddon?



# Lessons for the Office

# Seven Steps in a Successful Cyber-Attack

1. **Reconnaissance** - identify a vulnerable target and explore the best ways to exploit it.
2. **Scanning** - identify a weak point that allows access.
3. **Access and Escalation** - gain access and then escalate, usually with privileged access credentials.
4. **Exfiltration** - extract data, change or erase files.
5. **Sustainment** - stay in place quietly, ensuring an easy path to return.
6. **Assault** – stealth no longer important, alter or disable functionality.
7. **Obfuscation** - trail of obfuscation to confuse, disorientate and divert the forensic process to assign attribution.

POSTED IN EXPLOIT DEVELOPMENT, GENERAL  
SECURITY, HACKING ON JUNE 11, 2015  
ETHICAL HACKING TRAINING – RESOURCES (INFOSEC)

# Reduce Your Attack Surface

1. **Reconnaissance**
2. **Scanning**
3. **Access**



Are Your Cyber Threat Intelligence Feeds Doing All They Can?

- The key to avoiding a cyber attack is minimizing exploitable vulnerabilities.
- If you have access to, and act upon, the latest vulnerabilities, you have a fighting chance to avoid being compromised.
- Minimize your potential attack surface. Identify, Prioritize, Mitigate - Repeat.

POSTED IN EXPLOIT DEVELOPMENT, GENERAL SECURITY, HACKING ON JUNE 11, 2015  
ETHICAL HACKING TRAINING – RESOURCES (INFOSEC)

# Vulnerability Intelligence

1. CVE/NVD is far from a complete list of vulnerabilities.
2. Know what your scanner/service provider is using for a vulnerability feed.
3. Using CVSS to set priorities is a good start, but a “critical asset” review will uncover lower CVSS scores that need mitigation.
4. Integrate Common Platform Enumeration to determine what is running on each asset down to the exact version. Skip the vulnerability scanner guesswork and go straight to mitigation.
5. Don't forget Application security.
6. Don't accept mounds of data without prioritized mitigation actions.

*Ed Bellis, Kenna Security*

<https://www.alienvault.com/blogs/security-essentials/7-guidelines-for-vulnerability-management-scanning>



# Once they are in ...

1. Reconnaissance
2. Scanning
3. Access and Escalation
4. Exfiltration
5. Sustainment
6. Assault
7. Obfuscation

- Each step starting with number three requires privileged credentials to succeed.
- The key to minimizing a cyber attack is controlling privileged access.
- If you have the ability to control privileged access, a cyber attack can be significantly mitigated.



POSTED IN EXPLOIT DEVELOPMENT, GENERAL  
SECURITY, HACKING ON JUNE 11, 2015  
ETHICAL HACKING TRAINING – RESOURCES (INFOSEC)

# Implementing Privileged Identity Management

1. Create account holder profiles – what they may and may not do.
2. Create a privileged user account management policy.
3. Identify a responsible party to implement the policy.
4. Inventory and review privileged accounts regularly.
5. Audit privileged accounts for access creep.
6. Consider tools or specialized products for managing the accounts.

MANAGE, MONITOR AND AUDIT  
PRIVILEGED USERS

# Prepare by Playing Cyberwar Games

SHALL HE PLAY A GAME?

# Prepare by Playing Cyberwar Games

1. Conduct 'tabletop' cyber war games.
2. Much like a BCP/DR exercise, but focused on a potential cyber-attack.
3. Consider scenarios not directed at you. (Transportation, Financial Sector, Utilities, SaaS, Key Partners, Clients)
4. Shoot for asset and business process relevant and realistic.
5. Extend the circle - Involve product development, infrastructure, customer relations, operations, marketing, legal, government affairs, and corporate communications in addition to IT and security.

Tucker Bailey and James Kaplan; McKinsey Associates

# War Game Objectives

- Realistic simulated cyber-attacks.
- Exercise business continuity plans as needed.
- Exercise technology, processes, and people.
- Build confidence in resistance, reaction, recovery, and resuming normal operations.
- Witness your team's situational analysis, decision making, and communication.



# Parting Bullets...

- Cyber Warfare is better understood by playing Mind Craft or Strike Force.
- The cyber super powers need to adopt and publish a MACD doctrine.
- Deterrence is achieved when opposing sides are convinced that neither can win.
- Although prevention is unlikely, we can lessen the severity of a cyber-attack.
- While we wait for governments to take action, there are some things (beyond duck & cover) we can do to protect ourselves.

# Or Just Maybe it's All About Money

*“A wise cynic might suggest that the operations researchers on both sides were playing a cunning strategy in a game over funding, one that involved them cooperating with one another in order to convince their politicians to allocate more resources to weapons.” ~ Don Ross*



Thank you for your attention

Barry Kouns  
Risk Based Security, Inc.  
Email: [barry@riskbasedsecurity.com](mailto:barry@riskbasedsecurity.com)