CIS™ Center for Internet Security®

Stranger in a Changed Land

International Conference on Cyber Warfare and Security

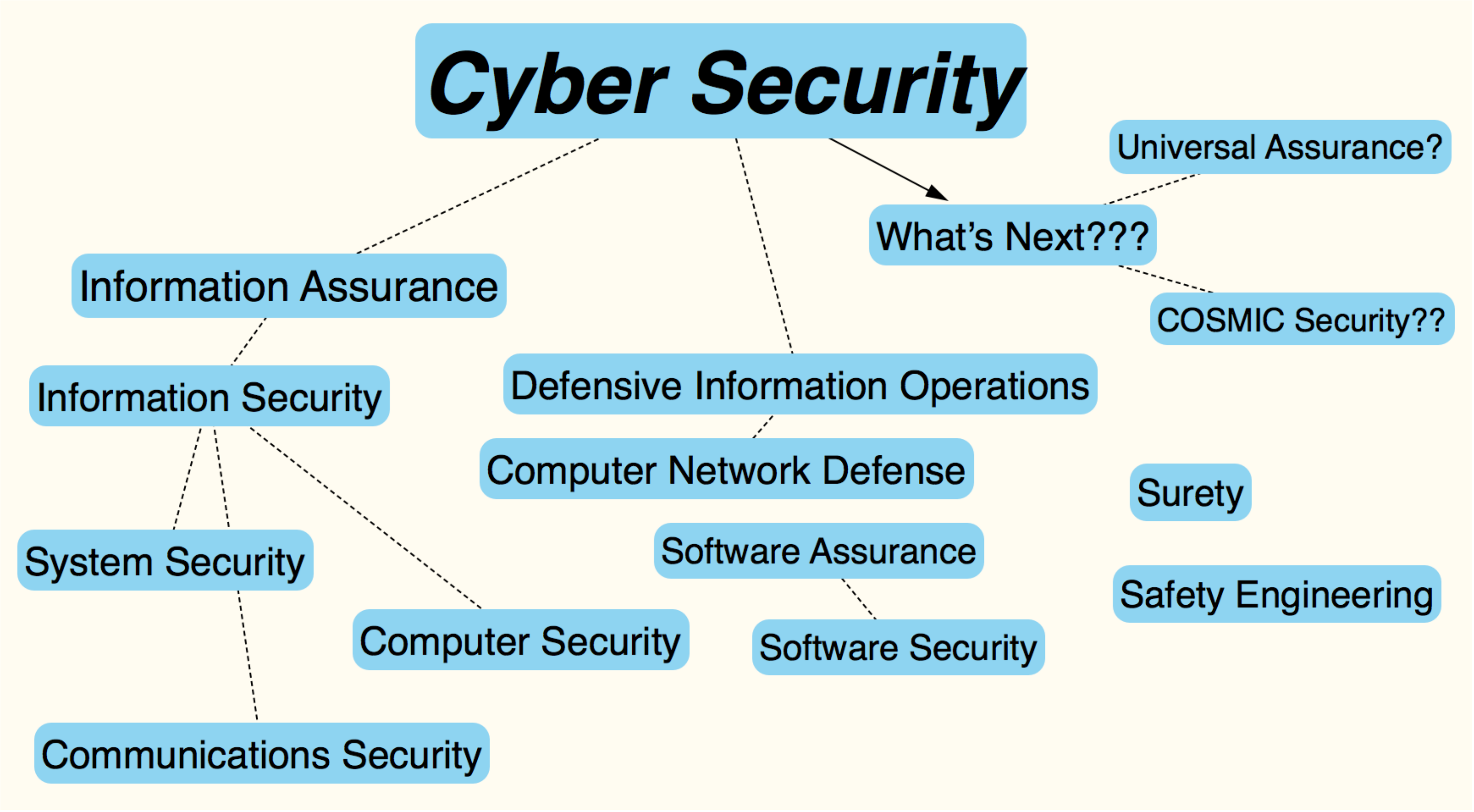
March 2022

Tony Sager

Senior VP & Chief Evangelist

Center for Internet Security

The Long and Winding Road….



Cyber Security

Universal Assurance?

What's Next???

COSMIC Security??

Information Assurance

Information Security

Defensive Information Operations

Computer Network Defense

Surety

System Security

Software Assurance

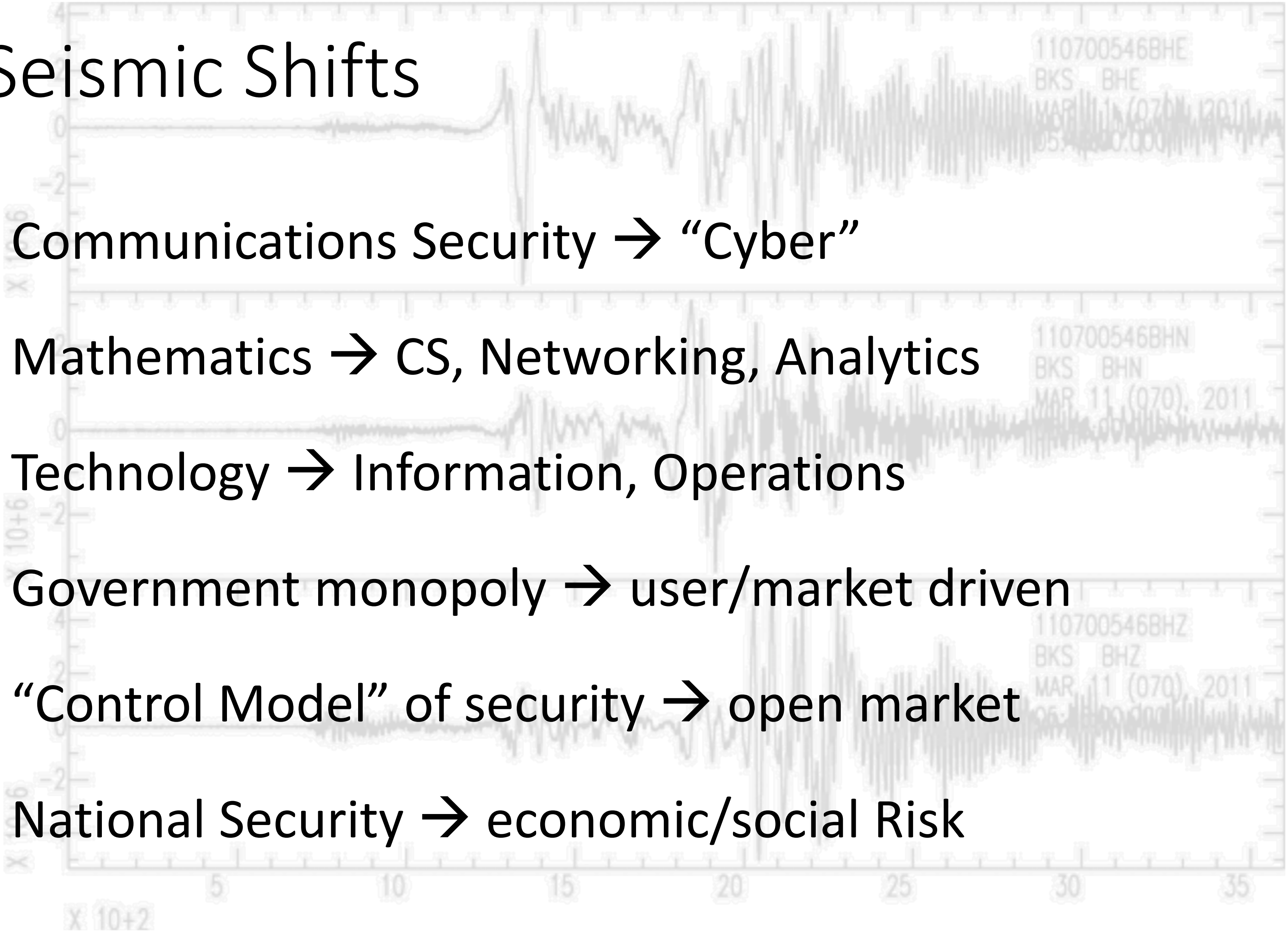
Safety Engineering

Computer Security

Software Security

Communications Security

Seismic Shifts



- Communications Security → “Cyber”
- Mathematics → CS, Networking, Analytics
- Technology → Information, Operations
- Government monopoly → user/market driven
- “Control Model” of security → open market
- National Security → economic/social Risk

A few lessons

- Knowing about flaws doesn’t get them fixed
- In Cyberspace, we all have more in common than different
- The Bad Guy doesn’t perform magic
    - and most attacks are repeats of a pattern
- There’s a large but limited number of defensive choices
    - and the 80/20 rule applies (The Pareto Principle)
- Cyber Defense is really Information Management
    - and when you see *“share”,* replace with *“translate”* and *“execute”*
- Cybersecurity is not an event, a tool, or training – it’s a machine
    - fueled by information
    - the optimal place to solve a security problem is …. *not* where you found it

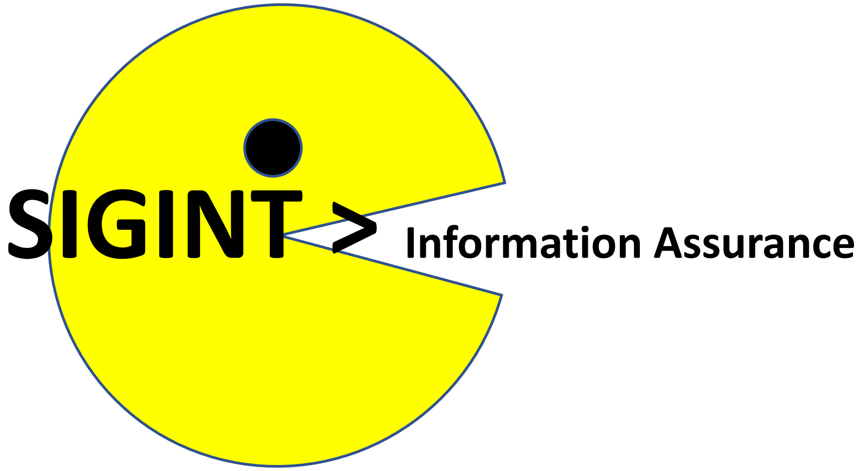
The National Security Agency (NSA)

Never Say Anything? *Not Seen Anywhere?* *Needs Scant Attention?*

- Signals Intelligence (SIGINT)
- Cybersecurity (from COMSEC, INFOSEC, Information Assurance…)

Offense + Defense = ???

The National Security Agency (NSA)



SIGINT > **Information Assurance**

- Resources
- Culture
- Recognition
- Leadership Attention

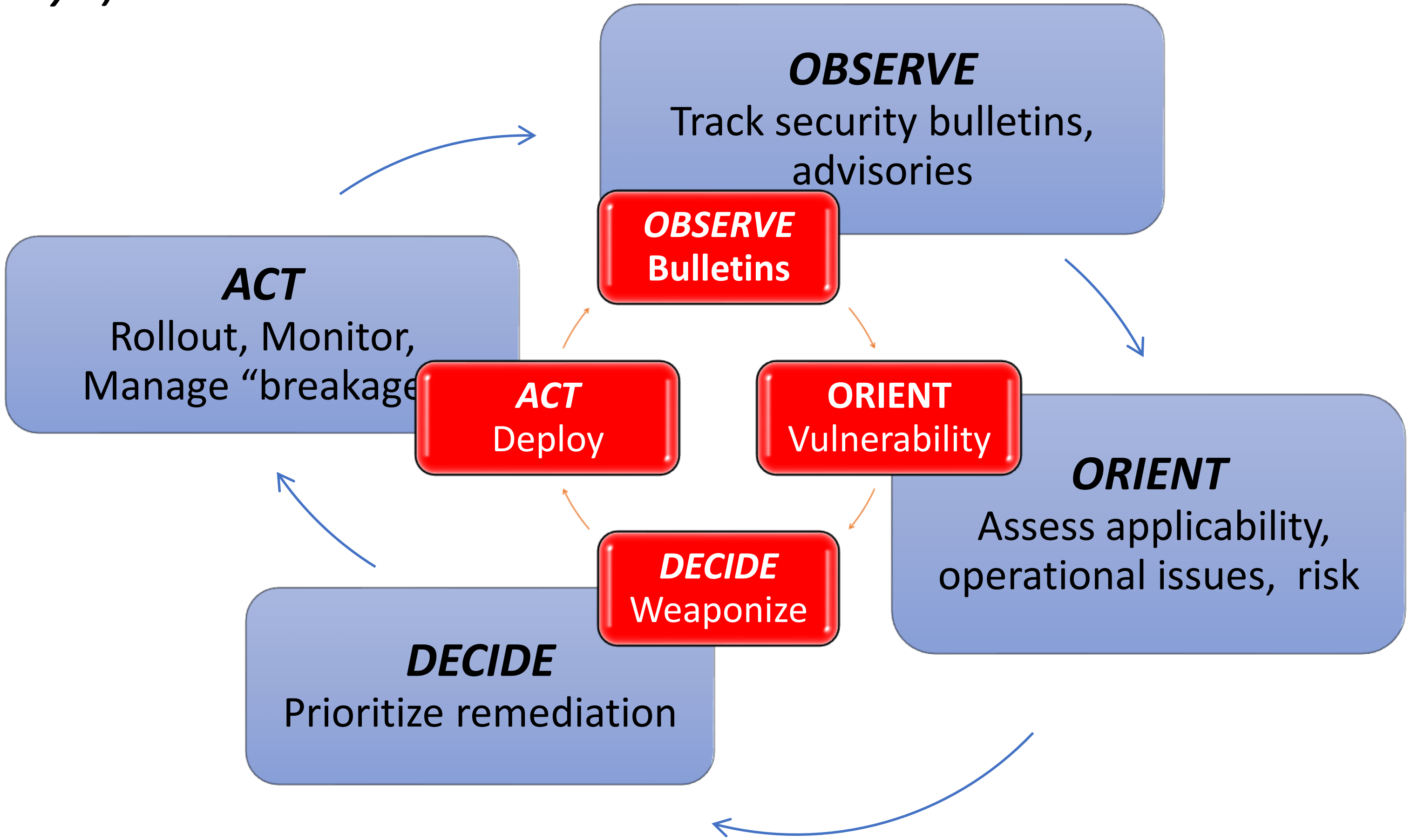
Defense wins games,
Offense wins budgets!

Offense + Defense =?

- Cross-training
- Access to resources (financial, technology, think-tanks…)
- Linkage to the ecosystem (Industry, Policy-Makers, Academia)
- World-wide insight
- Embedded in a highly complex infrastructure

A Cyberdefense OODA Loop

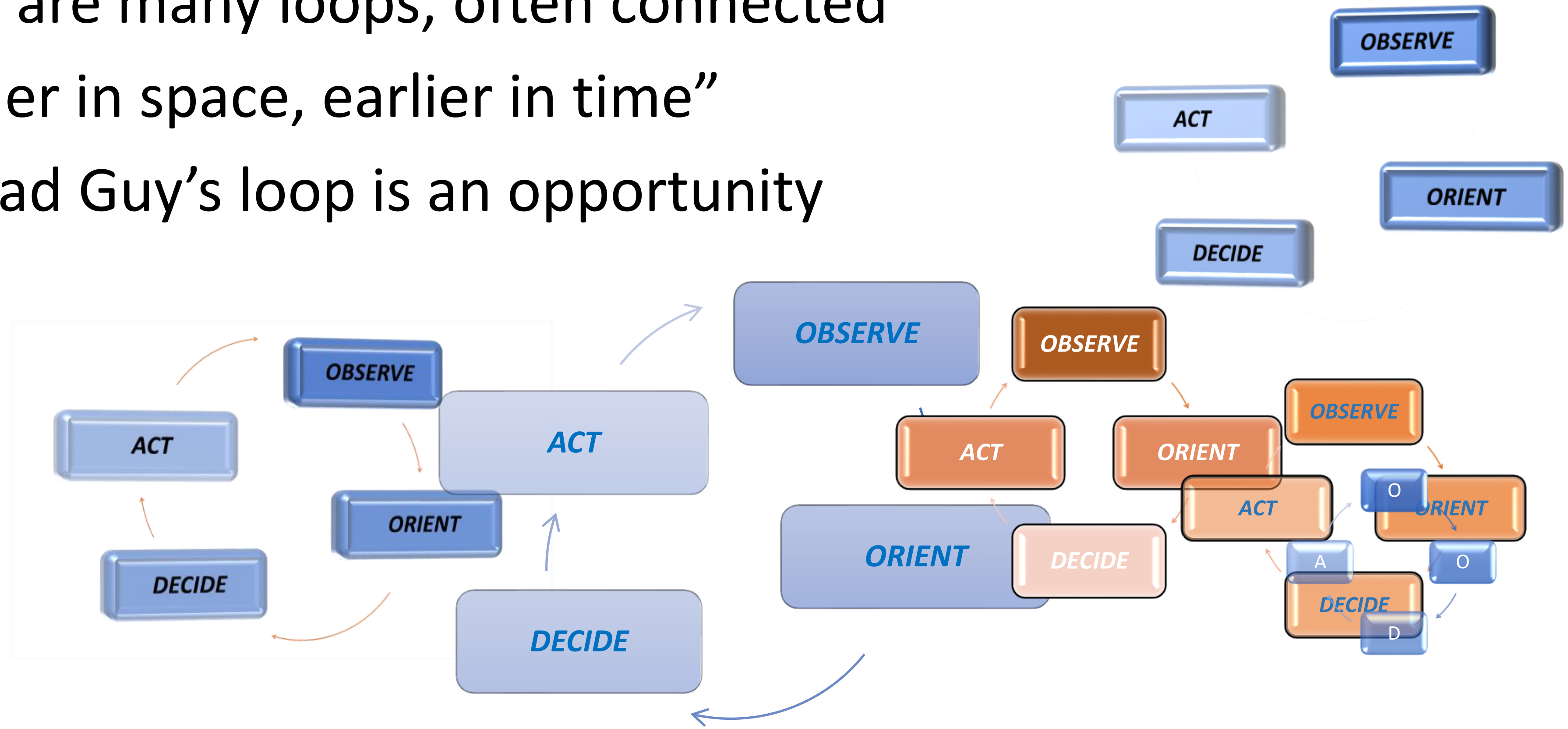
("Patch Tuesday")

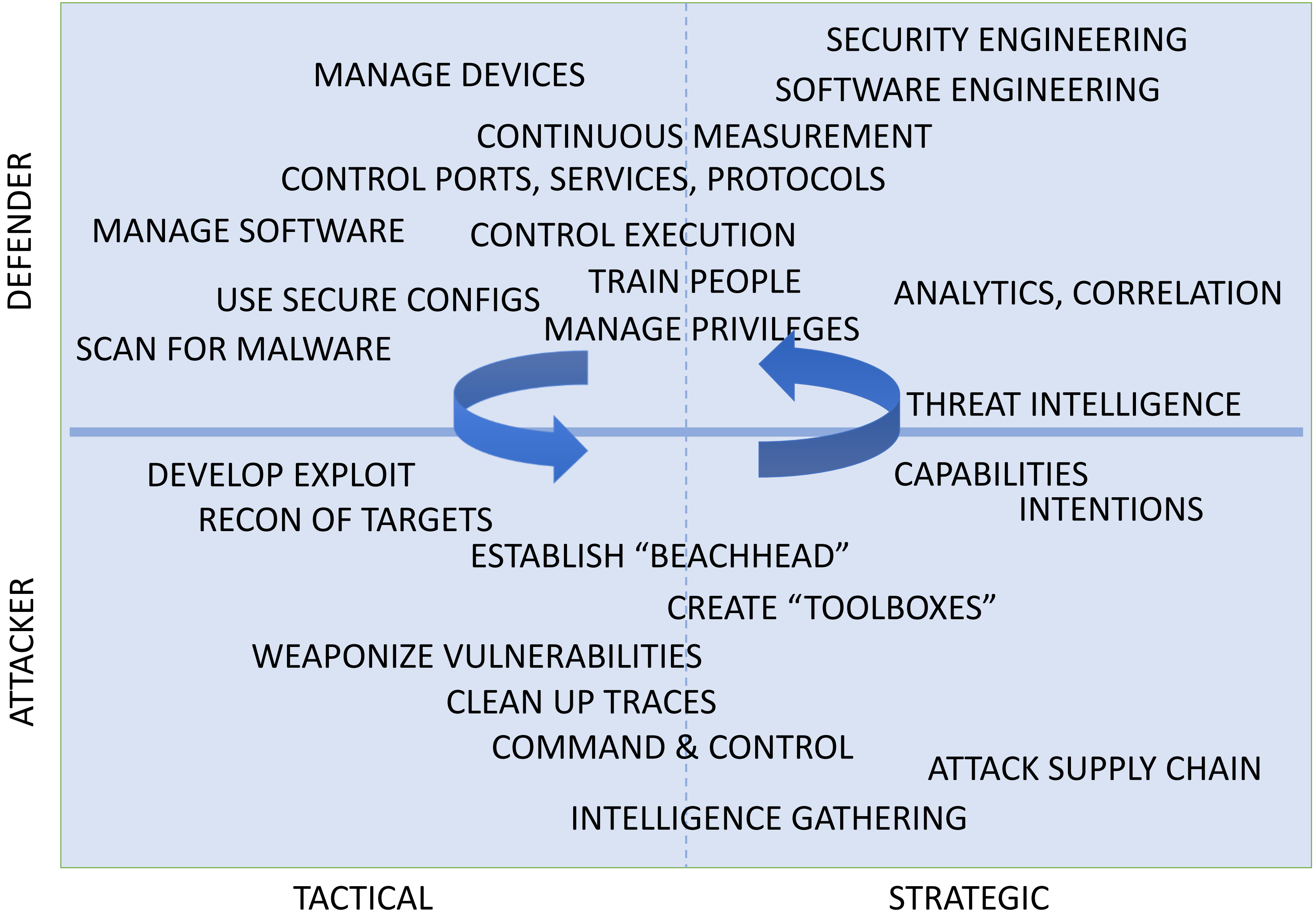


“Dueling OODAs”

(and the role of Threat Intelligence, Analytics)

- There are many loops, often connected
- “farther in space, earlier in time”
- The Bad Guy’s loop is an opportunity





SECURITY ENGINEERING

MANAGE DEVICES

SOFTWARE ENGINEERING

CONTINUOUS MEASUREMENT

CONTROL PORTS, SERVICES, PROTOCOLS

MANAGE SOFTWARE

CONTROL EXECUTION

TRAIN PEOPLE

ANALYTICS, CORRELATION

USE SECURE CONFIGS

MANAGE PRIVILEGES

SCAN FOR MALWARE

THREAT INTELLIGENCE

DEVELOP EXPLOIT

CAPABILITIES

INTENTIONS

RECON OF TARGETS

ESTABLISH “BEACHHEAD”

CREATE “TOOLBOXES”

WEAPONIZE VULNERABILITIES

CLEAN UP TRACES

COMMAND & CONTROL

ATTACK SUPPLY CHAIN

INTELLIGENCE GATHERING

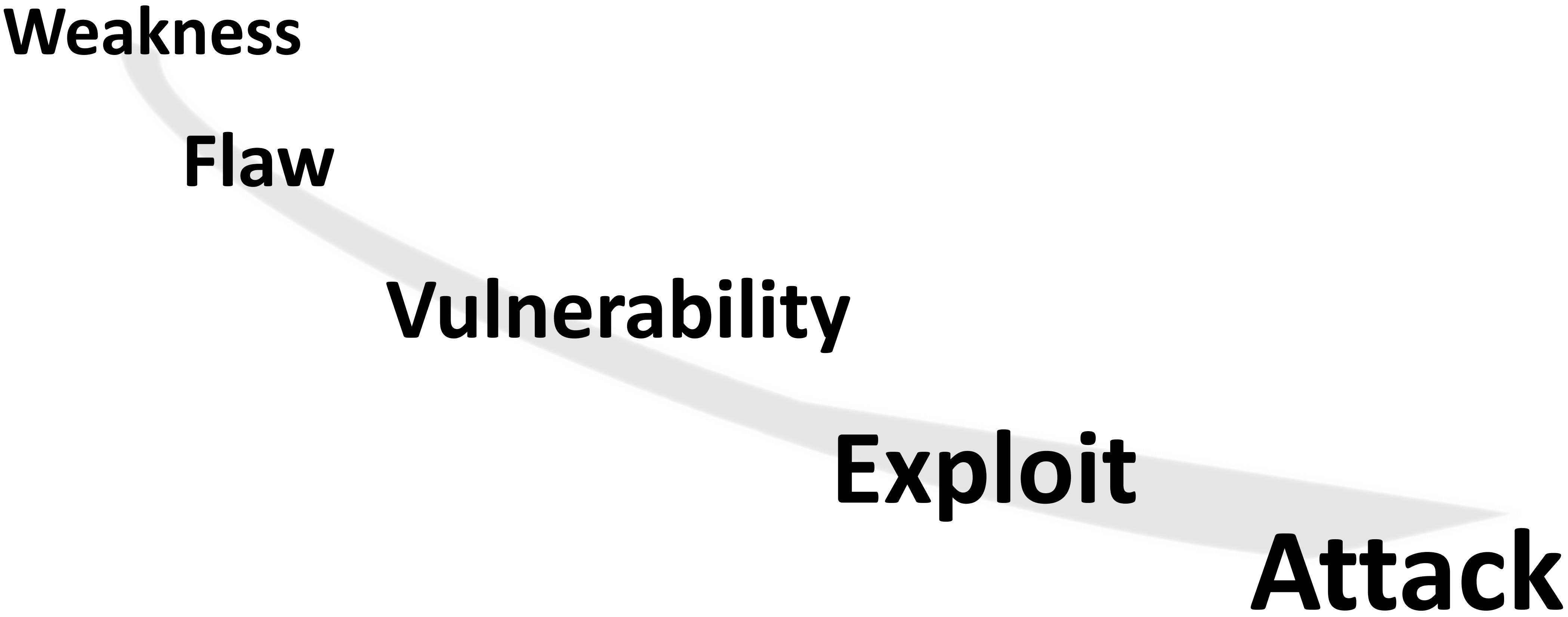
DEFENDER

ATTACKER

TACTICAL

STRATEGIC

How Much Should I Care?



Weakness

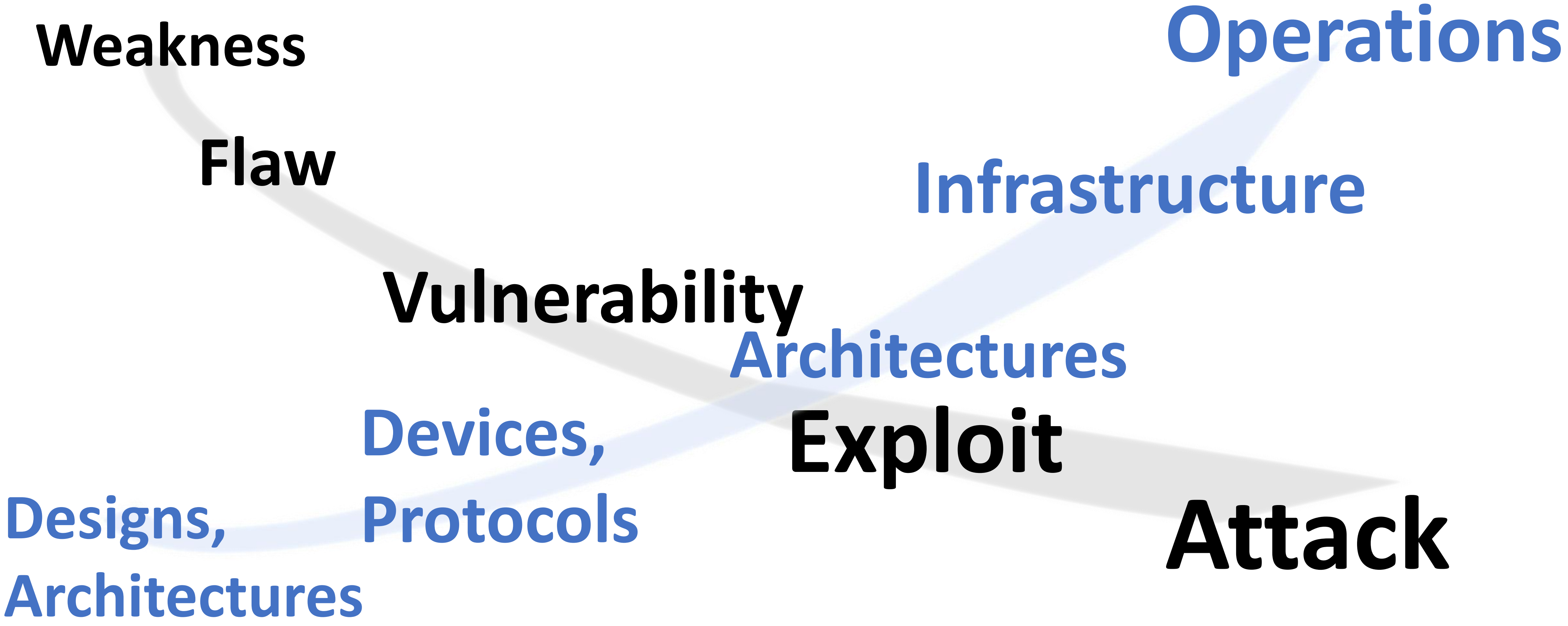
Flaw

Vulnerability

Exploit

Attack

How Much Should I Care?



Weakness

Flaw

Vulnerability

Exploit

Attack

Designs, Architectures

Devices, Protocols

Architectures

Infrastructure

Operations

WHAT YOU SHOULD KNOW	WHAT DOES IT MEAN?
Anyone in organized crime (or espionage) *who is not in this* (cyber) *ought to be sued for malpractice*	The Bad Guys are highly motivated
Almost all attacks are repeats of a type or class; Bad Guys do not perform ***magic***	Build a foundation before taking a “moonshot”; understand the types, classes, patterns of attackers
Just pointing out problems doesn’t get them fixed	Solutions are part of a complex system of feedback, incentives, and verification
It’s hard to have a unique problem or an original thought	Point to existing standards, ideas, frameworks
No security snapshot will work; trust is dynamic	Encourage machinery, not reports; measurement, not a state (of security); good IT and Ops management
Threat Sharing is over-rated	Focus on ***translation***, ***action***, efficiency, info management
Not every problem can be solved in the cyber domain	Diplomacy, economics, policy, social norms
Everyone’s role is changing (industry, government, academia, non-profits, standards)	Less control, more about behavior; less central and top-down, more cooperative
We need better components	Software quality, architectures, services

CIS

- Website: www.cisecurity.org
- Email: Controlsinfo@cisecurity.org
- Twitter: @CISecurity
- Facebook: Center for Internet Security
- LinkedIn: Center for Internet Security

Tony Sager, Center for Internet Security

www.sagercyber.org