



Operational Templates for State-Level Attack and Collective Defense of Countries

Greg Conti
Bob Fanelli



Greg Conti

greg.conti@ironnetcybersecurity.com
@cyberbgone



Bob Fanelli

robert.fanelli@ironnetcybersecurity.com



How do we defend organizations,
economic sectors, and entire
nations in cyberspace?

It feels like our adversaries have strategies, and we have tactics. That's not very good. I don't like being in that situation. I don't like having no strategy.

Jeff Moss

BH USA 2018

Keynote Introduction

MATURE 17+

TM

M

**Blood and Gore
Intense Violence
Strong Language
Use of the word Cyber
Nudity
Strong Sexual Content
Use of Drugs and Alcohol**

ESRB CONTENT RATING

www.esrb.org



Strategic: Nation-states deciding upon national security objectives and using elements of national power.

Operational: Theater commander tying together tactical engagements to support strategic objective.

Tactical: Individuals and small units engaging in direct hostilities to defeat enemy forces or seize terrain.



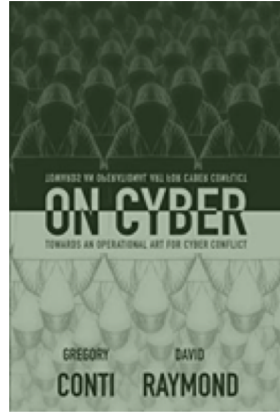
2014: Library of Sparta



2015: Applying Military Doctrine to Cybersecurity



2015: Deception for the Cyber Defender



2017: On Cyber: Towards an Operational Art for Cyber Conflict



2016-Present: IronDefense IronDome & Iron Shield



2015: Pen Testing a City



2018: What Would You Do With a Nation-State Cyber Army?



2018: Taking Down the Oil and Natural Gas Sector: Into the Mind of the Nation State Threat Actor



2015-Present: Training – Military Strategy and Tactics for Cyber Security, Information Operations



2019: Collective Cyber Defense in the Energy Sector



2019: Dim Mak - A Study of the Pressure Points that Could Take Down Cyberspace



2019: Collective Cyber Defense: Towards an Organizational Maturity Model

The Rout



<http://www.youtube.com/watch?v=92gP2J0CUjc&t=1m12s>

“a unit that has taken heavy casualties and/or believes itself about to be surrounded, annihilated or overrun by a superior force may suddenly disintegrate into a state of self-perpetuating mass panic”

Defeat in Detail (aka Divide and Conquer)



“...bringing a large portion of one's own force to bear on small enemy units individually, rather than engaging the bulk of the enemy force all at once.”

<http://www.youtube.com/watch?v=1jIP55liKSg&t=3m3s>



IRS.gov

Anthem



PORT of SAN DIEGO



Bristol Airport



MAERSK

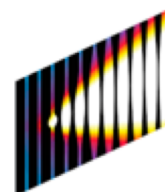
ECDIS



DEMOCRATS
CHANGE THAT MATTERS



United Airlines



SONY PICTURES



NMCI
NAVY MARINE CORPS INTRANET



DigiNotar
Internet Trust Services



Defense Travel System
A New Era of Government Travel

Google



GitHub

A Tale of Two Teams...



2004 Olympic Basketball Team - USA



2004 Olympic Basketball Team – Argentina

<http://www.youtube.com/watch?v=LtopNCH5-qY&t=2m39s>

http://greghornjudge.com/SUB_video_game_&_advertising/olympic_USA_basketball_team_2004.htm

<https://www.olympic.org/news/olympic-channel-presents-the-golden-generation-the-story-behind-argentina-s-iconic-victory-in-men-s-basketball-at-athens-2004>

Divide and Conquer Works Really Well When we are Already Divided



- We don't really even have a team
- We don't really have offense
- All of society depends on networked information systems
- Medium and small organizations at a severe disadvantage.
- **We will continue being defeated individually, unless we do something**

Defining Collective Defense

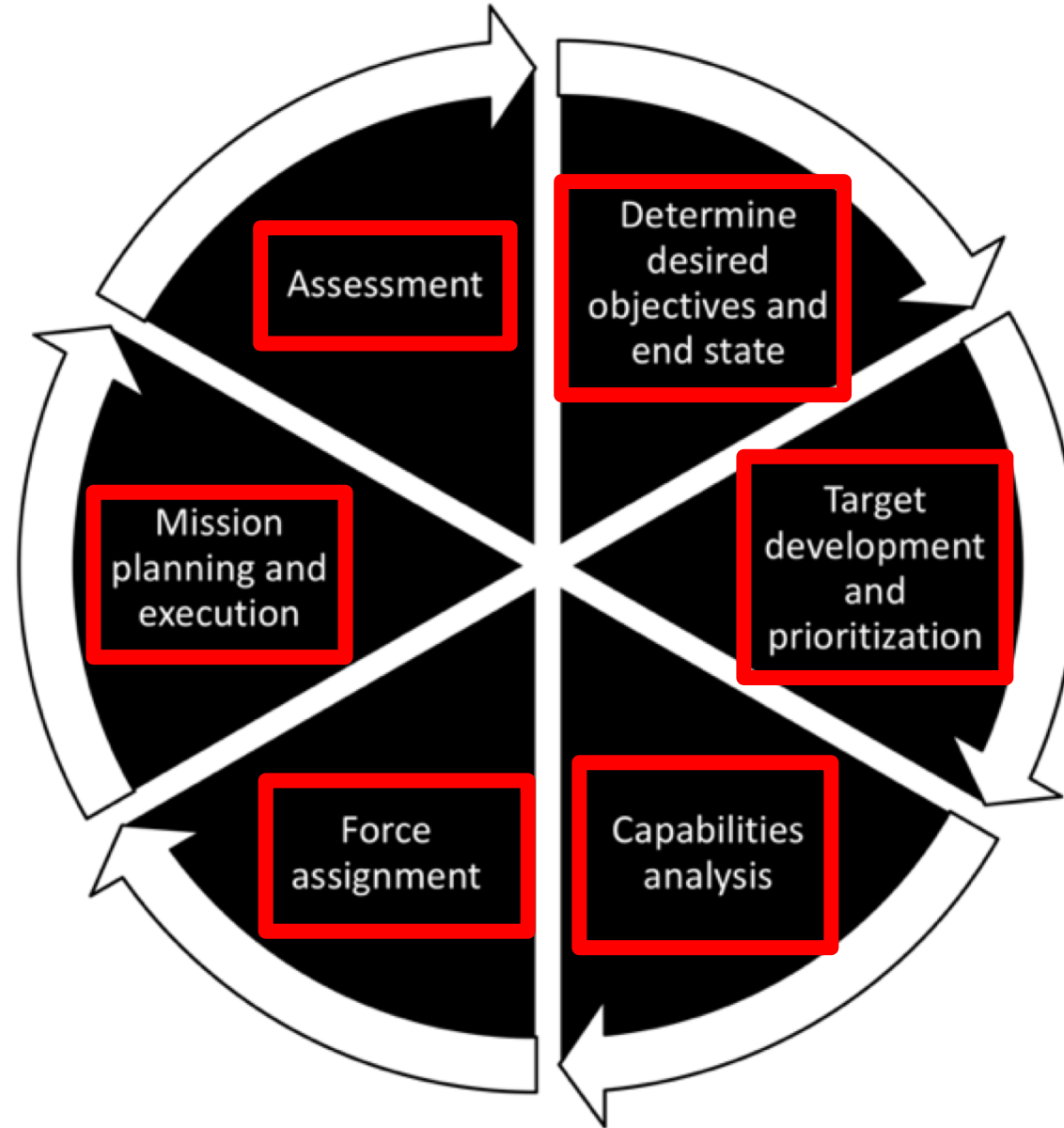


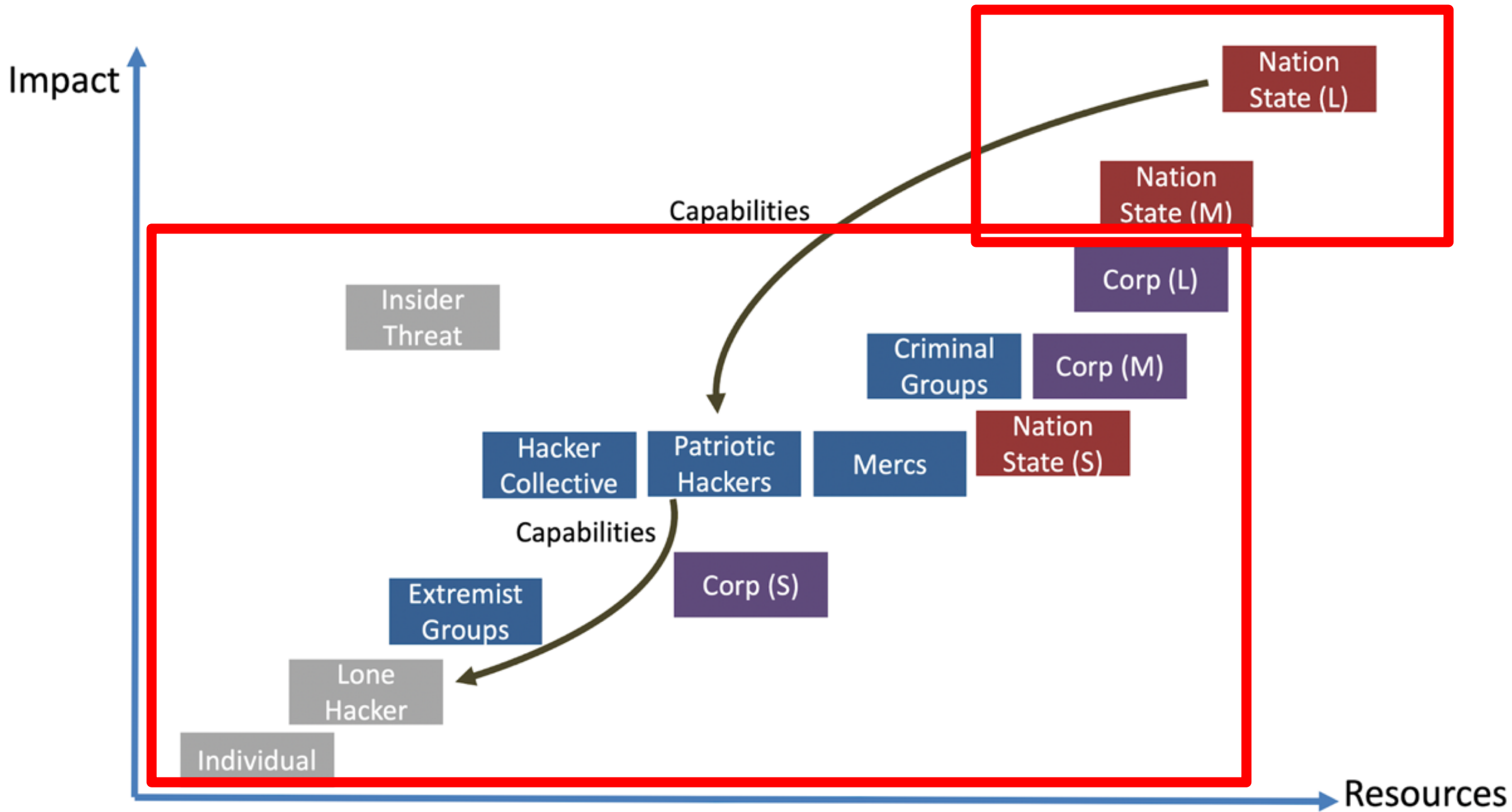
“Collective defence means that an attack against one Ally is considered as an attack against all Allies.” - NATO

- Collective defense is necessary, no company or sector 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

Collective Offense

The “Kill Chain”
happens here

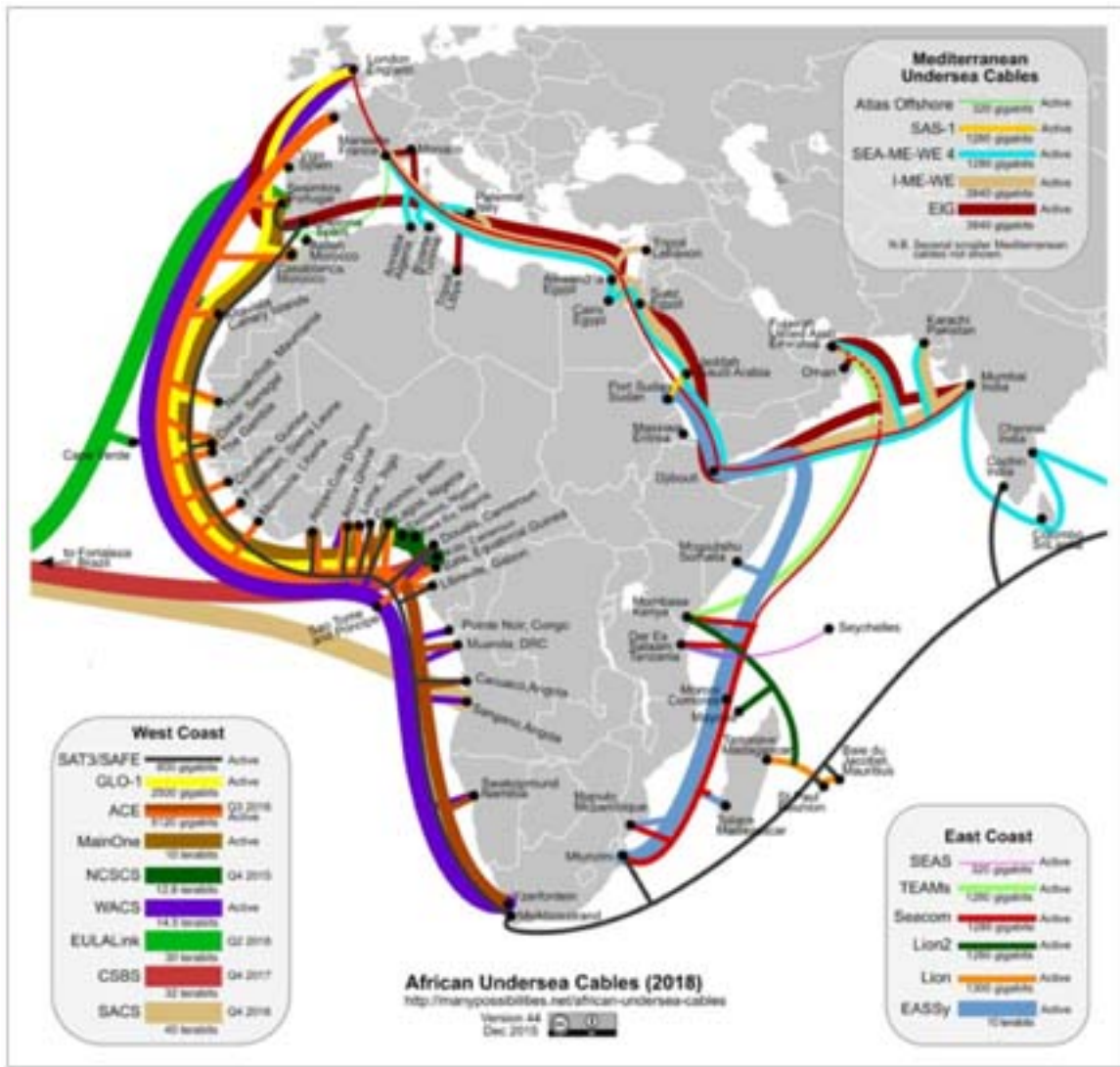




Instruments of National Power

D Diplomatic	I Informational	M Military	E Economic
<ul style="list-style-type: none">▪ Embassies/ Ambassadors▪ Recognition▪ Negotiations▪ Treaties▪ Policies▪ International forums	<ul style="list-style-type: none">▪ Military information▪ Public diplomacy▪ Public affairs▪ Communications resources▪ International forums▪ Spokespersons, timing, media and venues for announcements	<ul style="list-style-type: none">▪ Military operations▪ Engagement, Security Coop, Deterrence▪ Show of force▪ Military technology▪ Size, composition of force	<ul style="list-style-type: none">▪ Trade policies▪ Fiscal and monetary policies▪ Embargoes▪ Tariffs▪ Assistance

Undersea Cables



August 19, 2018 | Topic: Security | Region: Eurasia | Blog Brand: The Buzz | Tags: Military, Technology, Weapons, War, Russia

Russian Spy Submarines Are Tampering with Undersea Cables That Make the Internet Work. Should We Be Worried?

https://upload.wikimedia.org/wikipedia/commons/2/22/African_undersea_cables_v44.jpg

<https://nationalinterest.org/blog/buzz/russian-spy-submarines-are-tampering-undersea-cables-make-internet-work-should-we-be>

Electromagnetic Spectrum



DEFENSE

[G+](#) [Share](#) [in Share](#) [Tweet](#)

Navy declares EMS a full-fledged warfighting domain

BY LAUREN C. WILLIAMS • OCT 23, 2018

Space Force Proposal Could Create a Broader Military Department for Both Air and Space

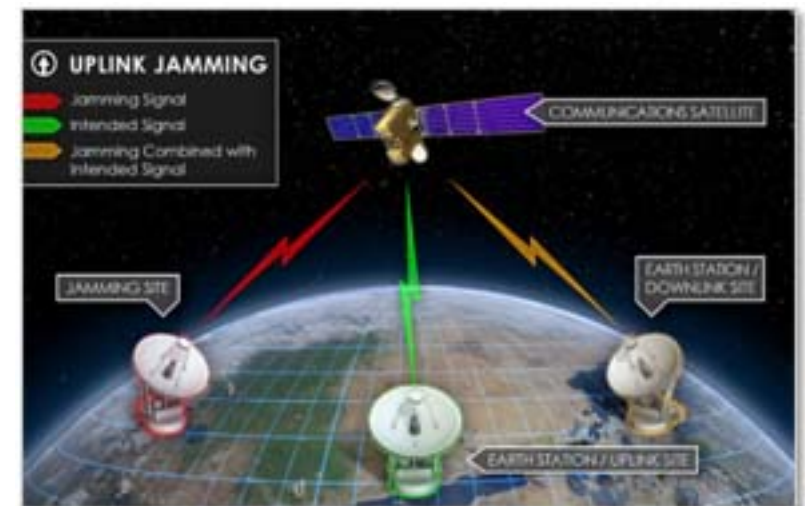
By Sartra Erwin, SpaceNews Staff Writer | December 9, 2018 07:28am ET

In cooperation with **SPACENEWS**



U.S. Vice President Mike Pence (left) and Defense Secretary James Mattis share a light moment during the Aug. 9 rollout of the Trump administrator's plan for establishing a Space Force.

Credit: Department of Defense



Global Intelligence Capability (HUMINT, SIGINT, OSINT, and more)

USB Drive Found on Jailed Mar-a-Lago Party-Crasher Contained Self-Executing Code

Dell Cameron and Tom McKay

4/08/19 9:50pm • Filed to: DO NOT INSERT




In this artist sketch, a Chinese woman, Yijing Zhang, left, listens to a hearing Monday, April 8, 2019, before federal Magistrate Judge William Matthewman in West Palm Beach, Fla. Secret Service agents arrested the 32-year-old woman March 30 after they say she gained admission by falsely telling a checkpoint she was a member and was going to swim.

Illustration: Daniel Portet / AP


The science of spying: how the CIA secretly recruits academics

In order to tempt nuclear scientists from countries such as Iran or North Korea to defect, US spy agencies routinely send agents to academic conferences - or even host their own fake ones. By [Daniel Golden](#)

Leverage

 **Rob^{beto} Graham** @ErrataRob · 17 Apr 2018
I'm compiling a list. What ethical dilemmas do we face in the field of infosec?

79 109 173

 **Tom Cross**
@_decius_ Following

Replying to @ErrataRob

Your government asks you to add a file hash to the anti-virus product you make and tell them if a match appears on one of your customers' computers. They won't tell you what the hash matches, but they insist it's a matter of life and death.

7:25 PM - 17 Apr 2018

Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice

PUBLISHED MON, MAR 4 2019 - 8:13 PM EST | UPDATED TUE, MAR 5 2019 - 12:33 AM EST



SHARE f t in e ...



Control of the Network High Ground

For two hours, a large chunk of European mobile traffic was rerouted through China

It was China Telecom, again. The same ISP accused last year of 'hijacking the vital internet backbone of western countries.'



By Catalin Cimpanu for Zero Day | June 7, 2019 -- 19:41 GMT (12:41 PDT) | Topic: Security

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

January 09, 2019 | by Muks Hirani, Sarah Jones, Ben Read

- Operating a national telecom comes with a position on the global network high ground
- Exclusive power to create and shape the network environment
- Most countries cooperate in good faith
- Uncooperative entities can manipulate the environment for advantage ...or break it altogether

Control of the Foundations of Cyberspace

Bloomberg Businessweek


The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Resident evil: Inside a UEFI rootkit used to spy on govts, made by you-know-who (hi, Russia)

Deep dive into motherboard firmware-lurking code

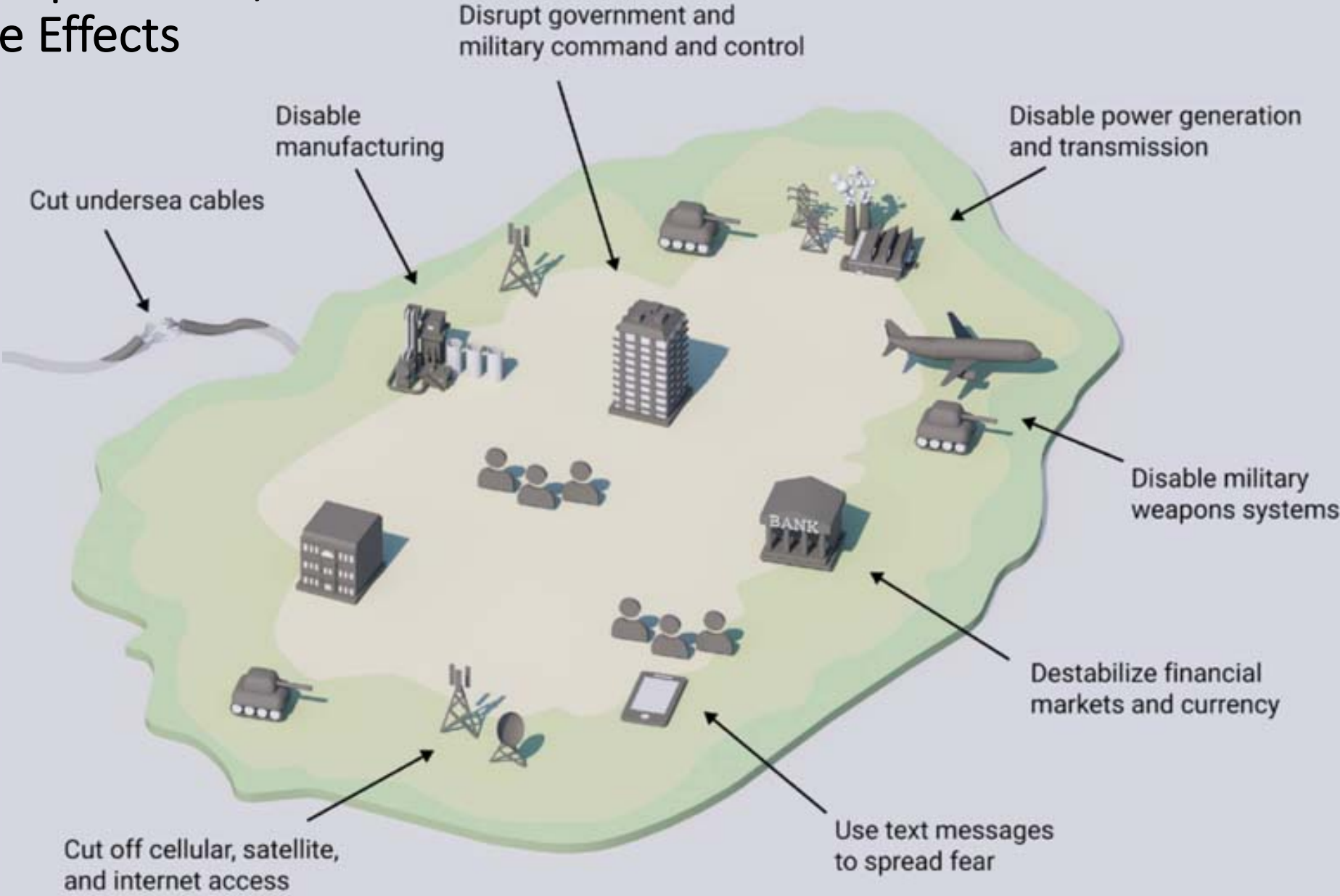
By John Leyden 28 Sep 2018 at 02:07

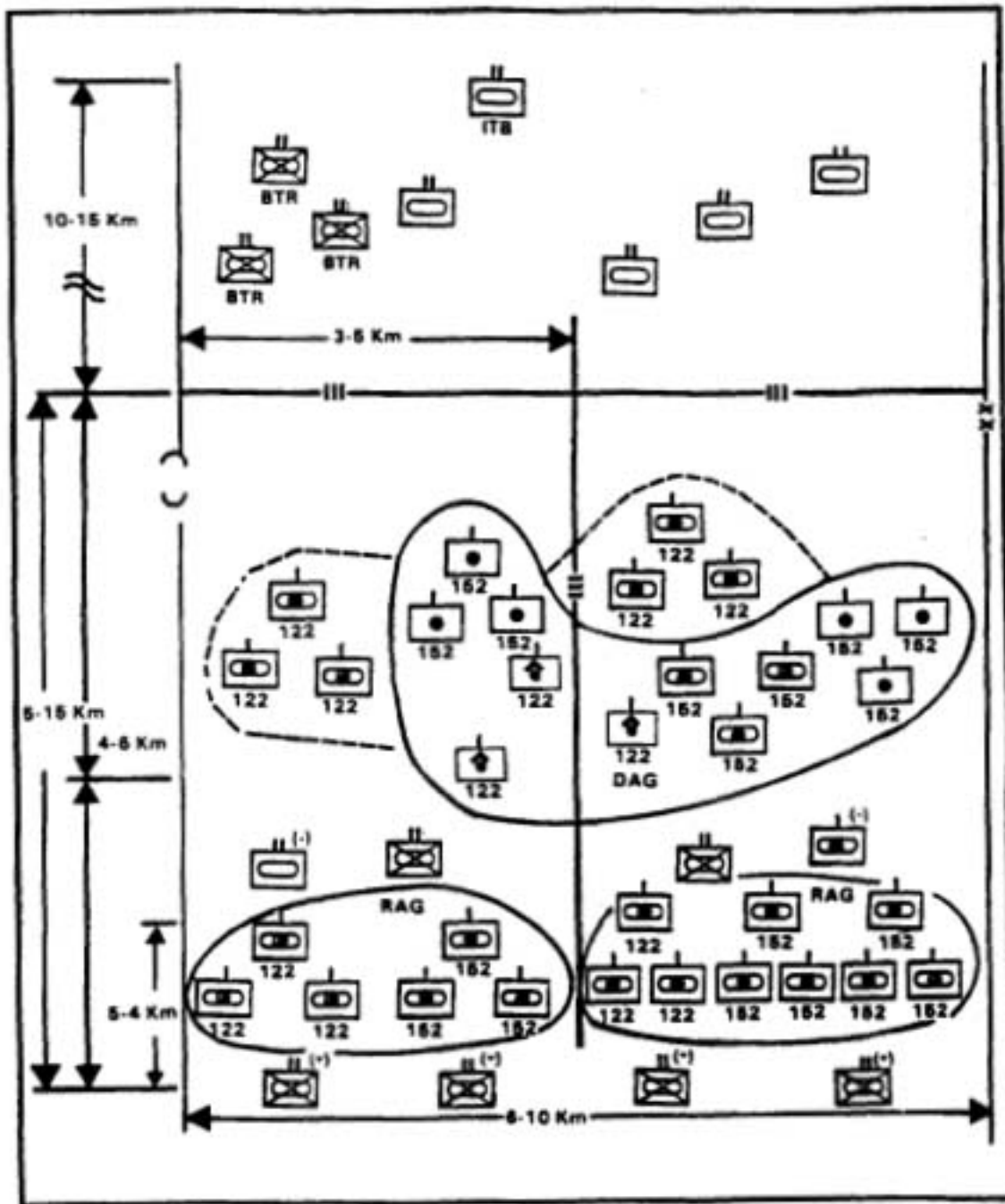
66  SHARE



- Global supply chains for hardware, software, firmware
- Risks of government influence
- Potential for kill switches, back doors, and other “features”
- Opportunity for a wide range of offensive effects

Combined Operations, Large-Scale Effects





What is a Doctrinal (Threat) Template?

- A model based on known or postulated adversary doctrine.
- Illustrates the disposition and activity of adversary forces and assets conducting a particular class of operation, under ideal conditions.
- Templates are adapted to the given operational environment.
- Depict the threat's preferred way to use its capabilities and perform the functions needed to achieve its objectives.

Offensive Templates

Critical Infrastructure Control

Cyberspace Denial

Influence Operations and
Perception Management

The Long Game

Defensive Templates

Basic

Evolving

Systematic

Advanced

Sophisticated

Hybrid Template

Defend Forward

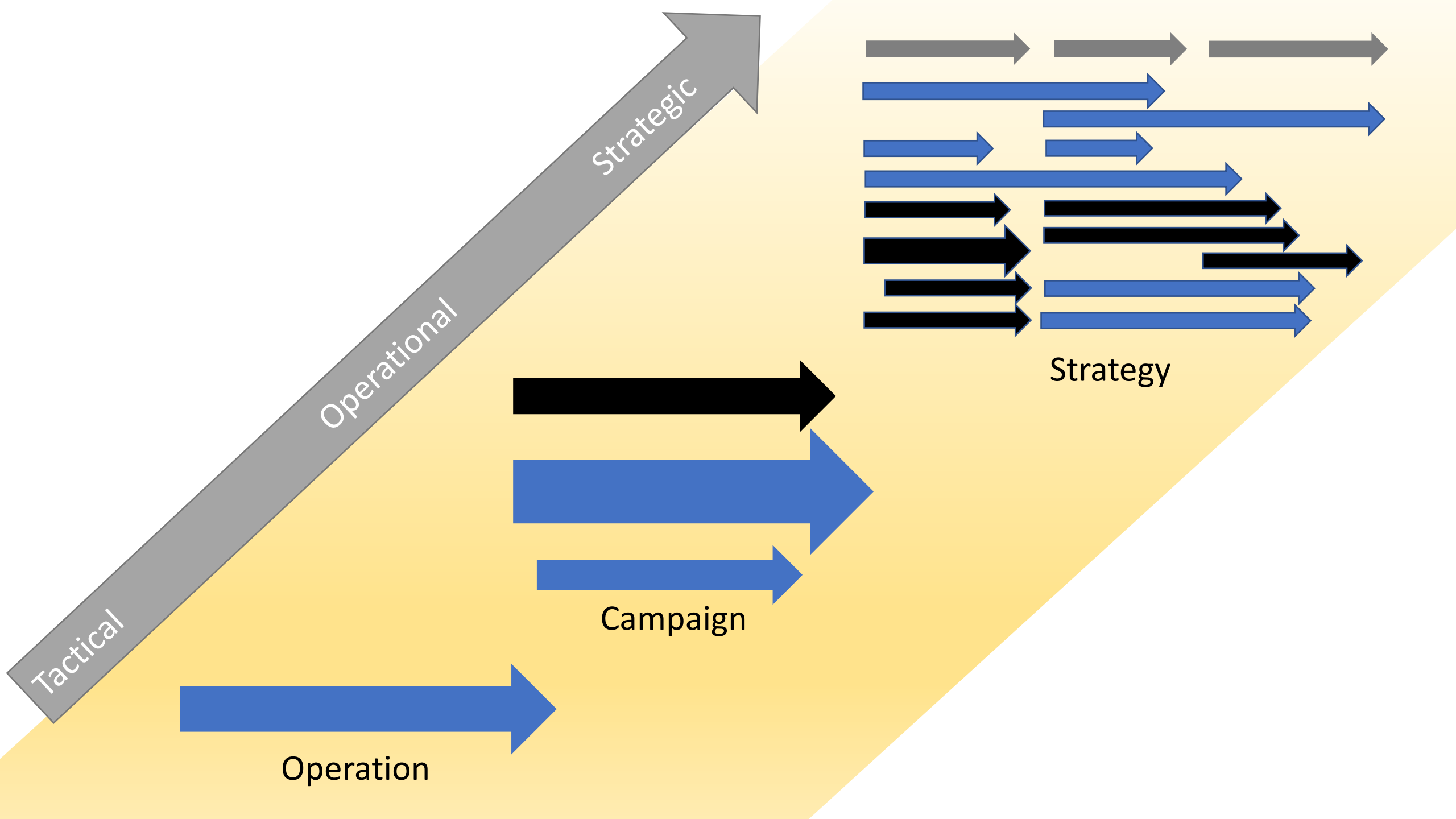
Offensive Templates

Organized by threat actor profiles and realistic other possibilities at current level of maturity

Defensive Templates



Tiered based on current and projected maturity



Tactical

Operational

Strategic

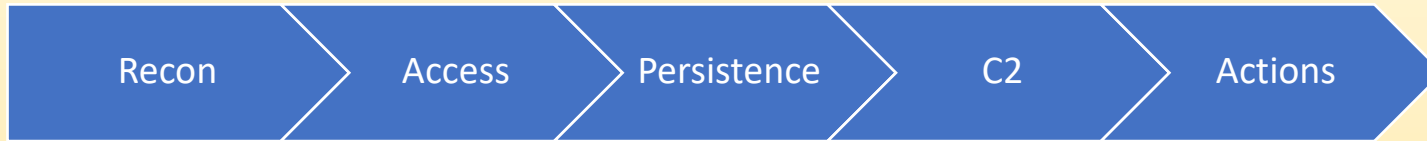
Operation

Campaign

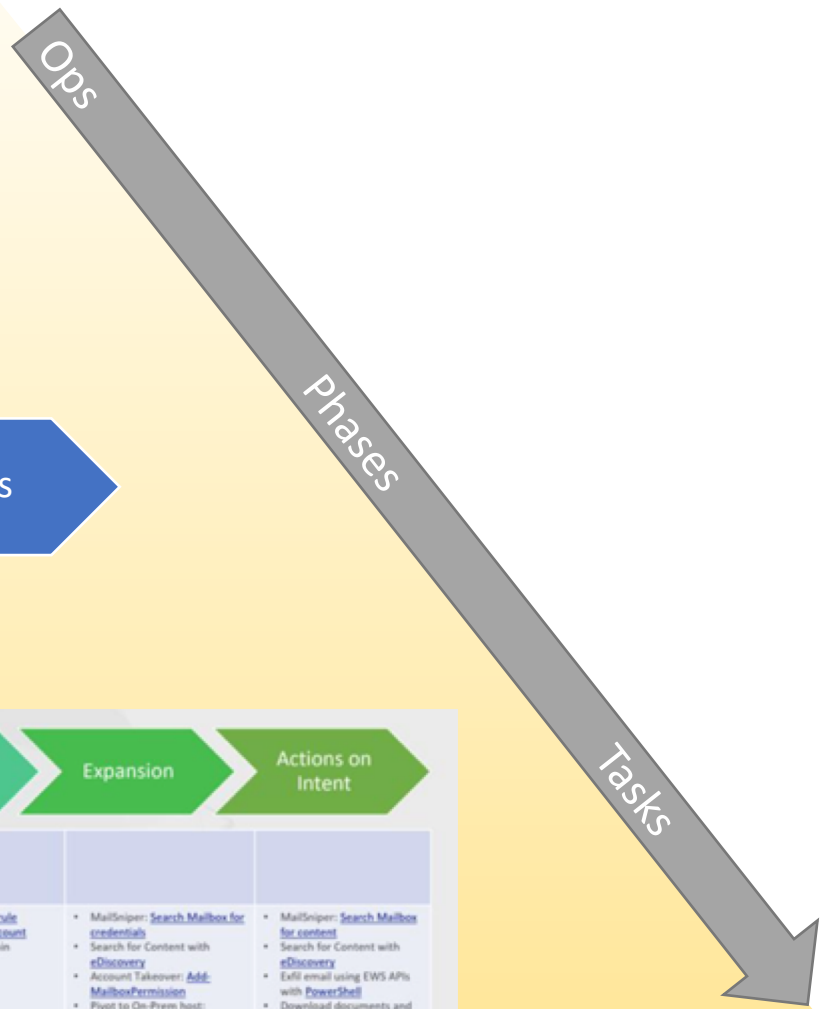
Strategy



Operation



Kill Chain

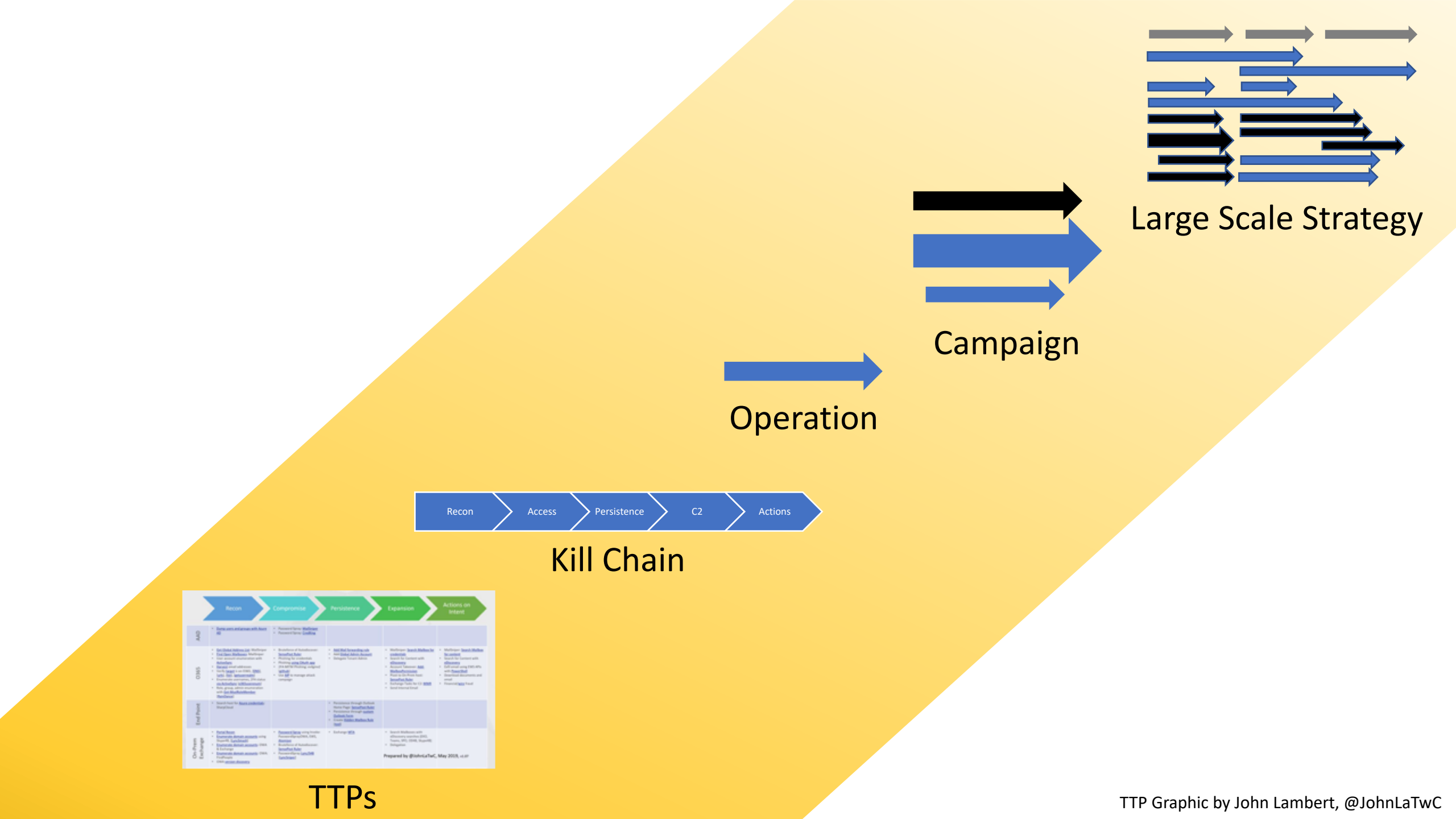


	Recon	Compromise	Persistence	Expansion	Actions on Intent
AAD	<ul style="list-style-type: none"> Dump users and groups with Azure AD 	<ul style="list-style-type: none"> Password Spray: MailSniper Password Spray: CredKing 			
O365	<ul style="list-style-type: none"> Get Global Address List: MailSniper Find Open Mailboxes: MailSniper User account enumeration with ActiveSync Harvest email addresses Verify target is on O365, [DNS], [url], [list], [getuserrealm] Enumerate usernames, 2FA status via ActiveSync [o365userenum] Role, group, admin enumeration with Get-MailRoleMember [RainDance] 	<ul style="list-style-type: none"> Bruteforce of Autodiscover: SensePost Ruler Phishing for credentials using DMuth app 2FA MITM Phishing: evligns2 Use AIP to manage attack campaign 	<ul style="list-style-type: none"> Add Mail forwarding rule Add Global Admin Account Delegate Tenant Admin 	<ul style="list-style-type: none"> MailSniper: Search Mailbox for credentials Search for Content with eDiscovery Account Takeover: Add-MailboxPermission Pivot to On-Prem host: SensePost Ruler Exchange Tasks for C2: MWR Send Internal Email 	<ul style="list-style-type: none"> MailSniper: Search Mailbox for content Search for Content with eDiscovery Exfil email using EWS APIs with PowerShell Download documents and email Financial/wire fraud
End Point	<ul style="list-style-type: none"> Search host for Azure credentials: SharpCloud 		<ul style="list-style-type: none"> Persistence through Outlook Home Page: SensePost Ruler Persistence through custom Outlook Form Create Hidden Mailbox Rule [tool] 		
On-Prem Exchange	<ul style="list-style-type: none"> Portal Recon Enumerate domain accounts using Skype48, LyncSmash Enumerate domain accounts: OWA & Exchange Enumerate domain accounts: OWA: FindPeople OWA version discovery 	<ul style="list-style-type: none"> Password Spray using Invoke-PasswordSprayOWA, EWS, Atomizer Bruteforce of Autodiscover: SensePost Ruler PasswordSpray LyncS48 [LyncSniper] 	<ul style="list-style-type: none"> Exchange MTA 	<ul style="list-style-type: none"> Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, ODA8, Skype48) Delegation 	

Prepared by @JohnLaTwC, May 2019, v1.07

TTPs

TTP Graphic by John Lambert, @JohnLaTwC



Operation

Campaign

Large Scale Strategy



Kill Chain

	Recon	Compromise	Persistence	Expansion	Actions on Object
ATO	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets
OTBS	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets
End Point	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets
On-Proxy Exchange	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets 	<ul style="list-style-type: none"> Identify and assess all assets

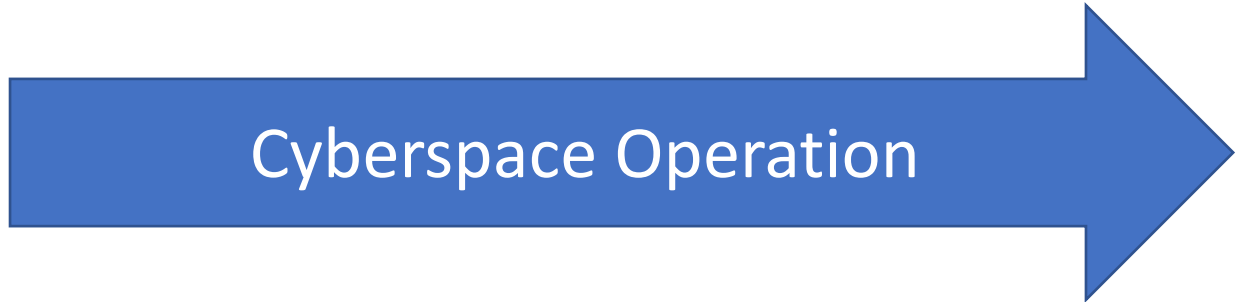
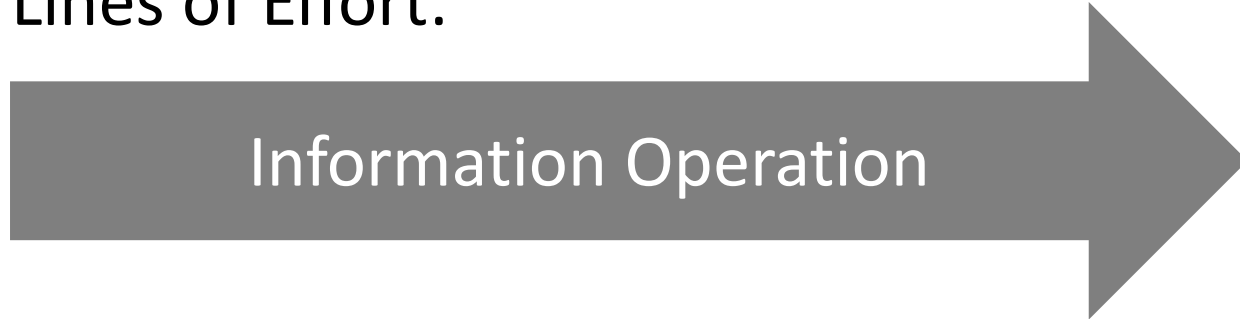
Prepared by @JohnLaTwC, May 2015, v.1.0

TTPs

TTP Graphic by John Lambert, @JohnLaTwC

Legend

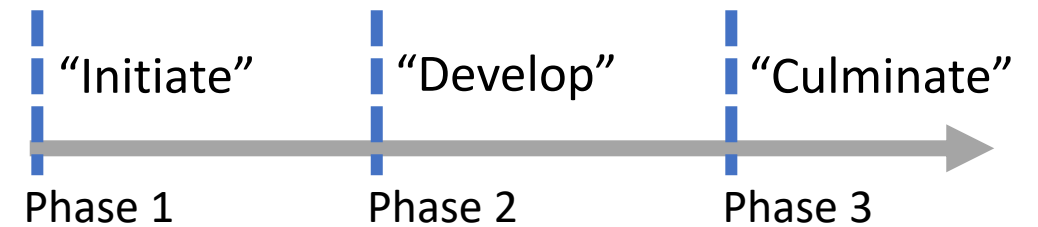
Lines of Effort:



Expected Effects:

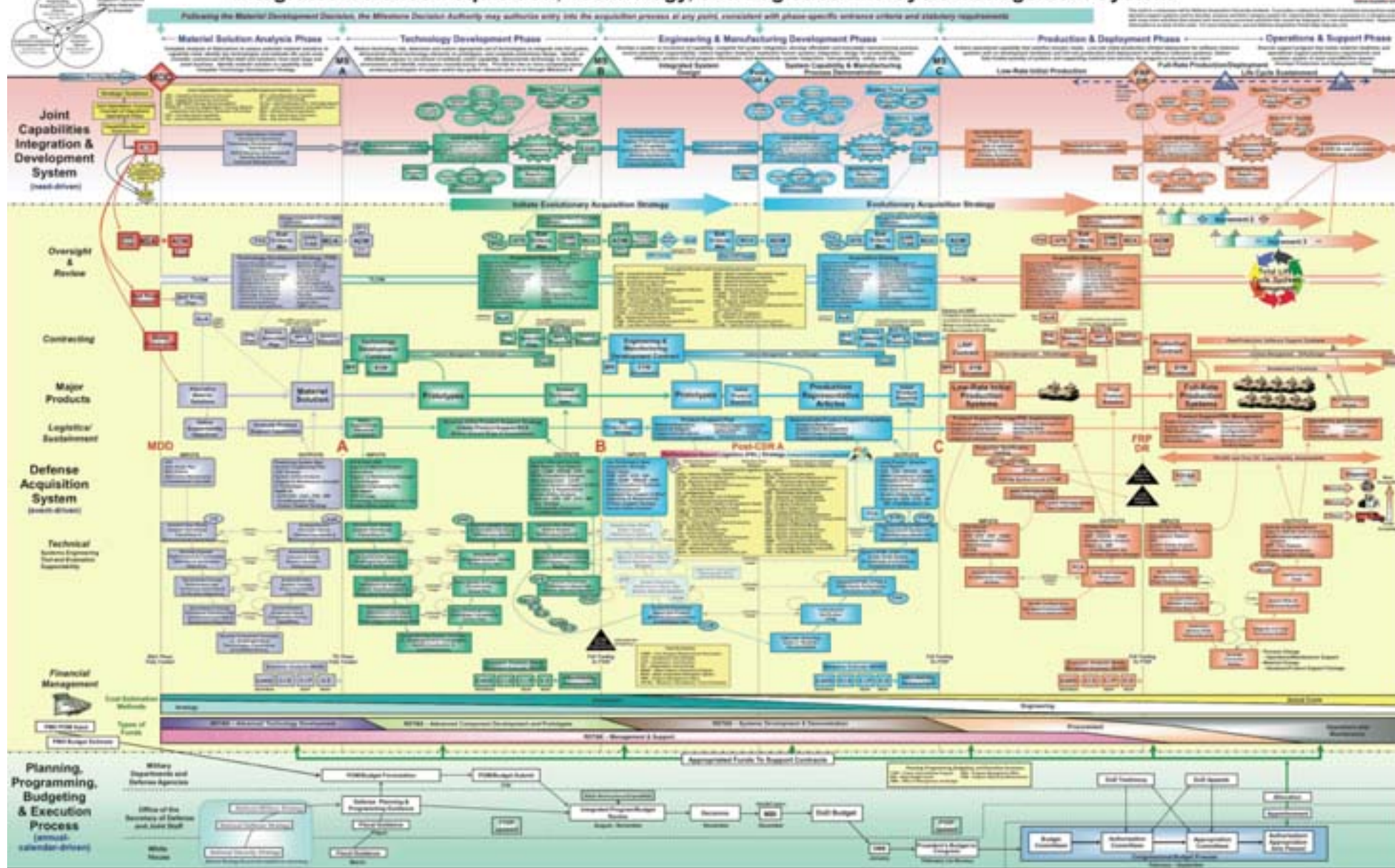


Time:



See also "An Effects-Based Approach to Planning," Annex 3-0 Operations and Planning, US Air Force, 2016
https://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-D19-OPS-Effects-Based-Plan.pdf

Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System



01

Critical Infrastructure Control

Approach: Achieve a degree of control over adversary critical infrastructure in order to exert power.

- Hold assets at-risk for deterrence purposes
- Conduct shows-of-force
- For economic warfare
- Create disruption for advantage in an armed conflict

O1 Critical Infrastructure Control

IO

Just Friendly Competition
Nothing to See Here

We didn't Do It



Show Us the Proof

Disinformation and Division



Virtual

Access Power Grid ICS

Disrupt Power Grid



Access Transportation ICS

Disrupt Transportation



Access Central Bank

Access Stock Market Systems

Disrupt Trading, Corrupt Records



Access & Surveil Corporate Communication Systems

Physical

Develop Insider Threats

Insider Operation
(across network gaps)



ZOOM

Infiltrate HW Supply Chain



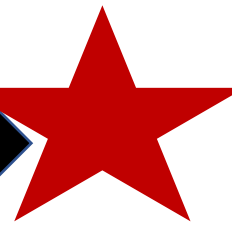
Infiltrate SW Supply Chain



Power Grid Sabotage



Armed Conflict

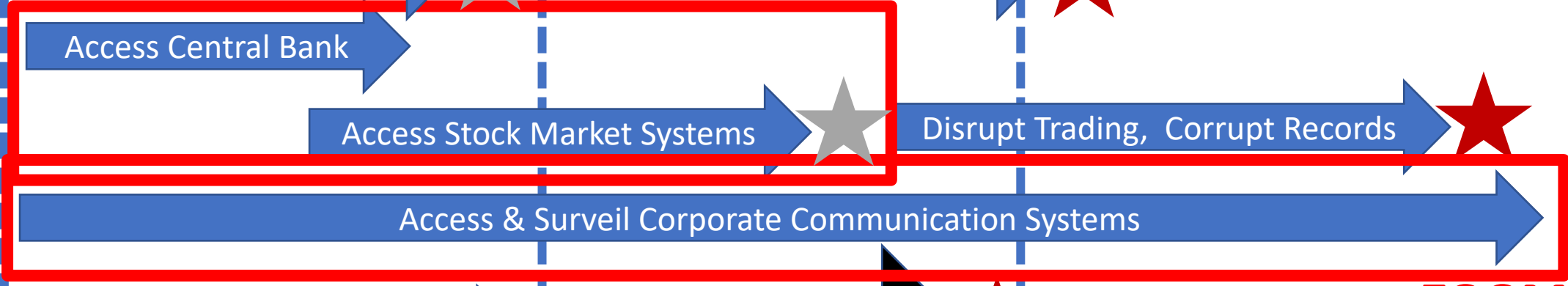


Time

Phase 1

Phase 2

Phase 3



Representative Kill Chain Detail View (w/TTPs)



AAD	<ul style="list-style-type: none"> • Dump users and groups with Azure AD 	<ul style="list-style-type: none"> • Password Spray: MailSniper • Password Spray: CredKing 			
O365	<ul style="list-style-type: none"> • Get Global Address List: MailSniper • Find Open Mailboxes: MailSniper • User account enumeration with ActiveSync 	<ul style="list-style-type: none"> • Bruteforce of Autodiscover: SensePost Ruler • Phishing for credentials • Phishing using OAuth app • 2FA MITM Phishing: evilginx2 [github] 	<ul style="list-style-type: none"> • Add Mail forwarding rule • Add Global Admin Account • Delegate Tenant Admin 	<ul style="list-style-type: none"> • MailSniper: Search Mailbox for credentials • Search for Content with eDiscovery • Account Takeover: Add-MailboxPermission • Pivot to On-Prem host: SensePost Ruler • Exchange Tasks for C2: MWR • Send Internal Email 	<ul style="list-style-type: none"> • MailSniper: Search Mailbox for content • Search for Content with eDiscovery • Exfil email using EWS APIs with PowerShell • Download documents and email
End Point	<ul style="list-style-type: none"> • Search host for Azure credentials: SharpCloud 		<ul style="list-style-type: none"> • Persistence through Outlook Home Page: SensePost Ruler • Persistence through custom Outlook Form • Create Hidden Mailbox Rule 		
On-Prem Exchange	<ul style="list-style-type: none"> • Portal Recon • Enumerate domain accounts using Skype4B • Enumerate domain accounts: OWA & Exchange • Enumerate domain accounts: OWA: FindPeople • OWA version discovery 	<ul style="list-style-type: none"> • Password Spray using Invoke-PasswordSprayOWA, EWS • Bruteforce of Autodiscover: SensePost Ruler 		<ul style="list-style-type: none"> • Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B) • Delegation 	O365/Exchange related attack techniques By @JohnLaTwC

From John Lambert, <https://twitter.com/JohnLaTwC/status/1126148047518363649>



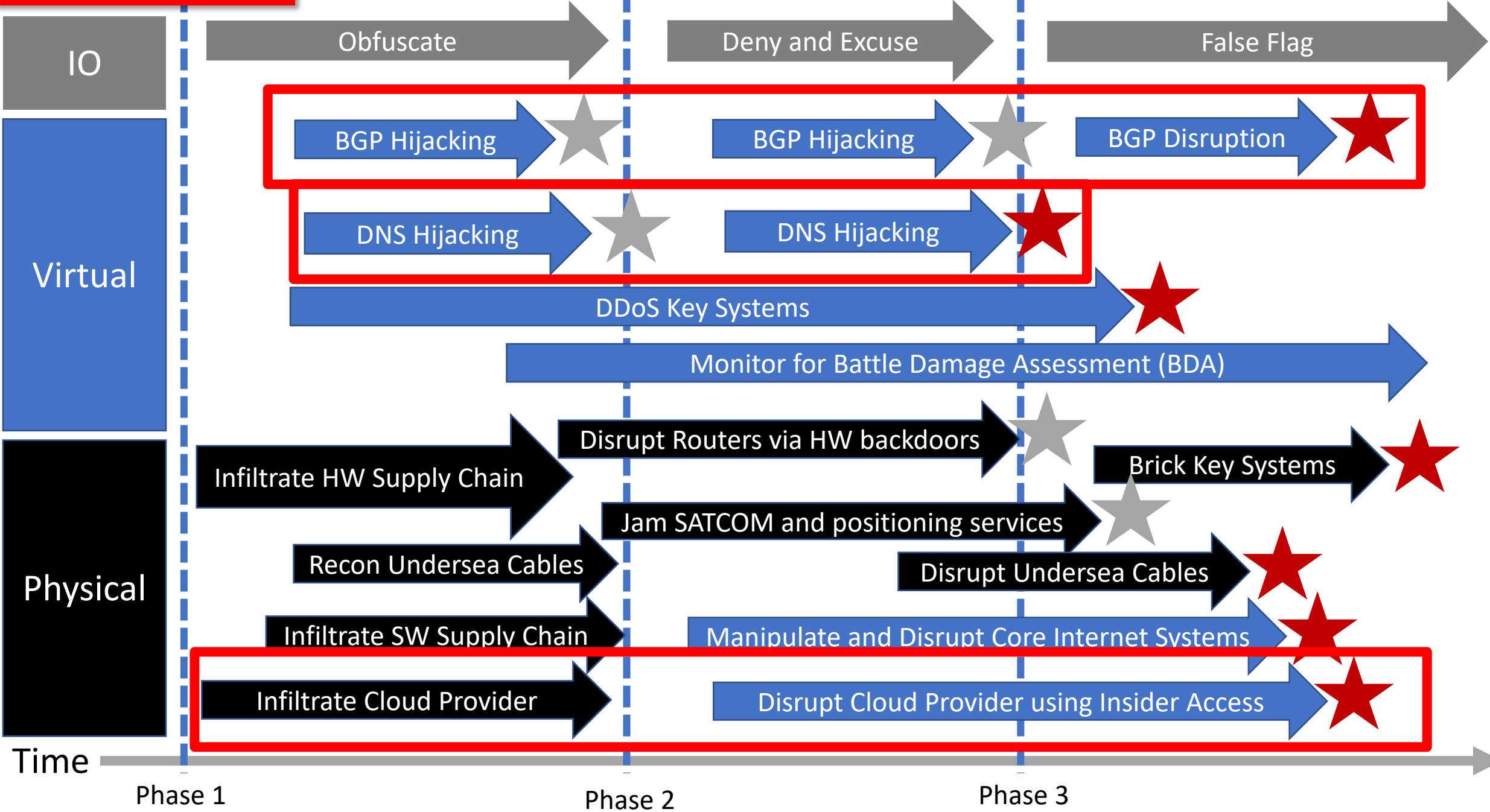
02

Cyberspace Denial

Approach: Degrade, deny, disrupt, or destroy the ability to use interconnected networks.

Exert power and induce costs by creating a loss of availability that is more intolerable for the adversary than it is for you.

O2 Cyberspace Denial





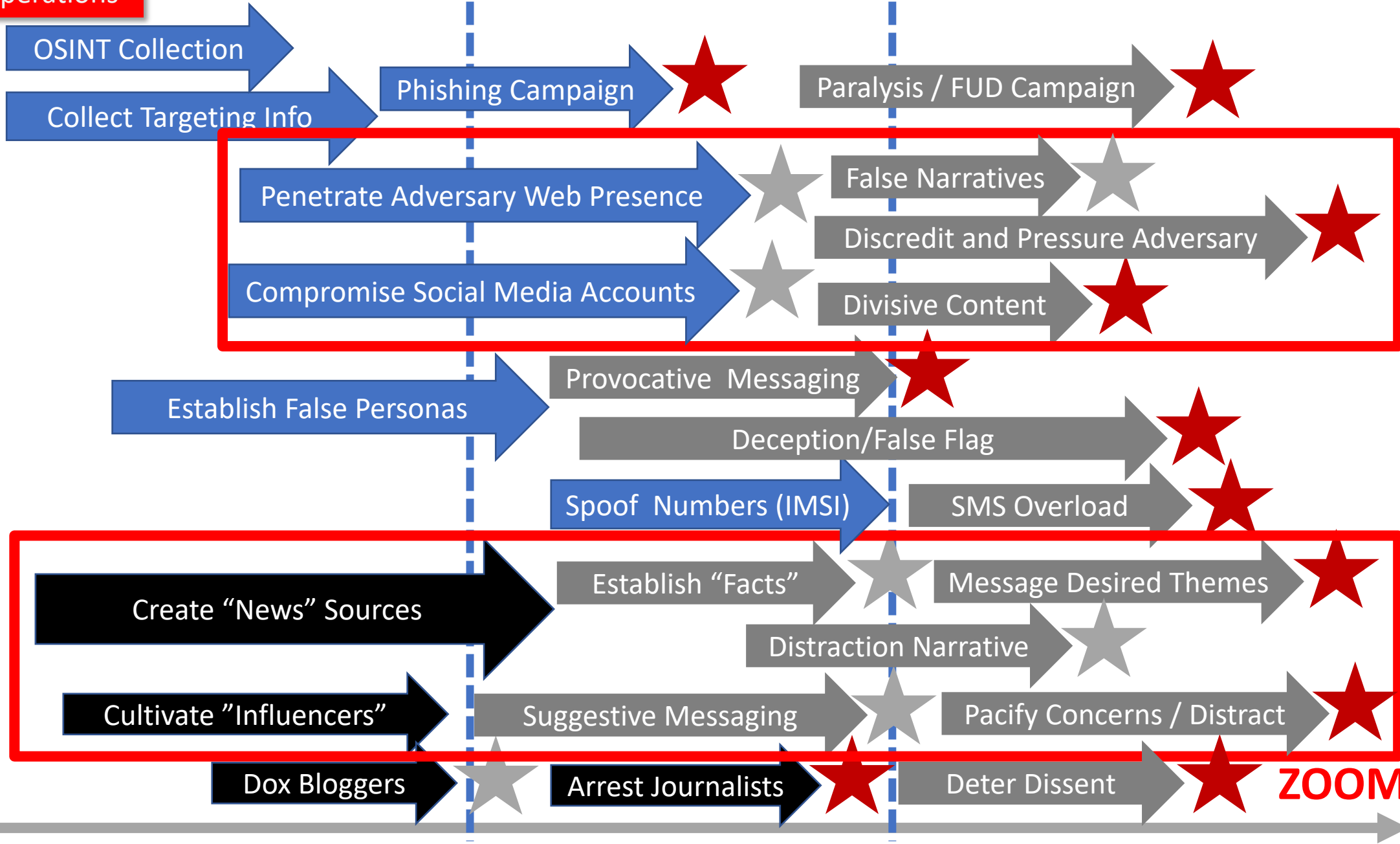
03

Influence Operations and Perception Management

Approach: Use cyberspace capabilities as intended, at least from a technical perspective, to persuade, dissuade, deceive, and influence.

Construct and deliver a body of information designed to induce your adversary to willingly act in a manner that furthers your goals.

O3 Influence Operations



Time

Phase 1

Phase 2

Phase 3

ZOOM

Information Operations Kill Chain (Zoom)



04

The Long Game – *Death of a Thousand Cuts*

Approach: Achieve long term goals through a series of actions each designed to remain below the threshold of meaningful national response.

Achieve a win without the adversary recognizing that there has even been a fight.

Staircase of Apathy

Katherine Archuleta, Director of Personnel Agency, Resigns



An adversary takes a **series of steps** over time toward their goal.

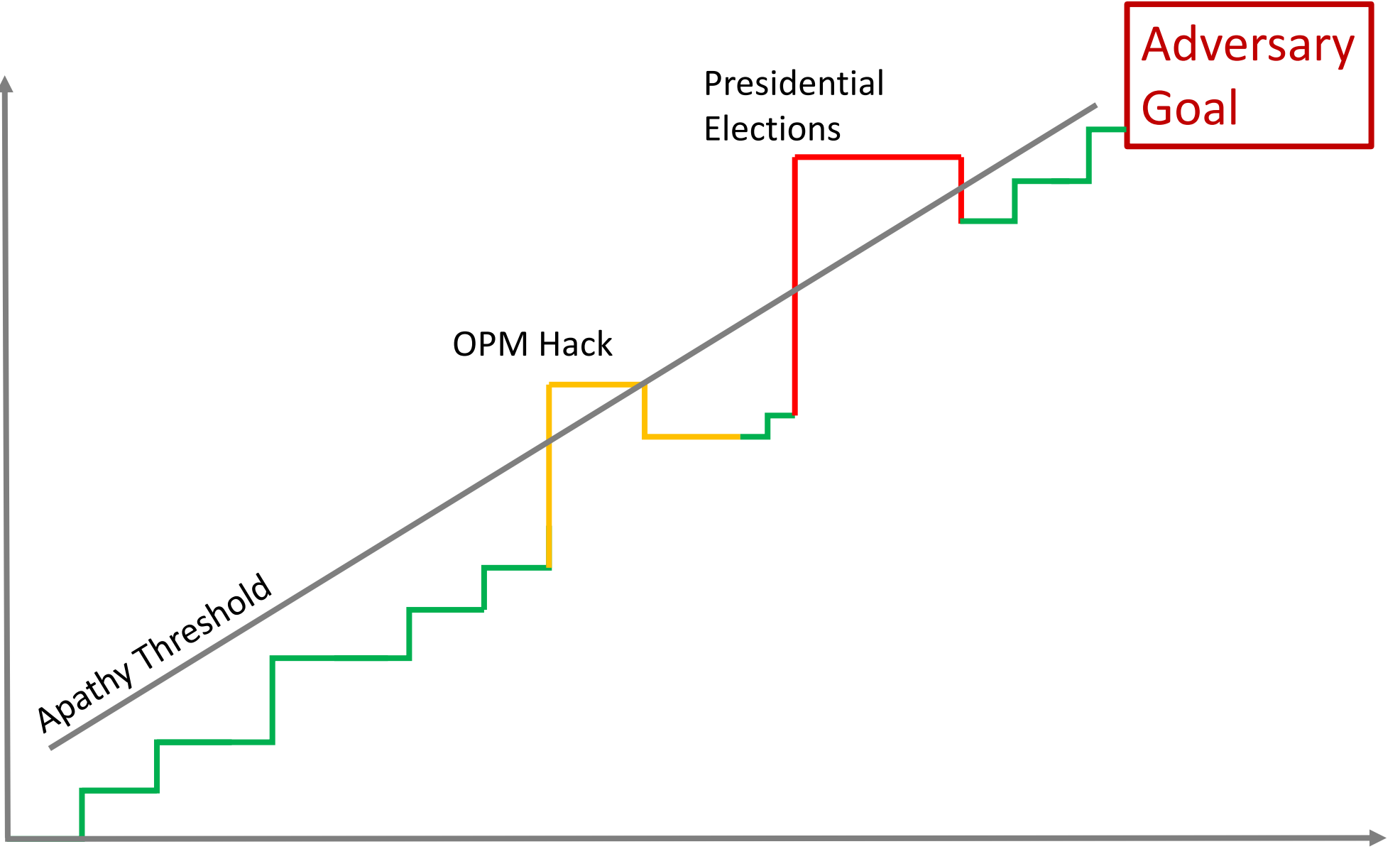
Small steps aren't noticed or acted upon.

Large steps are noticed and generate increasingly organized response

A smart adversary seeks to operate below an apathy threshold to achieve their goal

... Except when the benefit is so high that an organized response is worth the cost

Progress



OPM Hack

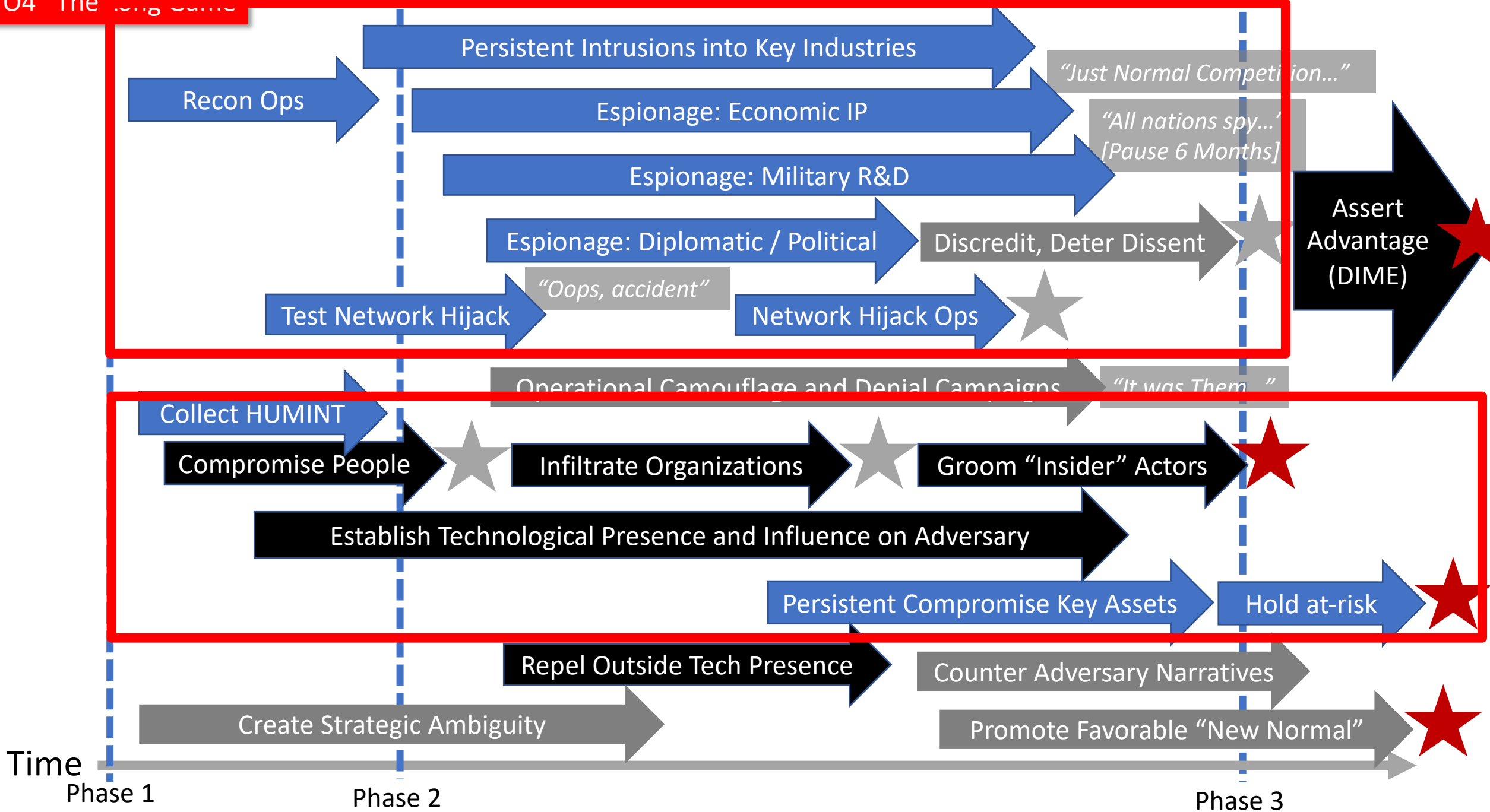
Presidential
Elections

Adversary
Goal

Apathy Threshold

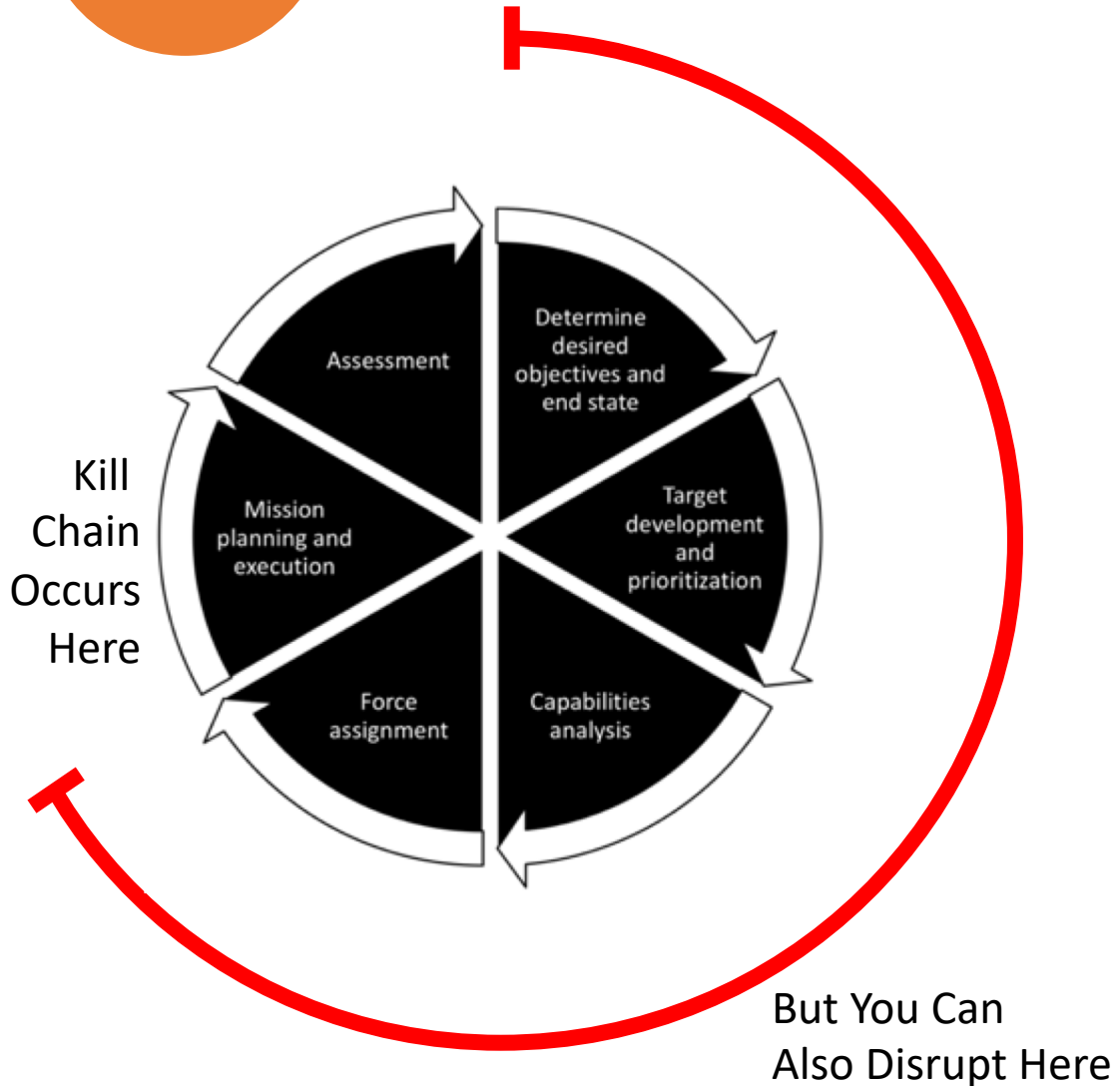
Time

O4 The Long Game



H1

Defend Forward



Approach: Reach beyond your national networks to conduct reconnaissance, detect attack preparations, and disrupt attacks, ideally preventing attacks from even taking place.

H1 Defend Forward

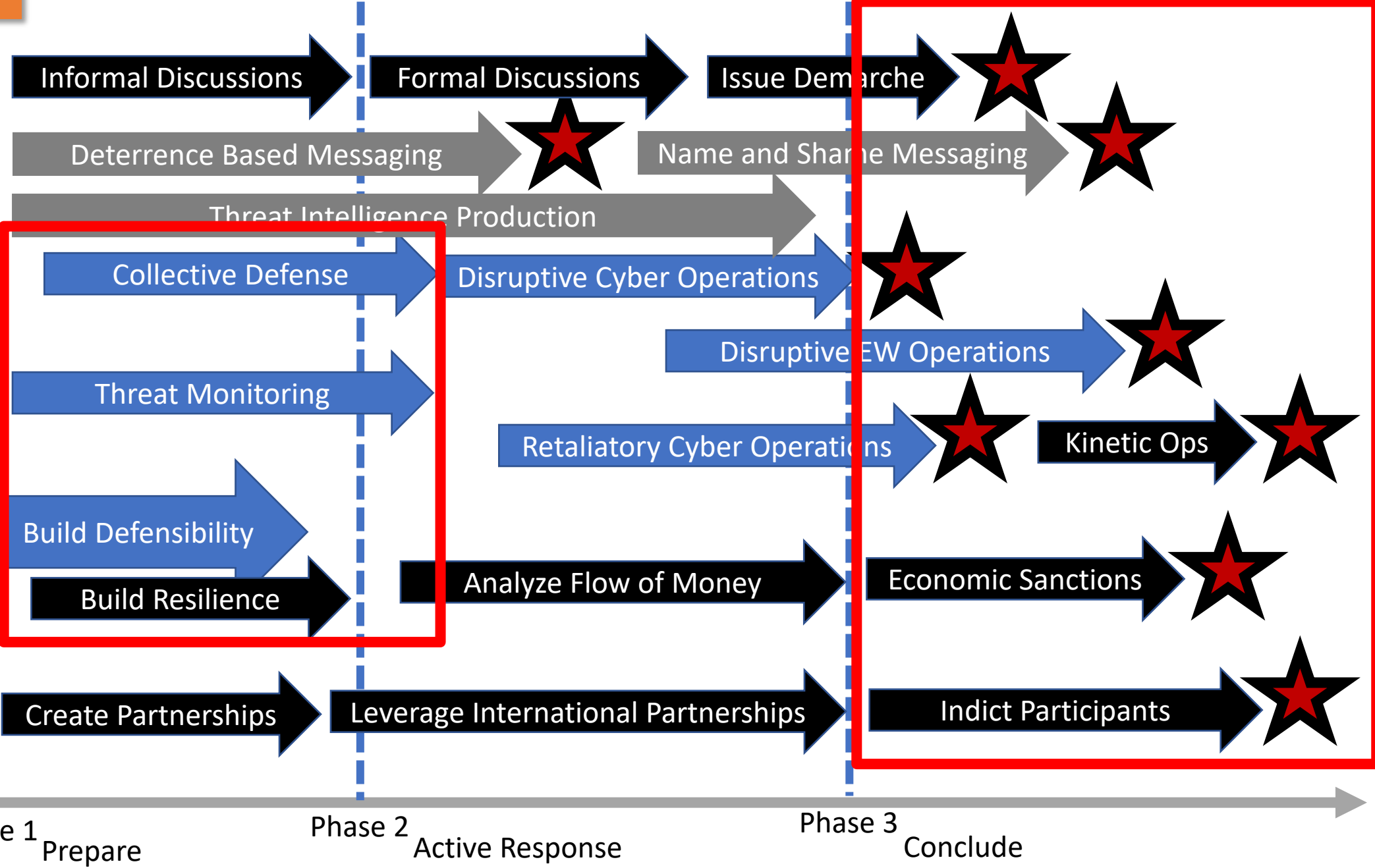
Diplomatic

IO

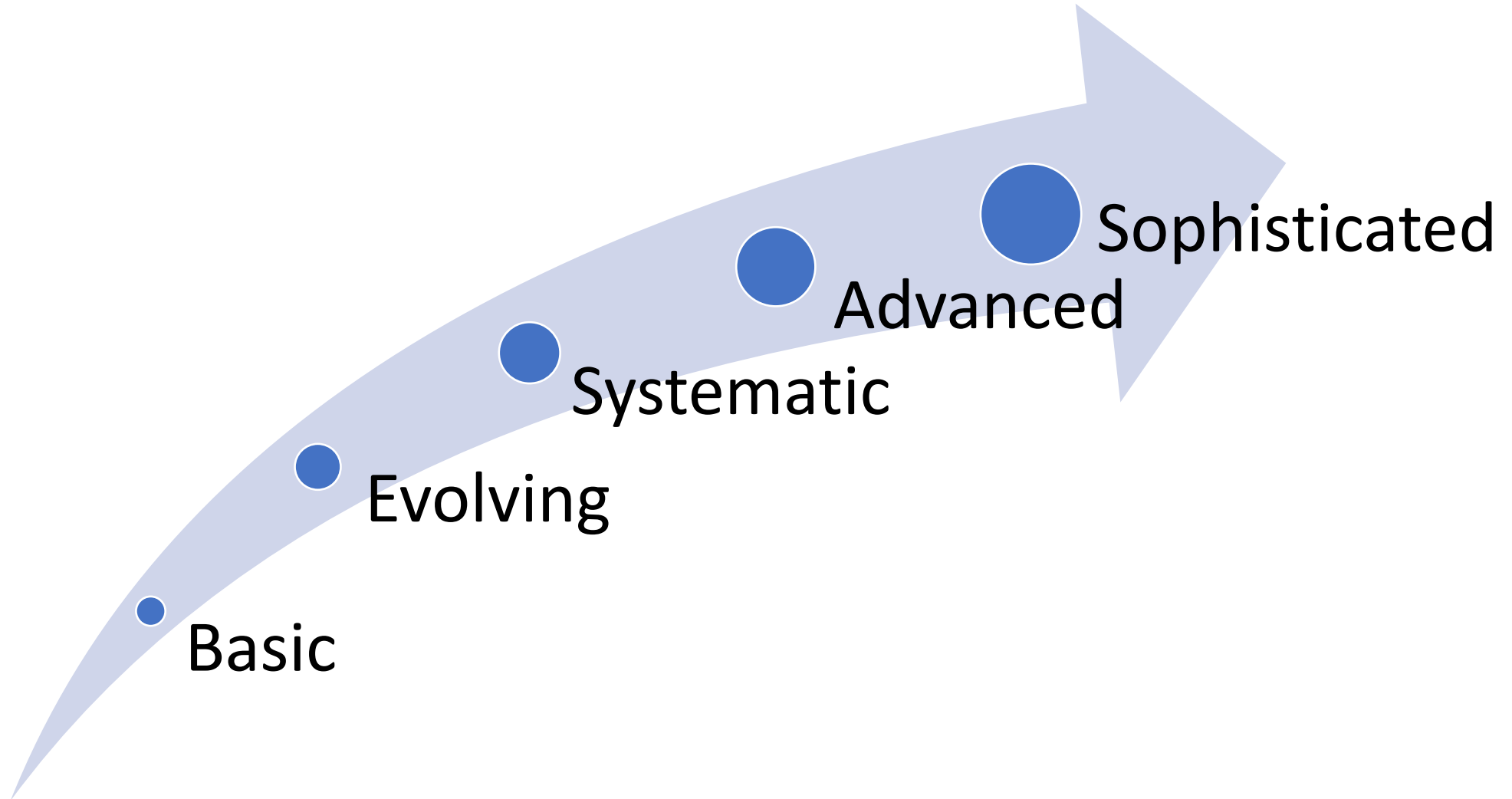
Military

Economic

Law Enforcement



Defensive Templates by Maturity



Organizational
Readiness

Interoperability &
Information Sharing

Collective
Defense

Strong



Moderate



Weak

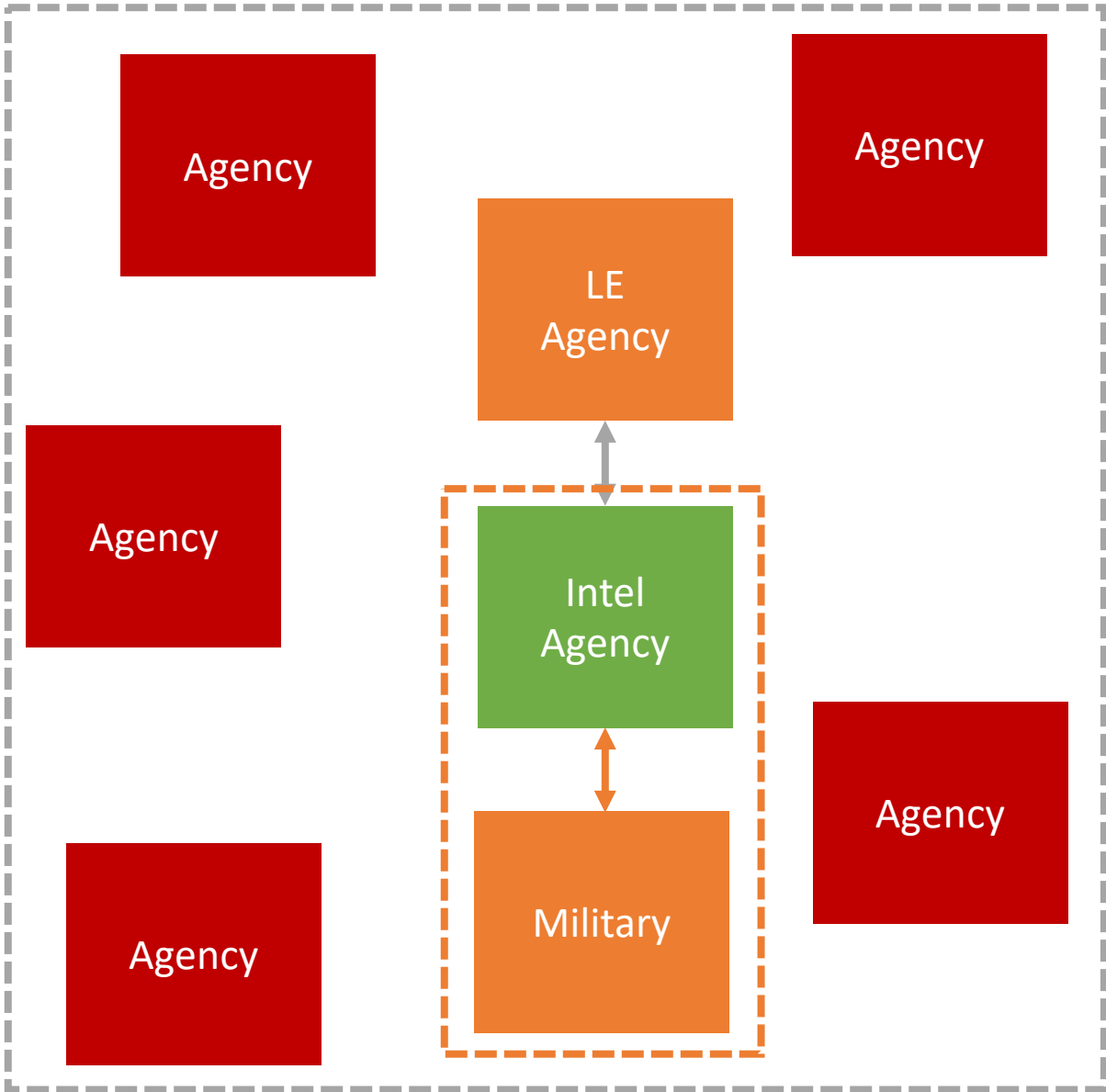


1

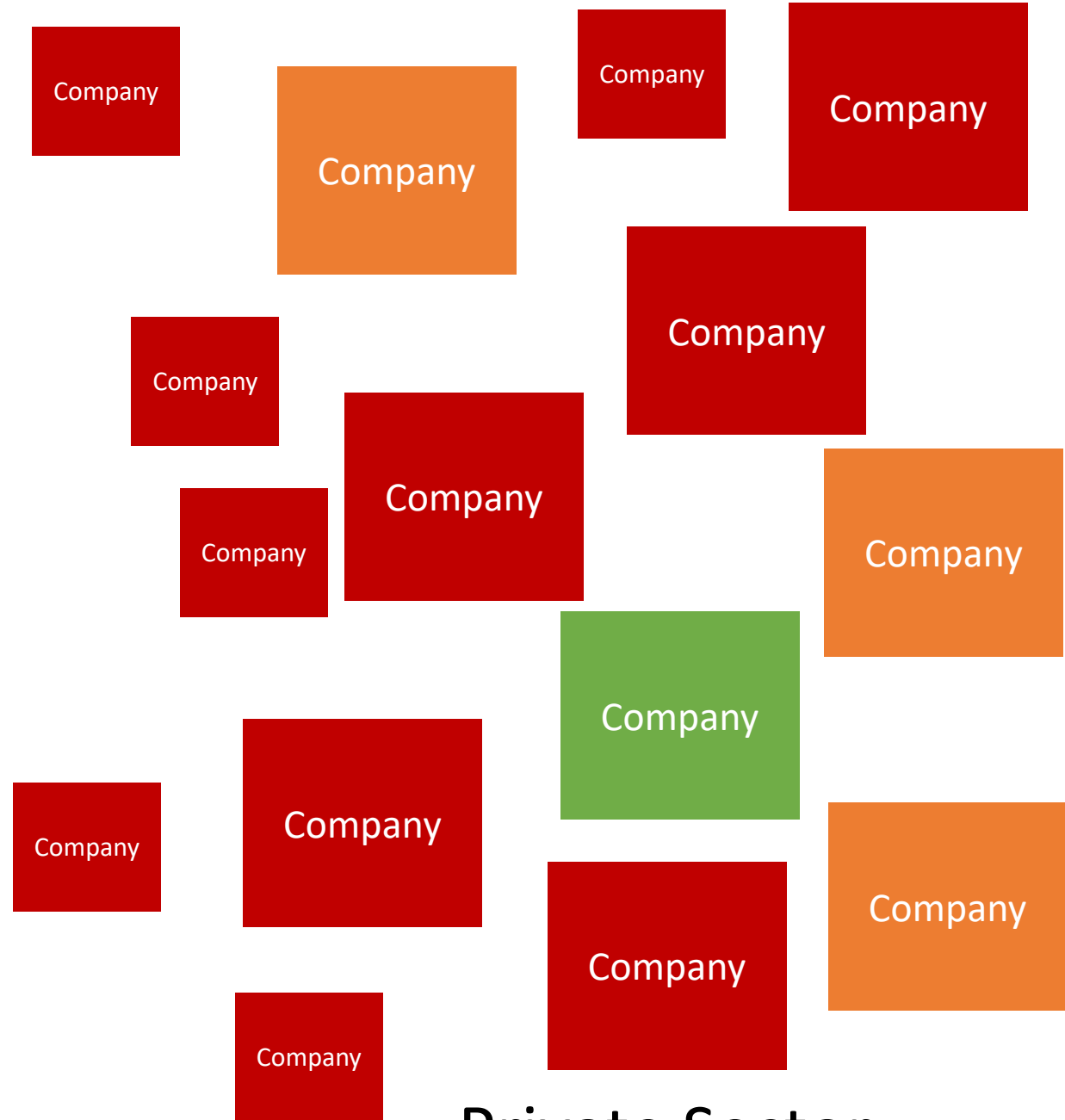
Basic

- **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

Level 1 - Basic



Government



Private Sector

What to Expect



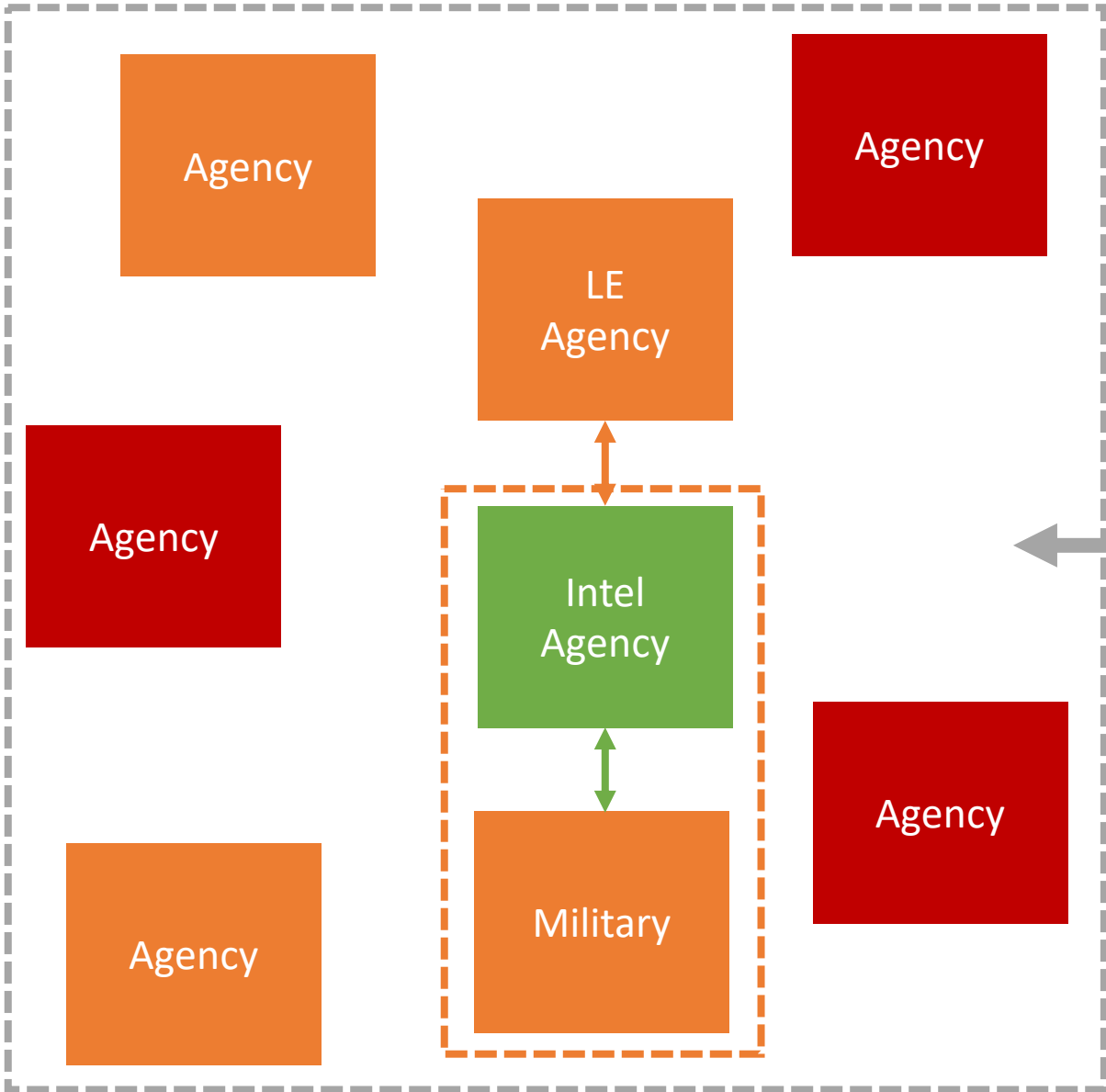
- Slow or non-existent government support (**First-ever Government interaction?**)
- Many companies corporate security will be routed
- Phone calls, post-it notes, and bulletin boards
- Running down halls unplugging systems
- Work stops
- Total disruption
- Weeks/months to recover if isolated incident

2

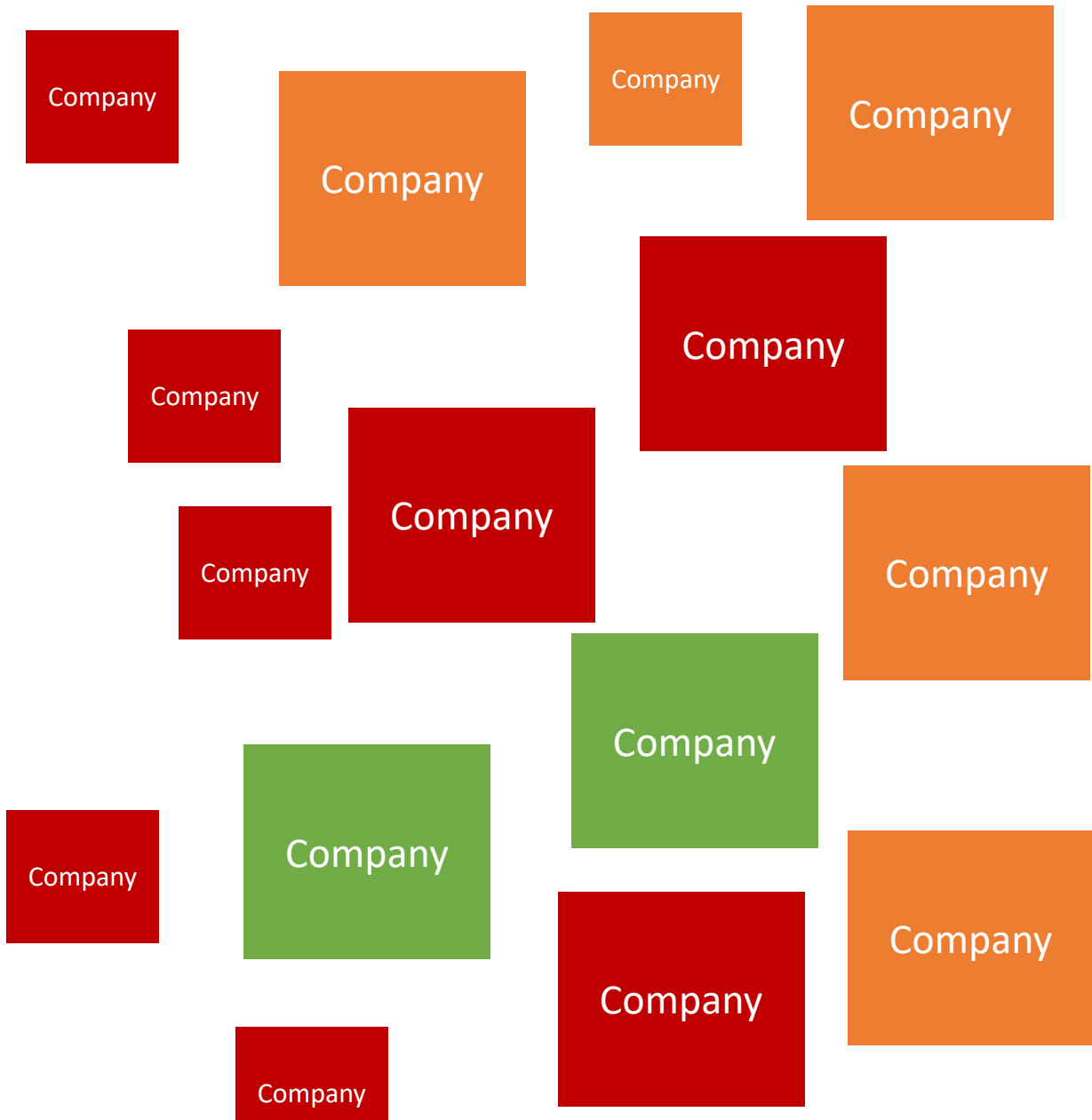
Evolving

- 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

Level 2 - Evolving



Government



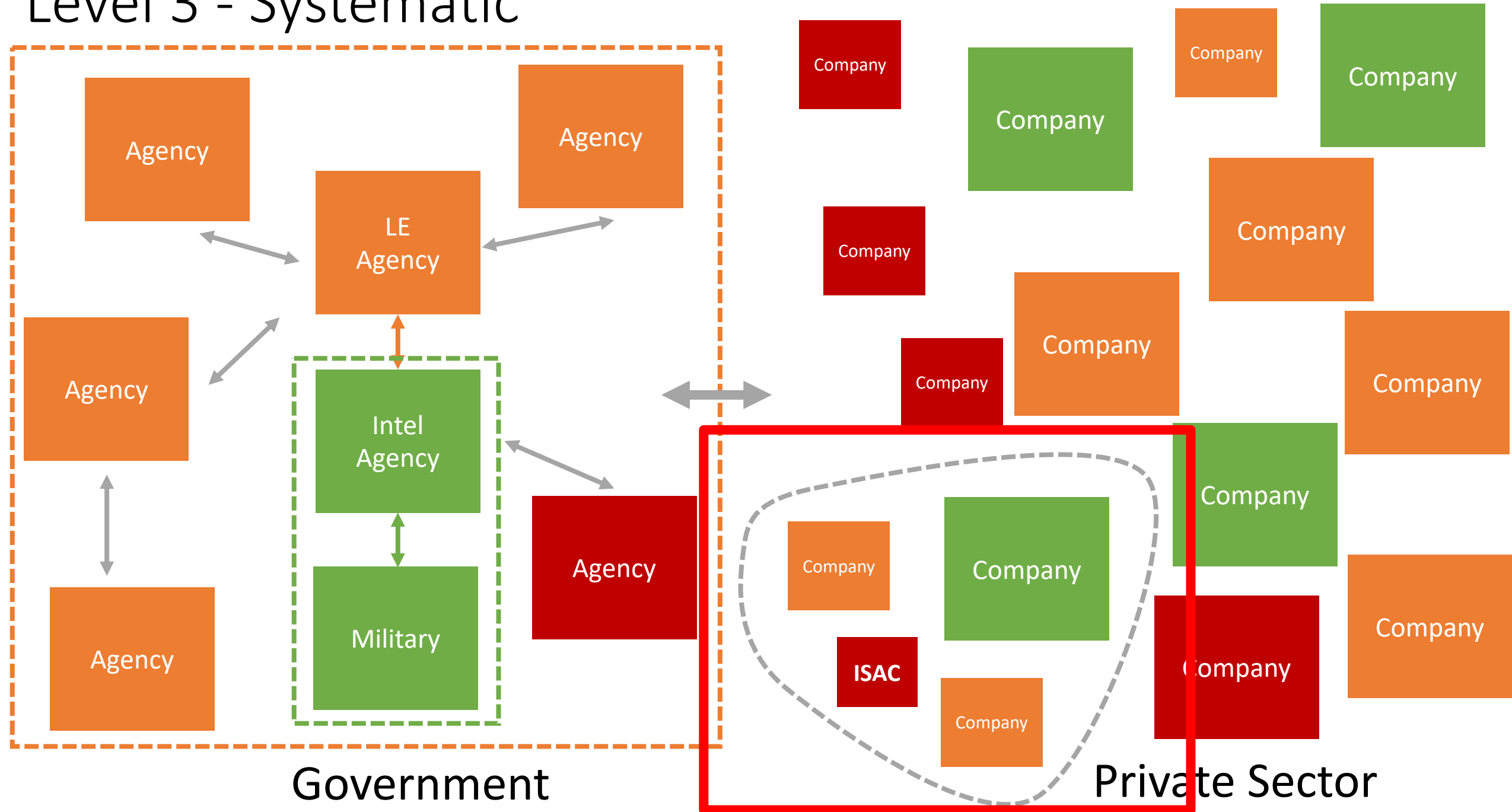
Private Sector

3

Systematic

- **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**

Level 3 - Systematic

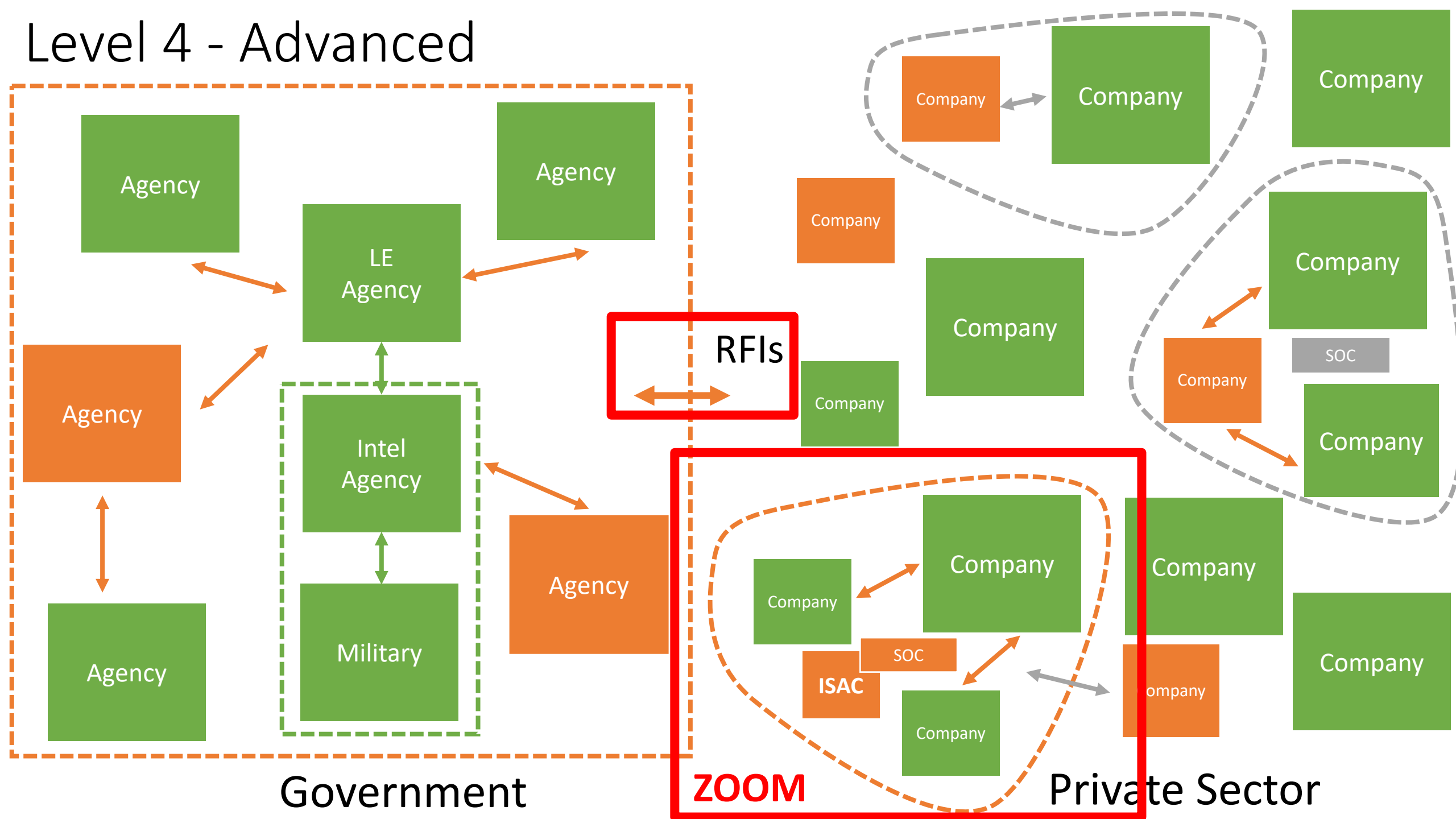


4

Advanced

- 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

Level 4 - Advanced



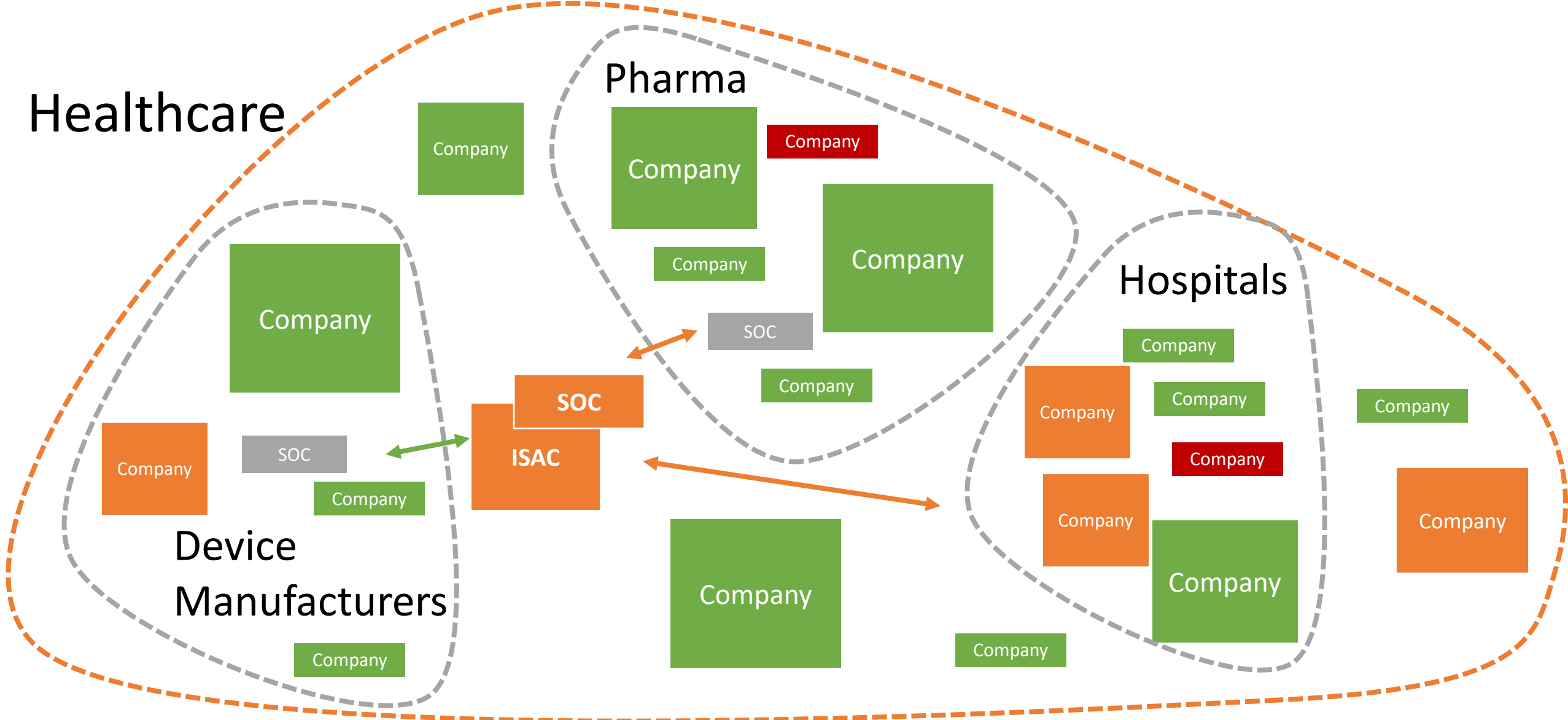
Level 4 – Advanced (Sub-Sector Zoom)

Healthcare

Pharma

Hospitals

Device
Manufacturers



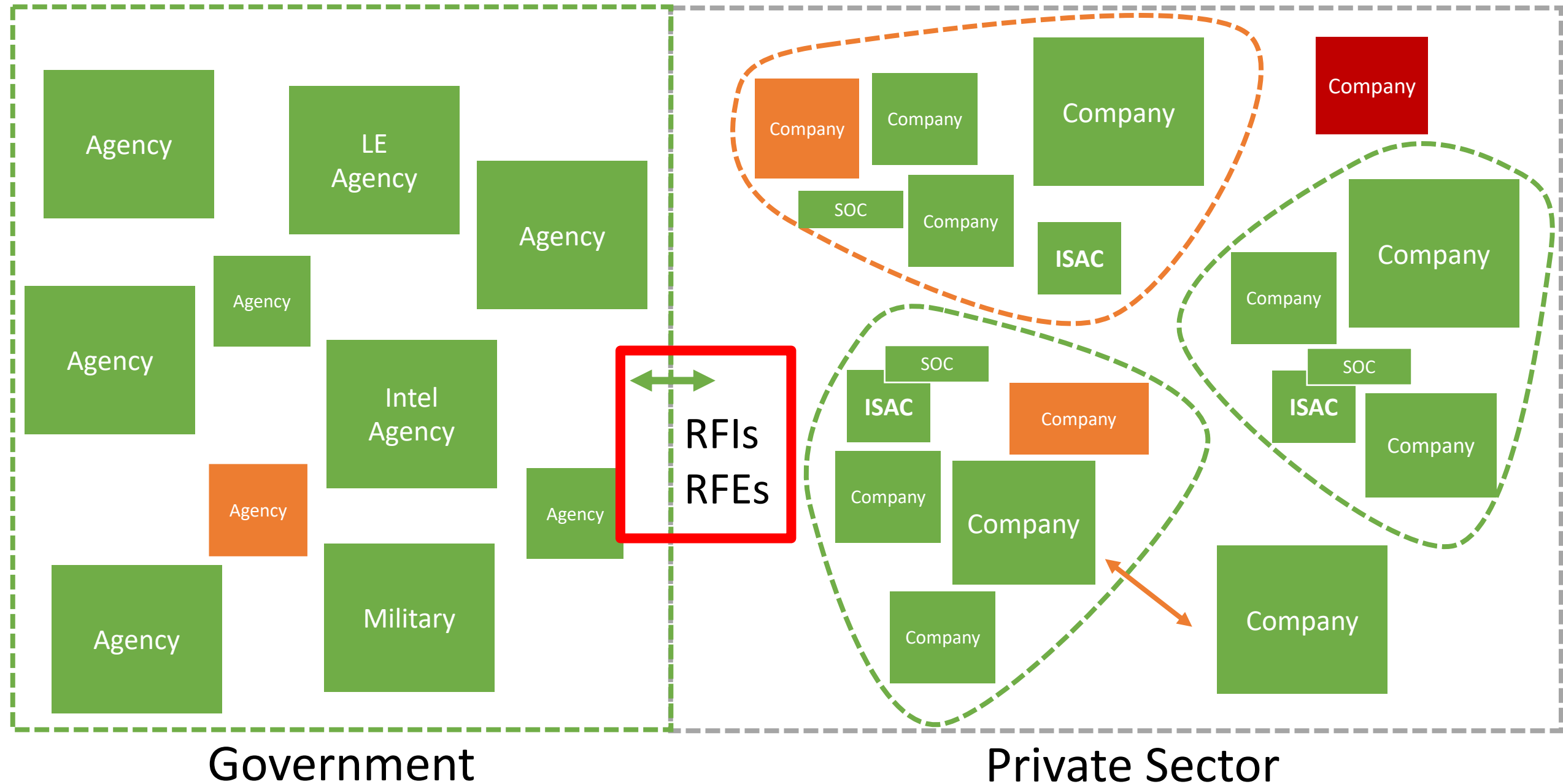
5

Sophisticated

- **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
- Advanced AI/ML defensive systems mature and widely employed

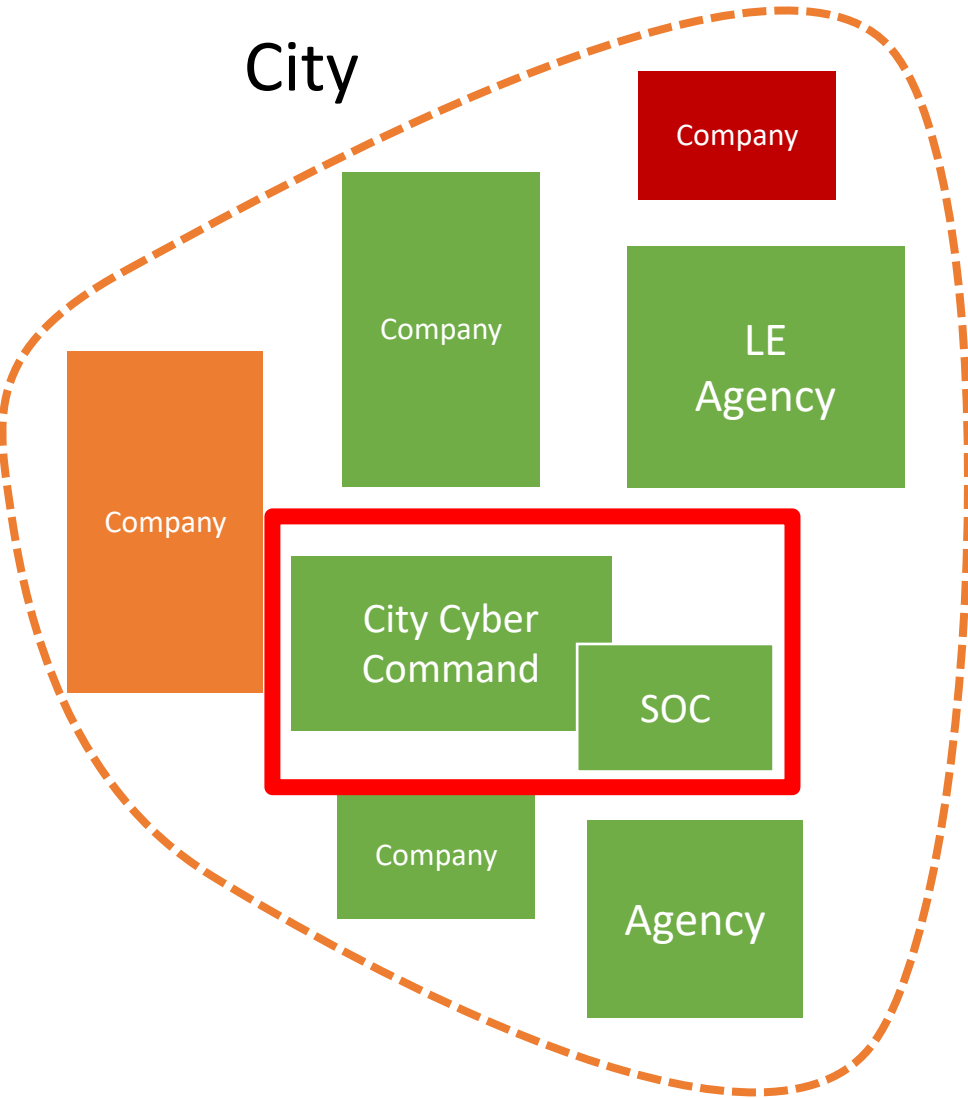
What we aspire to be

Level 5 - Sophisticated

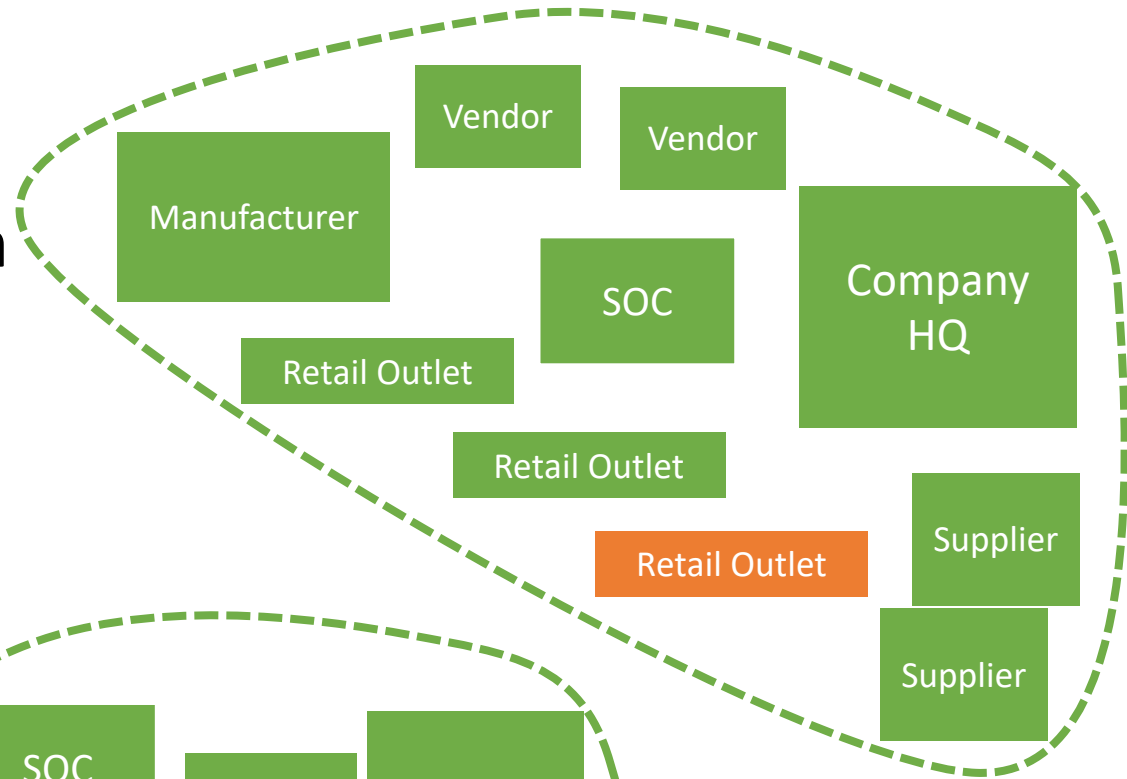


Other Models

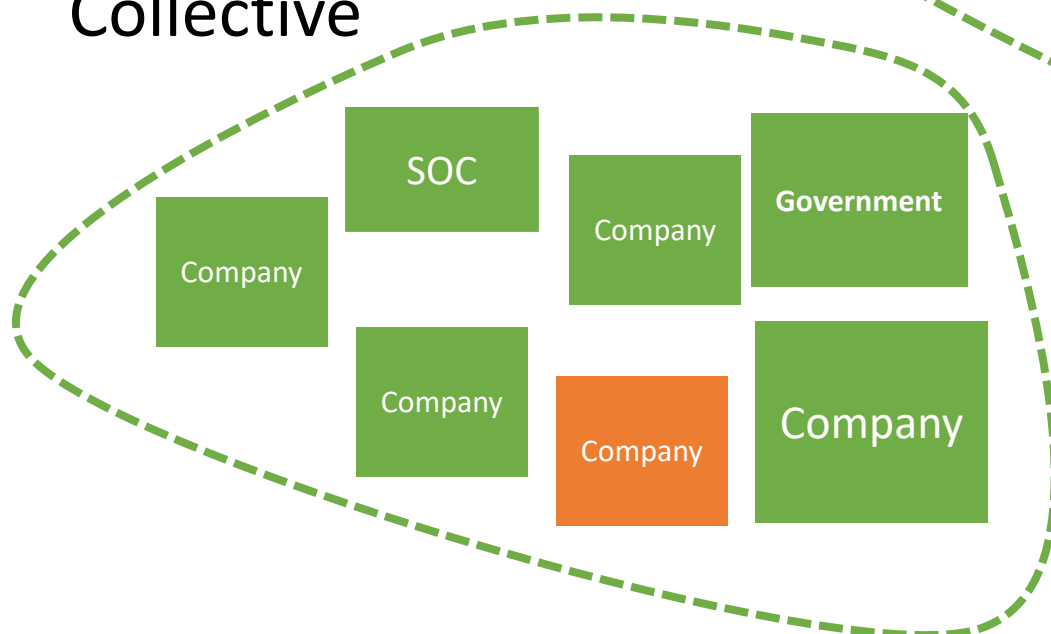
City



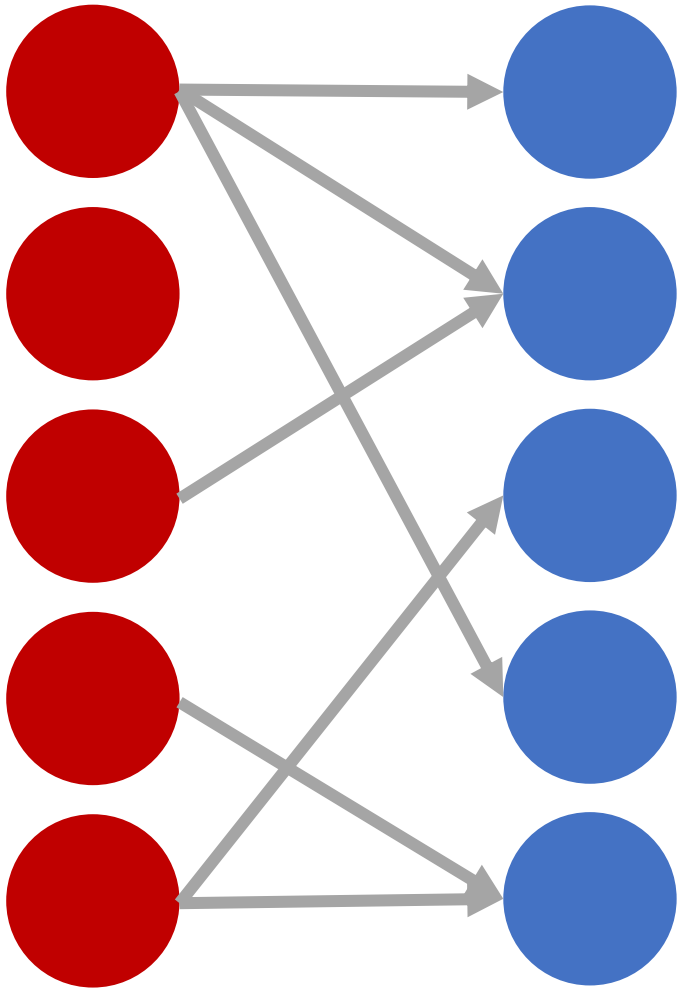
Corporate Ecosystem



Ad Hoc Collective

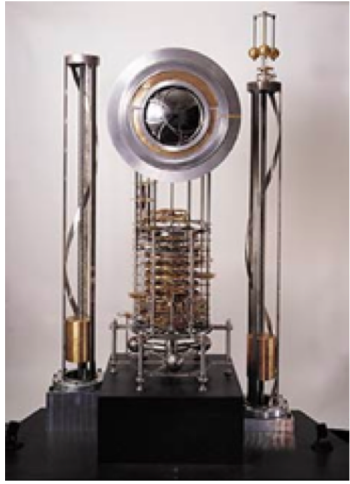


Evolving and Applying Templates



- Develop more Offensive and Defensive Templates
 - Corollary: Reverse engineer today's operations too
- Refine the Defensive Maturity Model and extend the Templates
- Link templates to TTP work, wargaming, scenario development, and training/exercises
- Attackers and defenders will apply specific templates to give them an advantage

What Can Help?



Think in Longer Time Horizons



Public/Private Partnerships for the Defense and Offense



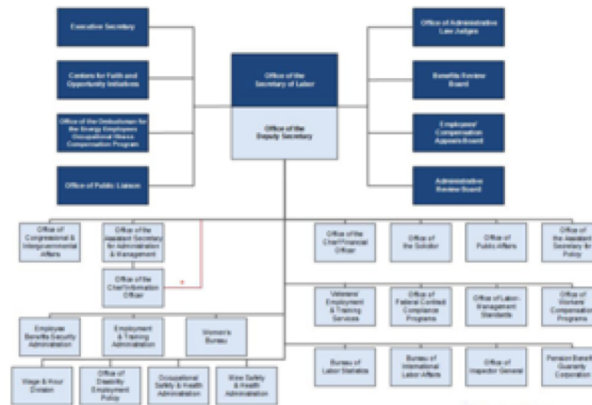
Public/Private Doctrine and Policy for Working Together



Interoperability and NRT Threat Information Sharing



Collective Exercises and Training



Re-think organizational structures and facilities



Automated Response

<http://longnow.org/clock/background/>
<https://www.pondco.com/project/combined-arms-collective-training-facility/>
<https://www.vanityfair.com/hollywood/2016/06/game-of-thrones-season-6-episode-9-battle-of-the-bastards-photos?verso=true>

Conclusions



- Collective defense is necessary. Individual heroic response (common today) is the wrong answer
- You can win or lose the battle based on your preparations
- Strong organizational defenses are necessary, but not sufficient
- Trust, teamwork, and a sense of urgency are essential for collective defense
- Military strategy and tactics apply (alarmingly) well to cybersecurity
- The Government might provide some leadership, but it won't do it for you
- **Feedback** is welcome, and see the **Whitepaper...**

Thanks...



- Terry Rice
- H-ISAC Community
- Matt Dolan
- Nick DeTore
- IronNet
- Keith Alexander
- Dave Raymond
- Tom Cross
- Our Black Hat Training Students

Questions

Greg Conti

greg.conti@ironnetcybersecurity.com

@cyberbgone

Bob Fanelli

robert.fanelli@ironnetcybersecurity.com



<https://www.youtube.com/watch?v=OWAkNNWo920>