Collective Cyber Defense:
Towards An Organizational Maturity Model

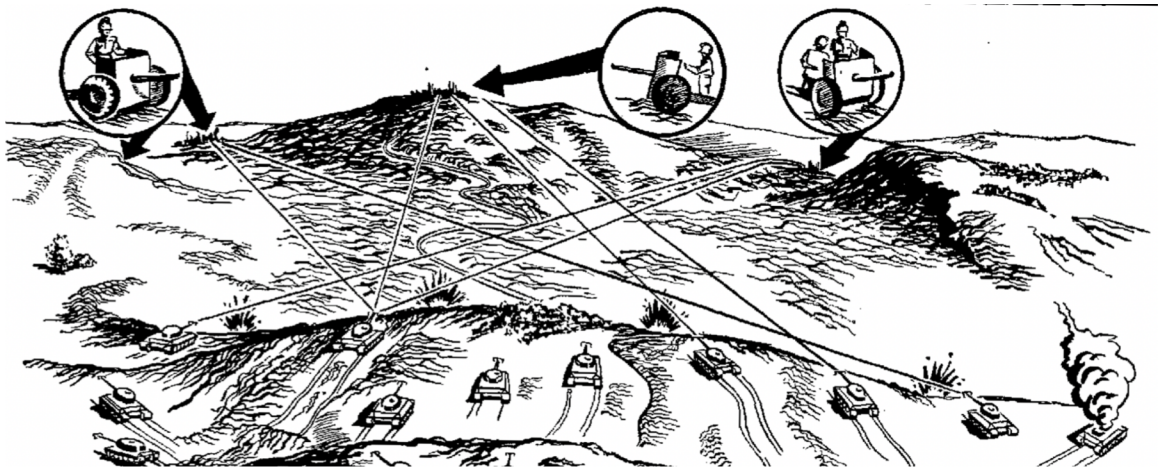
Terry Rice
Greg Conti

The views expressed in this talk are those of the speakers and do not reflect the official policy or position of our current or past employers.

Terry Rice
VP, IT Risk Management & CISO
@terry_rice

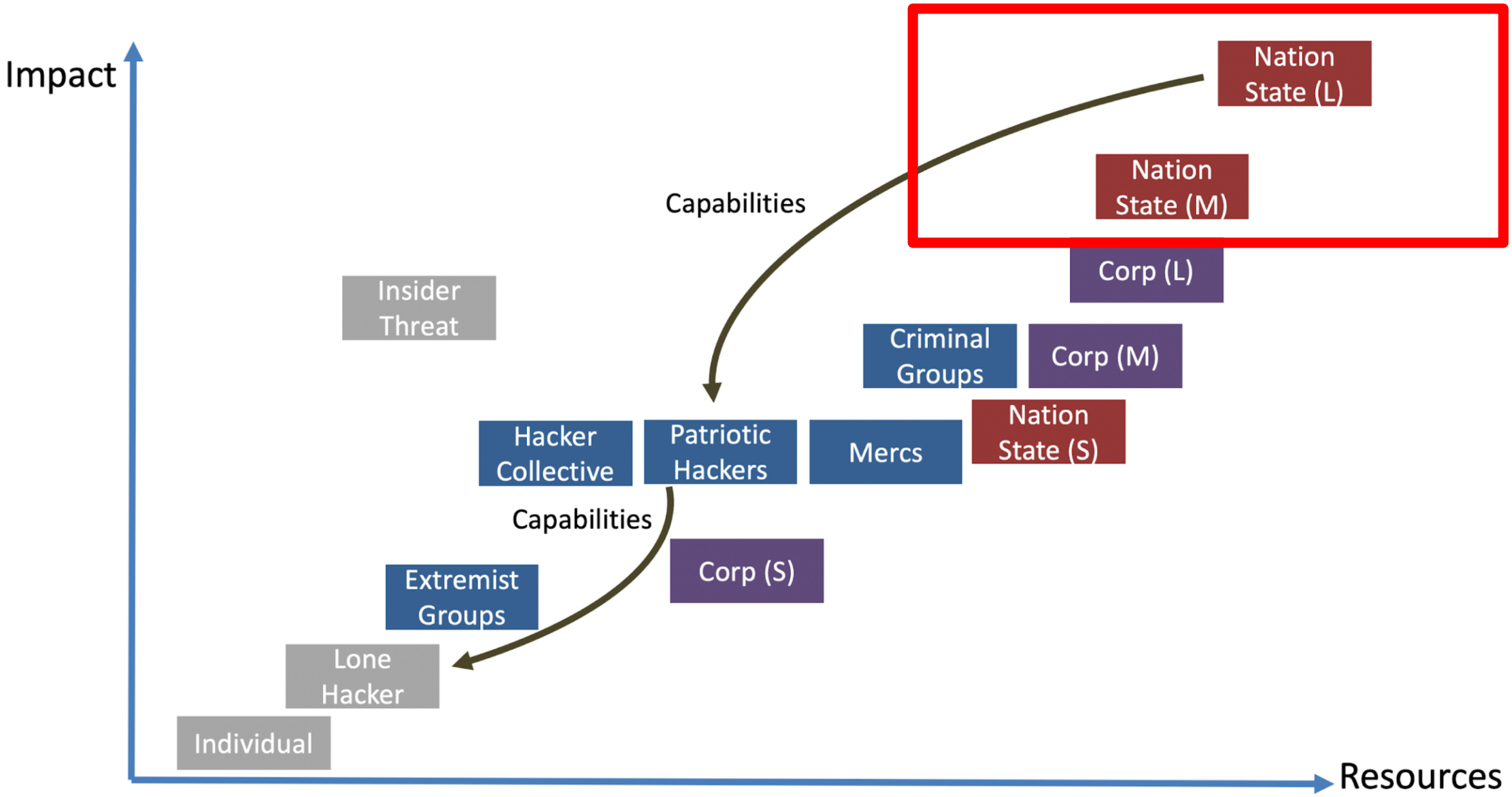
Gregory Conti
Security Strategist
@cyberbgone

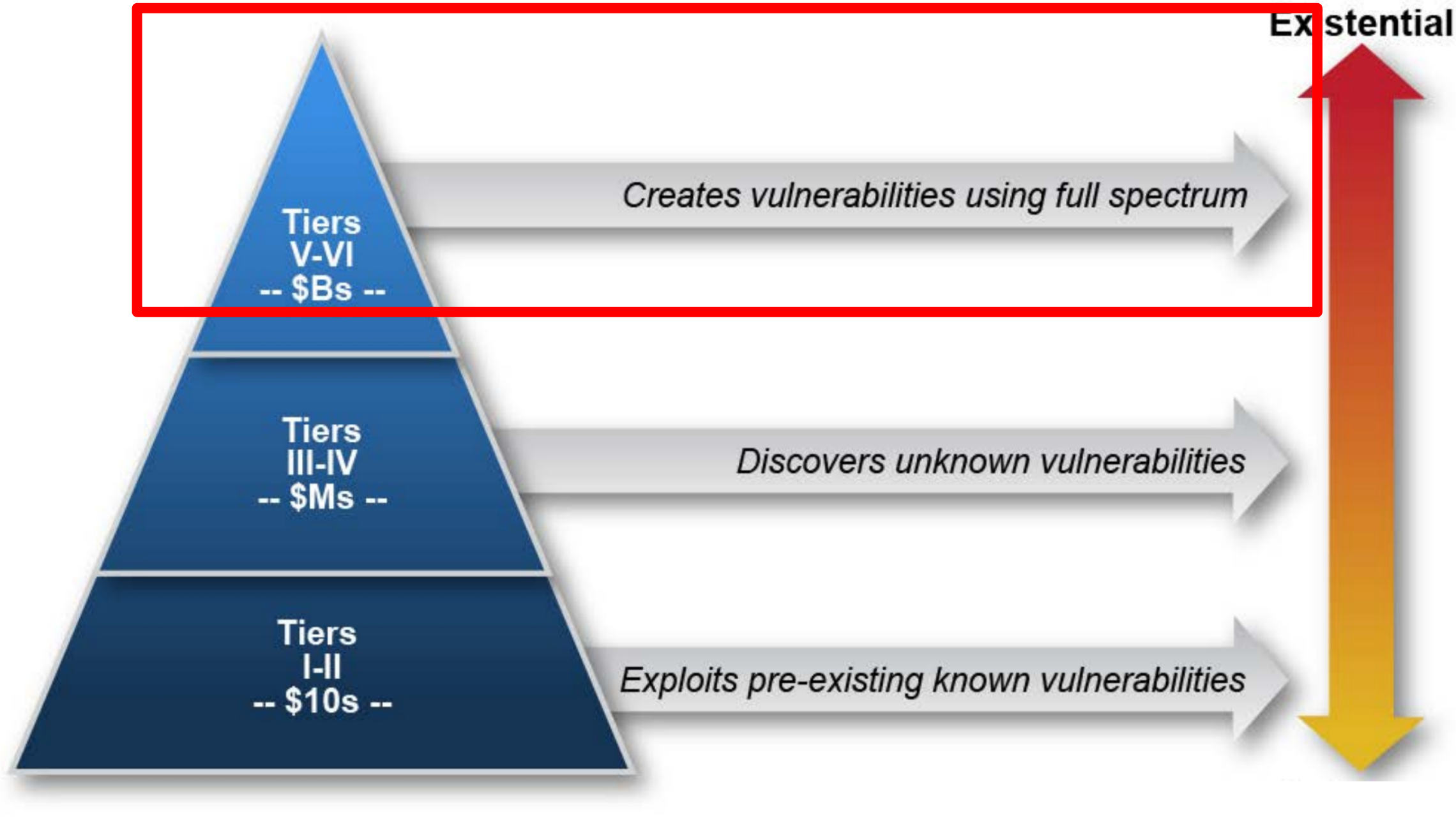
Why Collective Defense?



- Collective defense is necessary, no company can stand-alone against state-level threats
- Everyone faces state-level threats, either by chance or by deliberate targeting
- Both the private sector and the public sector need to participate or collective defense is impossible

- Honestly assess where you are in your organization’s development
- Outline a plan of where to go next
- Set an objective goal of an ideal
- Help make the case to the board for improved cybersecurity


Impact
Nation State (L)
Nation State (M)
Capabilities
Corp (L)
Insider Threat
Criminal Groups
Corp (M)
Hacker Collective
Patriotic Hackers
Mercs
Nation State (S)
Capabilities
Corp (S)
Extremist Groups
Lone Hacker
Individual
Resources



https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

Gap Analysis

	Individual	Lone Hacker	Hacker Collective	Organized Crime	Nation-State
Physical Security					
Wireless Security					
Network Security					
OS					
Application					
Web					
OPSEC					
BYOD					
Users					

Gap Analysis

	Individual	Lone Hacker	Hacker Collective	Organized Crime	Nation-State
Physical Security					
Wireless Security					
Network Security					
OS					
Application					
Web					
OPSEC					
BYOD					
Users					

Gap Analysis

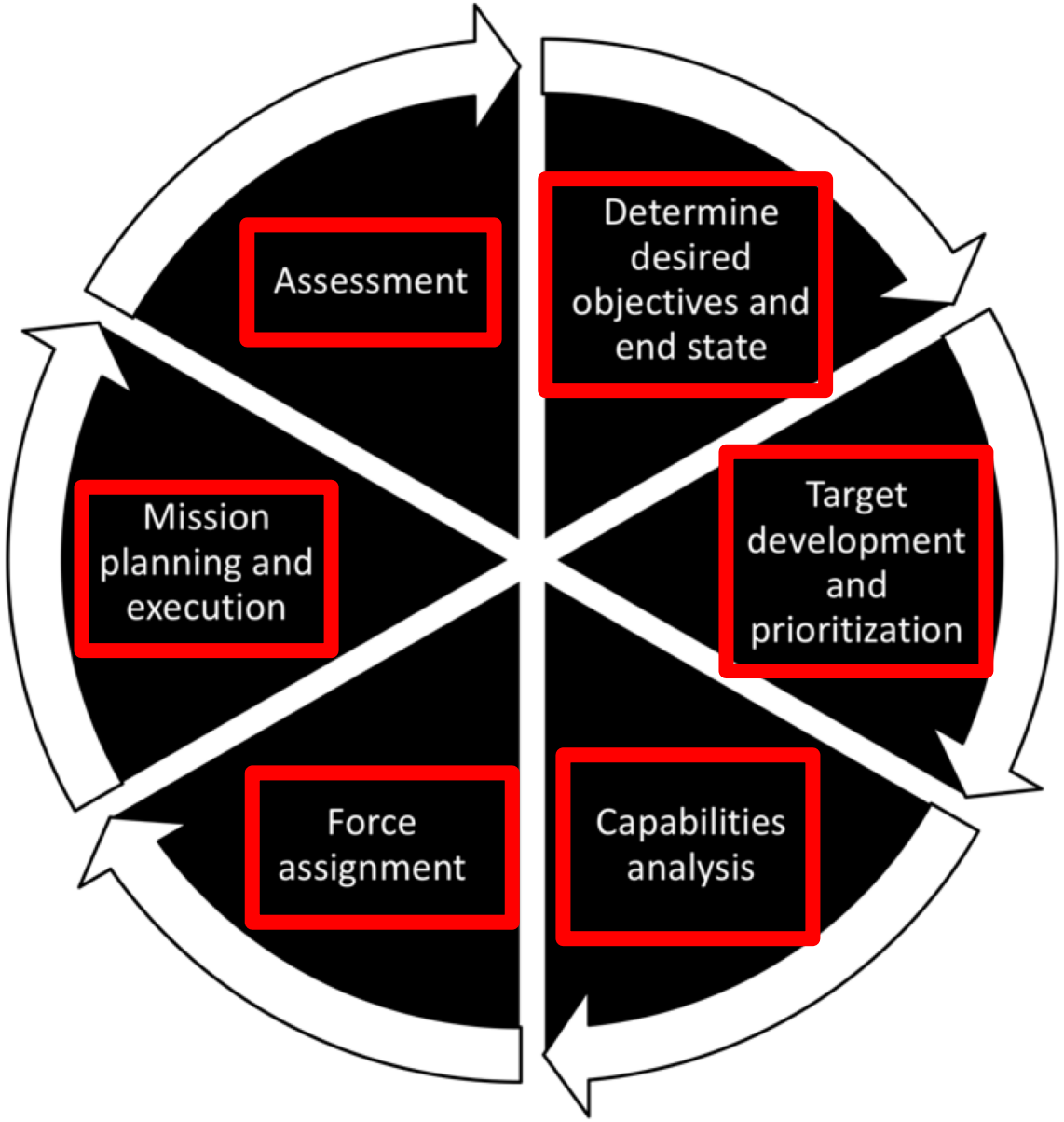
	Individual	Lone Hacker	Hacker Collective	Organized Crime	Nation-State
Physical Security					
Wireless Security					
Network Security					
OS					
Application					
Web					
OPSEC					
BYOD					
Users					

Gap Analysis

	Individual	Lone Hacker	Hacker Collective	Organized Crime	Nation-State
Physical Security					
Wireless Security					
Network Security					
OS					
Application					
Web					
OPSEC					
BYOD					
Users					

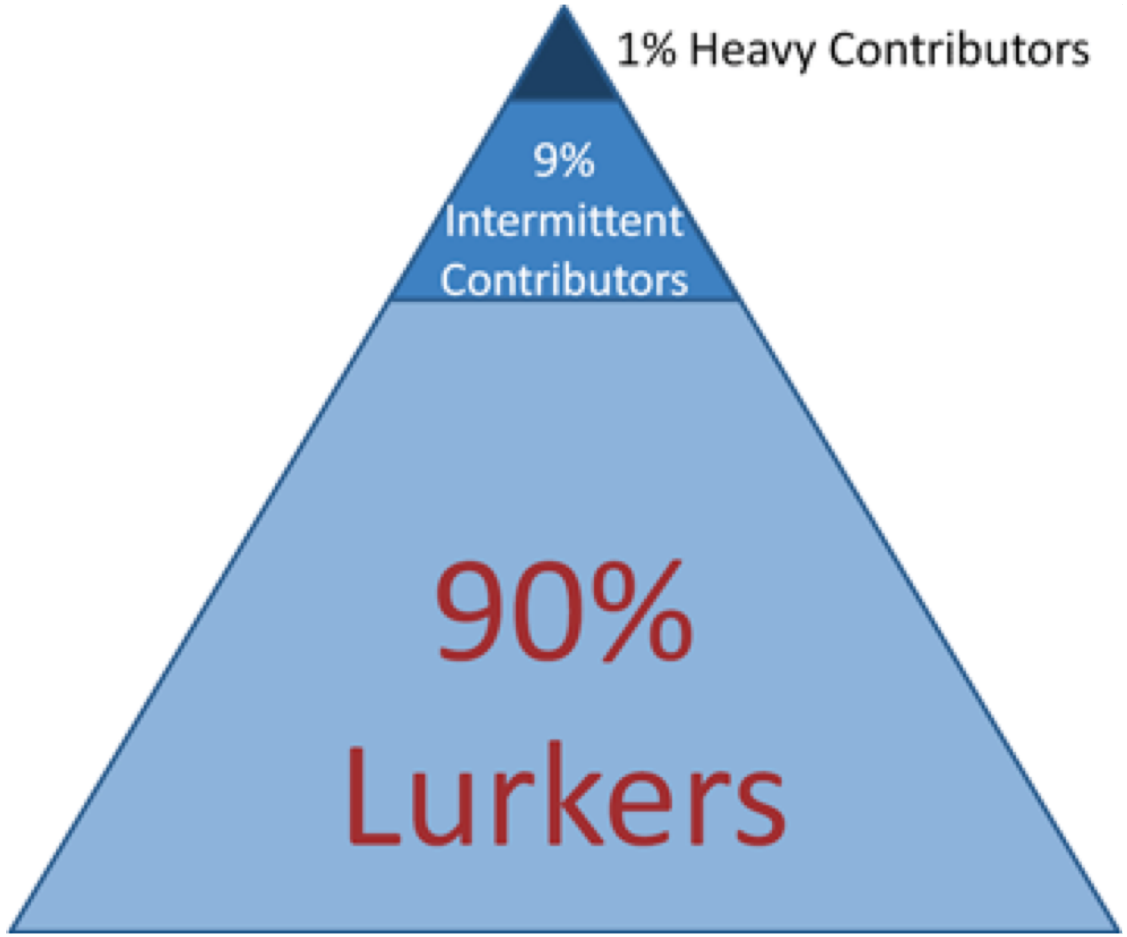
Targeting Process

The “Kill Chain” happens here



http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf

Participation Inequality (90-9-1)



"In most online communities, 90% of users are lurkers who never contribute, 9% of users contribute a little, and 1% of users account for almost all the action."

- Jackob Nielsen

https://www.nngroup.com/articles/participation-inequ

What Attributes Might We Measure?

Sector-level Situational Awareness

Interoperability

Teamwork

ISAC Membership

Information Sharing

Sensor Coverage

Sector-level Analytics

Aligned Incentives

Trust

Speed

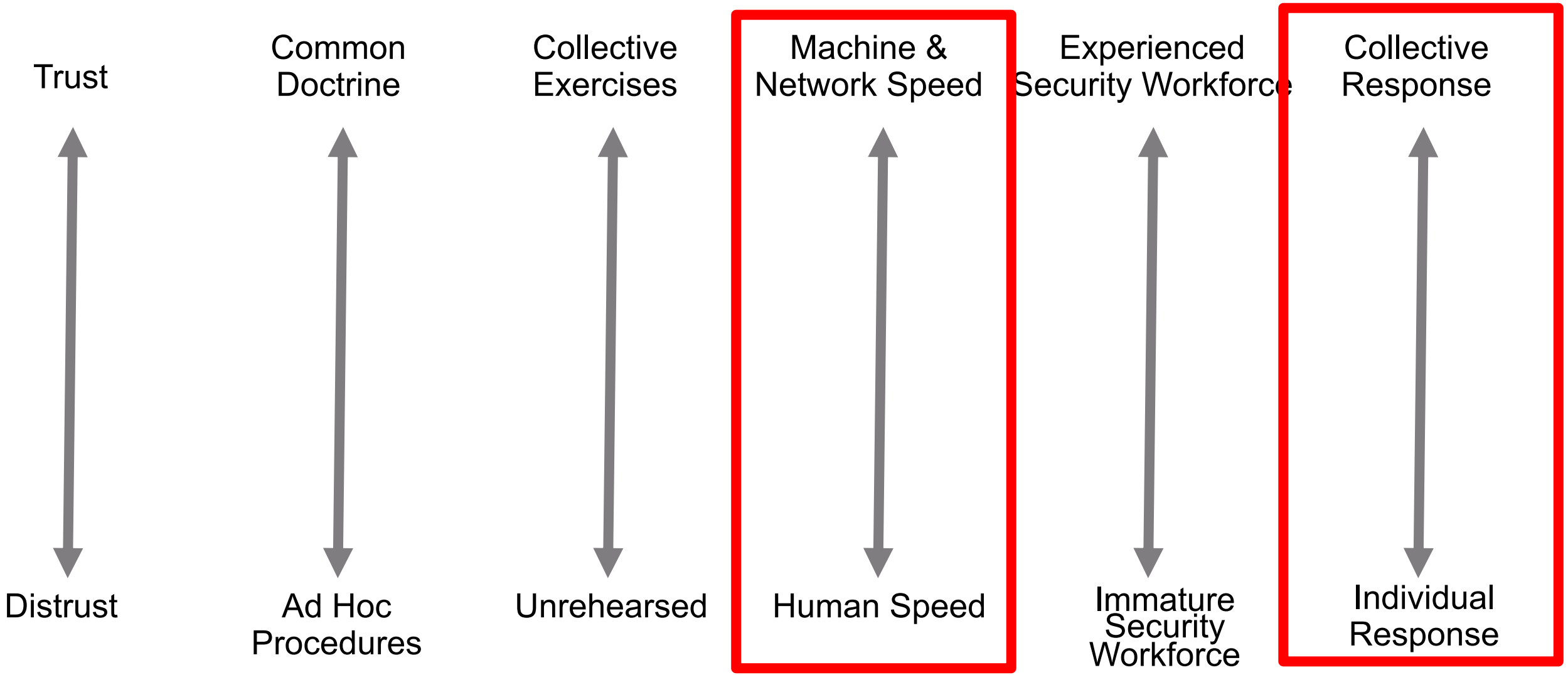
Established Playbook

Common SOPs & Doctrine

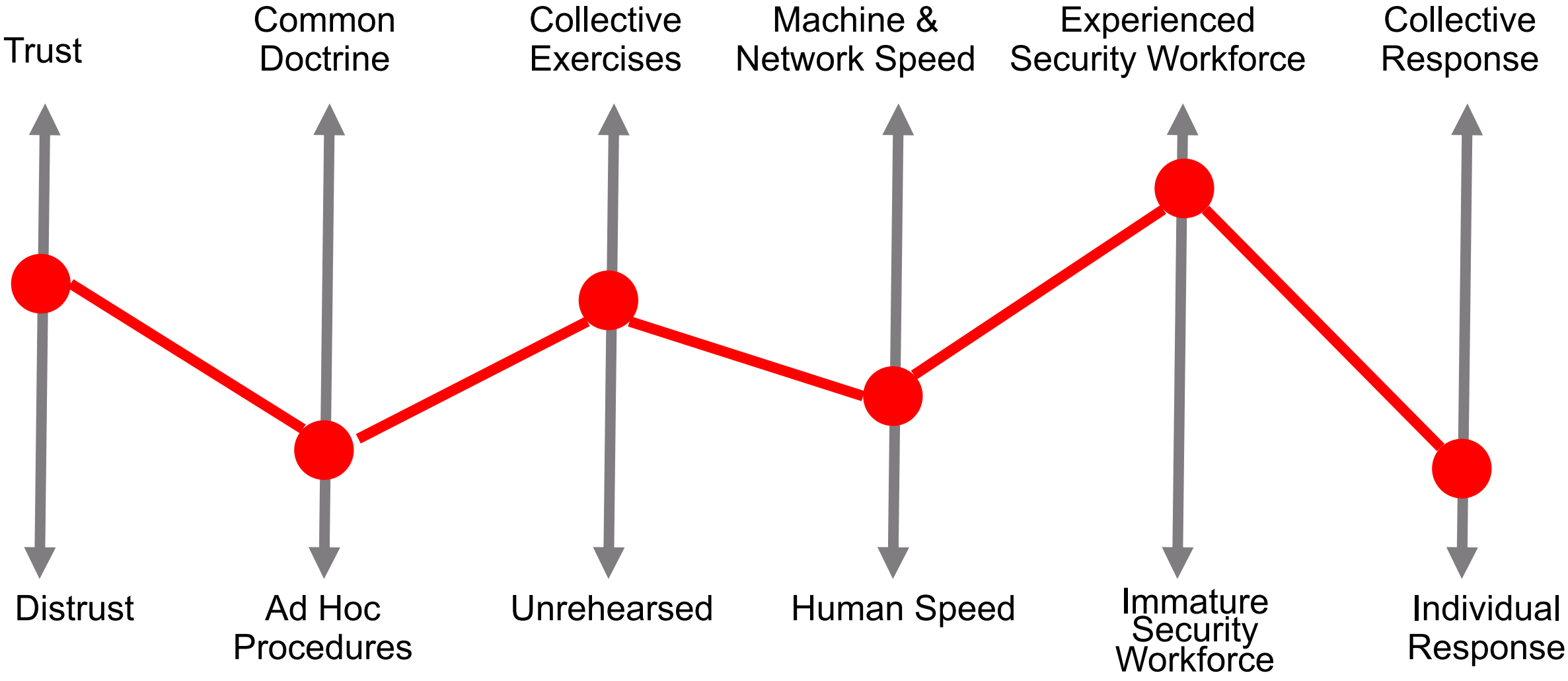
Participation in Community Exercises

Individual and Collective SOCs

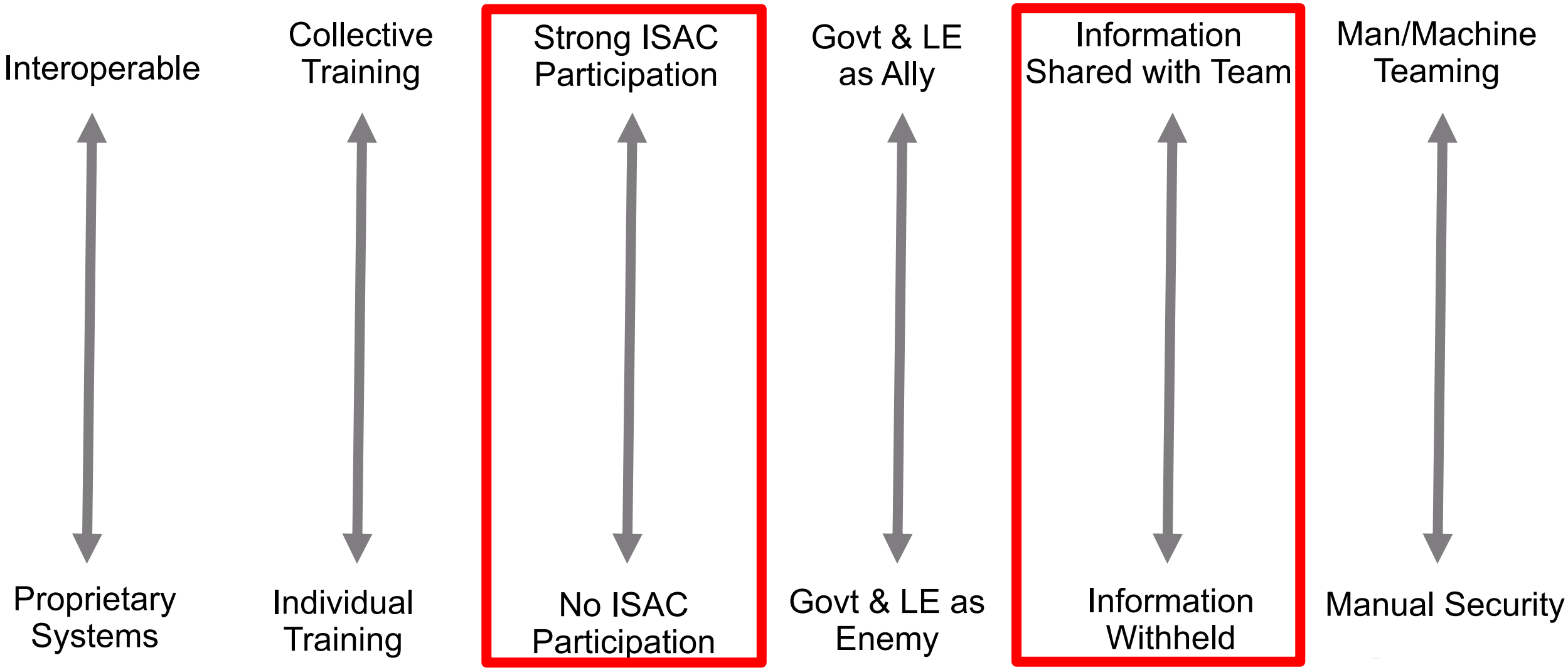
On What Scales?



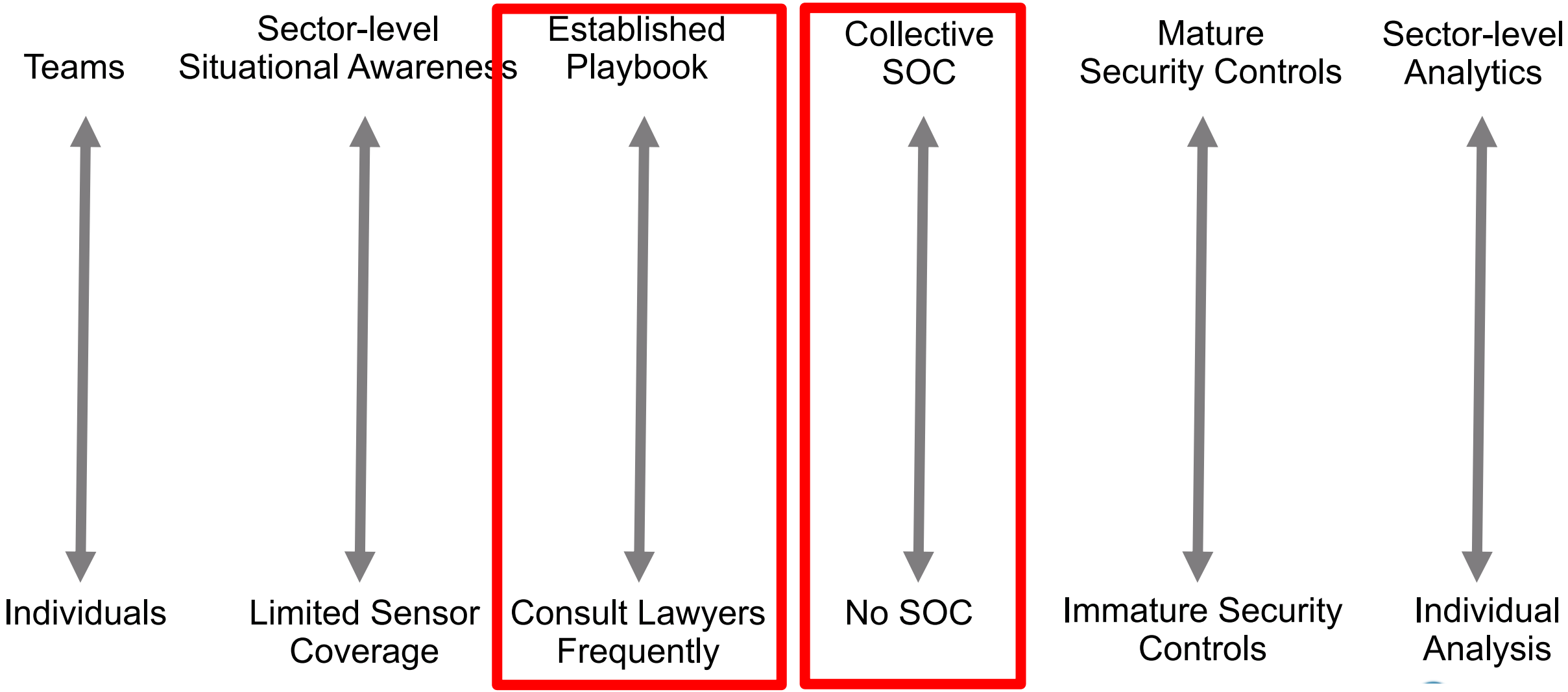
On What Scales?



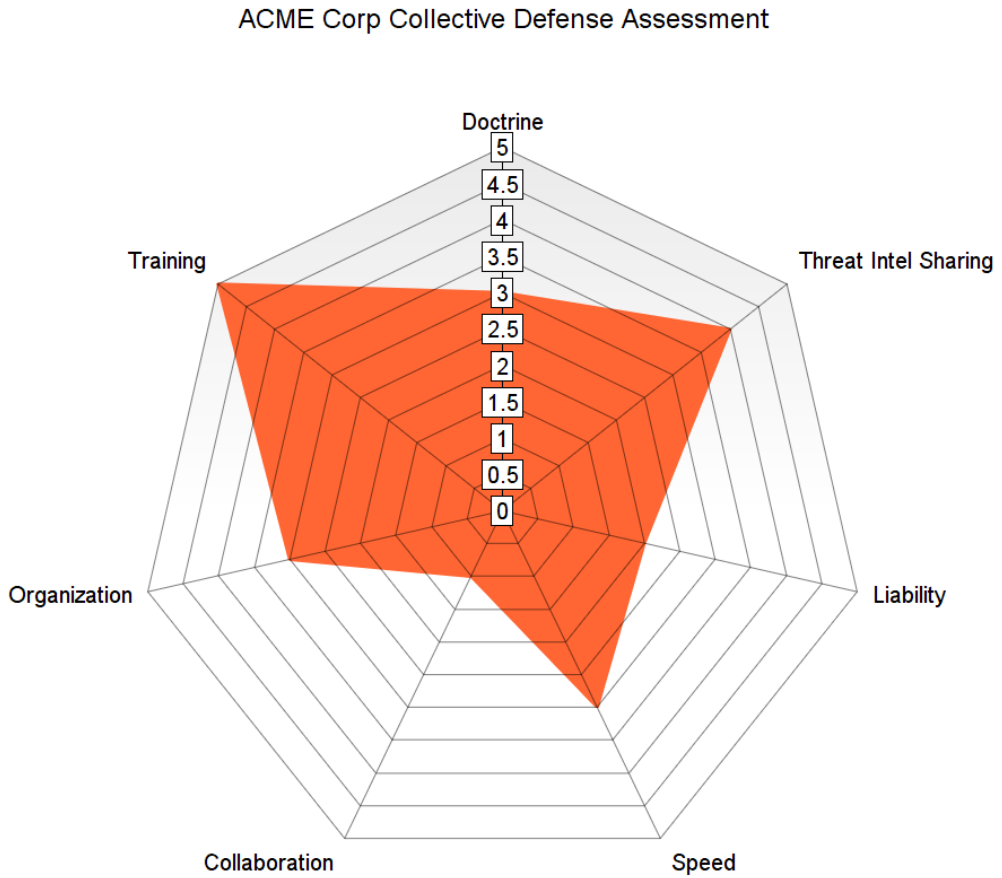
On What Scales?



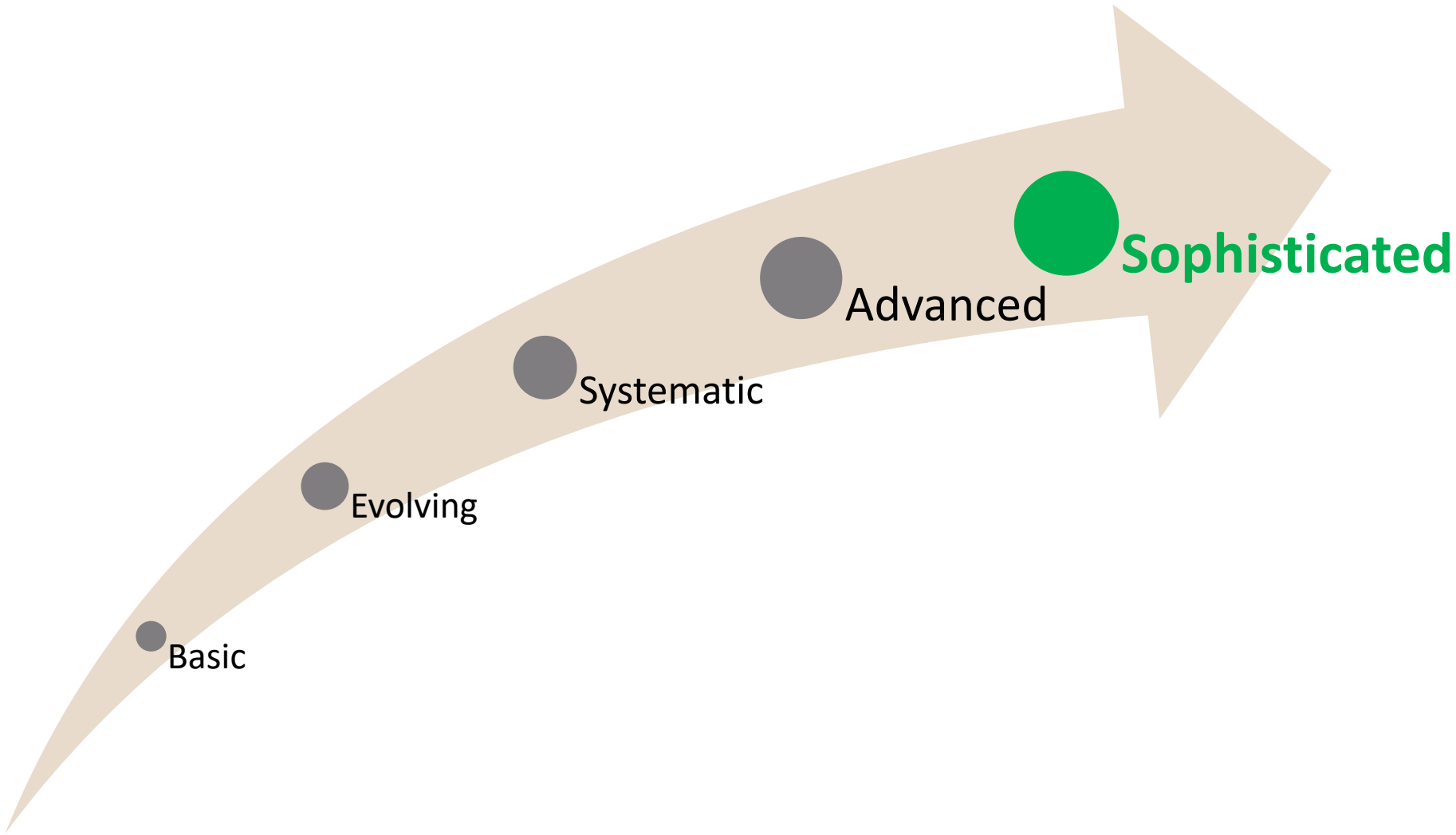
On What Scales?



A Way to Visualize the Assessment?



Five Tiers



1

- Organizations act as individual islands
- Law enforcement deals with major incidents on limited, case-by-case basis with modest effect
- Limited ability to collect forensic information frustrates response
- North-South sensor coverage
- Suspicion of others in business sector
- Working toward CIS Top 20 controls
- Misaligned incentives
- Primarily signature-based defensive systems
- Government works to defend itself
- Cybersecurity seen as cost center and impediment to business function

2

- Some internal system interoperability
- Need for collective defense understood
- Limited, but more effective government offensive response
- General ambivalence toward others in business sector
- CIS Top 20 controls in place
- Some external threat intelligence
- Outsourced SOC
- Slow, relationship-based information sharing
- Cybersecurity seen as enabler of business function

3

- North-South & East-West sensor coverage
- Member of ISAC
- Occasional trust of others in business sector
- Robust internal security
- Internal SOC
- Organizational information sharing and situational awareness
- Sound ability to collect forensic information
- Government response procedures documented
- Signature and some behavioral-based defensive systems
- Professionalized cybersecurity workforce
- Routine internal security exercises, employ threat emulation
- Board actively supports cybersecurity initiatives
- Internal threat intelligence team

4

- Aligned incentives
- Collaboration with others in business sector
- Sector-level situational awareness
- Participation in sector-level security exercises
- Sensor coverage extended to ICS systems, supply chain, and organizational ecosystem
- Sharing of threat information across small, medium, and large organizations
- Inter-organization standard operating procedures
- Councils of CISOs and CEOs address collective cybersecurity
- Sector-level SOC
- Behavioral-based defensive systems widely employed
- Joint public/private training

5

- Regular participation in joint public/private exercises
- Broad, well developed trust between organizations
- Robust, evolving common doctrine
- Government provides rapid effective response
- Automated, adaptive defenses
- Automated, adaptive requests for government response
- National-level situational awareness
- Comprehensive system coverage
- Effective, international government response
- AI/ML defensive systems mature and widely employed

	Doctrine	Organization	Training	Exercises
1	Ad hoc common operating procedures	No or limited security teams	No interorganizational training	No internal exercises
2	Basic internal operating procedures	Outsourced SOC Identified IR team	Ad hoc interorganizational training	Occasional internal exercises
3	Solid internal operating procedures, initial external operating procedures	Internal SOC	Occasional, small scale interorganizational training	Regular, challenging internal exercises
4	Prototype external doctrine	Dedicated threat intel team	Regular, small scale interorganizational training	Prototype interorganizational exercises (e.g. Jack Voltaic)
5	Time-tested, flexible, effective, agreed upon, and followed common doctrine	LNOs at state, federal, and/or sector Ops Centers	Flagship, collaborative, sector-level and national/private training	Regular, challenging interorganizational exercises

Sub-Sector	Level 1	Level 2	Level 3	Level 4	Level 5
Insurance					
Pharma					
Medical Devices					
Hospital					
Medical Services					

Notional

- Are you interested in concept of collective defense maturity?
- What are the three biggest hurdles?
- What are the three most important things to measure?
- How do you measure your own maturity?
- Would you participate in a formal (anonymous) survey?

Discussion

Terry Rice
VP, IT Risk Management & CISO
@terry_rice

Gregory Conti
Security Strategist
@cyberbgone