Choosing Where to Hit
How Defenders Can Shape Adversary Behavior

Greg Conti
Tom Cross

KOPIDION

whoami

Greg Conti

Long-time Defcon and Black Hat Trainer

West Point, NSA, US Cyber Command, Georgia Tech

Extensive research and publishing on privacy and security

Defcon speaker (11x) and Black Hat Speaker (7x)

Principal at **Kopidion**

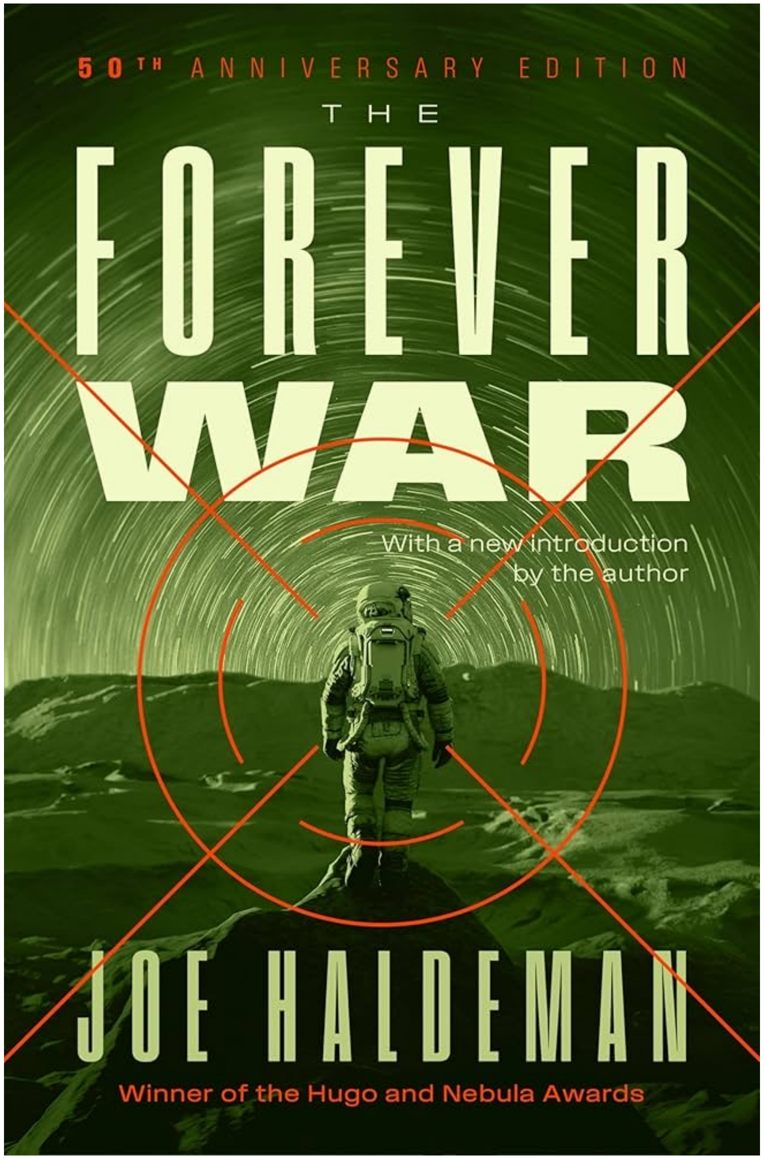
Tom Cross (Decius)

Director of Threat Research at **GetRealSecurity**

Previously: Security researcher (**IBM X-Force, Lancope**), CTO (**Drawbridge Networks, OPAQ, Fruitful**)

Principal at **Kopidion**

The views in this talk are those of the speakers and do not reflect the policy or position of our current or former employers. As we analyze types of companies, operations and tactics, we aren't suggesting any particular company has done anything or has the ability to do a given thing, that's for you to decide. All companies we describe are fictional, unless noted. You should seek qualified legal and business advice before undertaking any activities suggested here.



The Problem

Cybersecurity is too reactive

The enterprise bureaucracy measures Success™ by tickets closed, vulns patched, MTTR, KPIs, etc.

Today's model doesn't change attacker incentives or behavior

Our Thesis

The cybersecurity profession has rich models of adversary TTPs and behavior, but we do not model adversary **systems of dependencies**

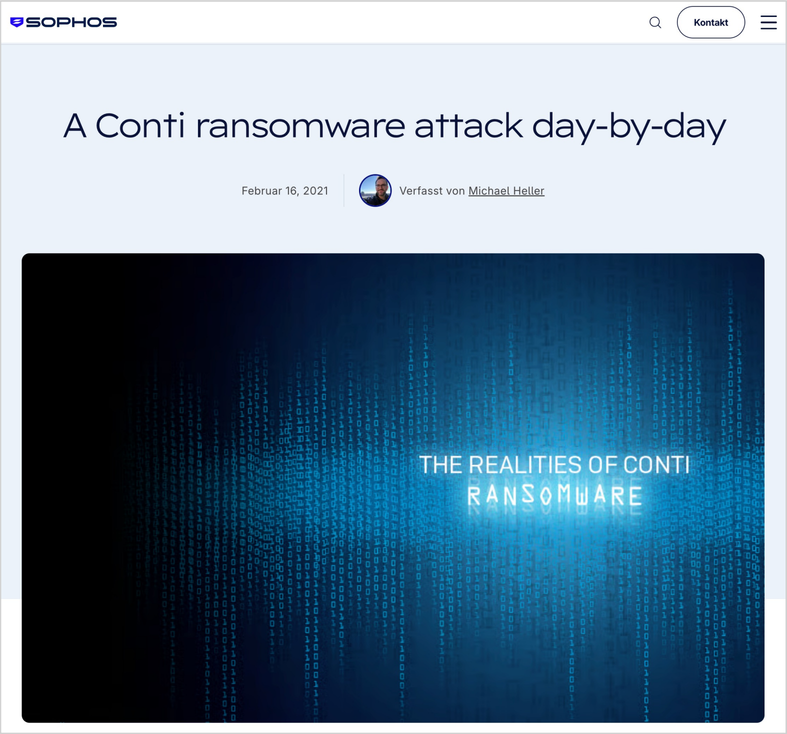
Organizations already influence adversaries, but often without focused purpose

By employing systematic Center of Gravity analysis to threat actors, it is possible to identify opportunities to apply pressure, undermine dependencies, and shape behavior

Our Ultimate Goal

Reframe how you and your organization apply power to effect adversary behavior, alone and with partners

Criminal Campaign Examples



SOPHOS

Kontakt

A Conti ransomware attack day-by-day

Februar 16, 2021 | Verfasst von Michael Heller

Initial access brokerage

Business email compromise fraud

Payment card theft campaign

Ransomware campaigns

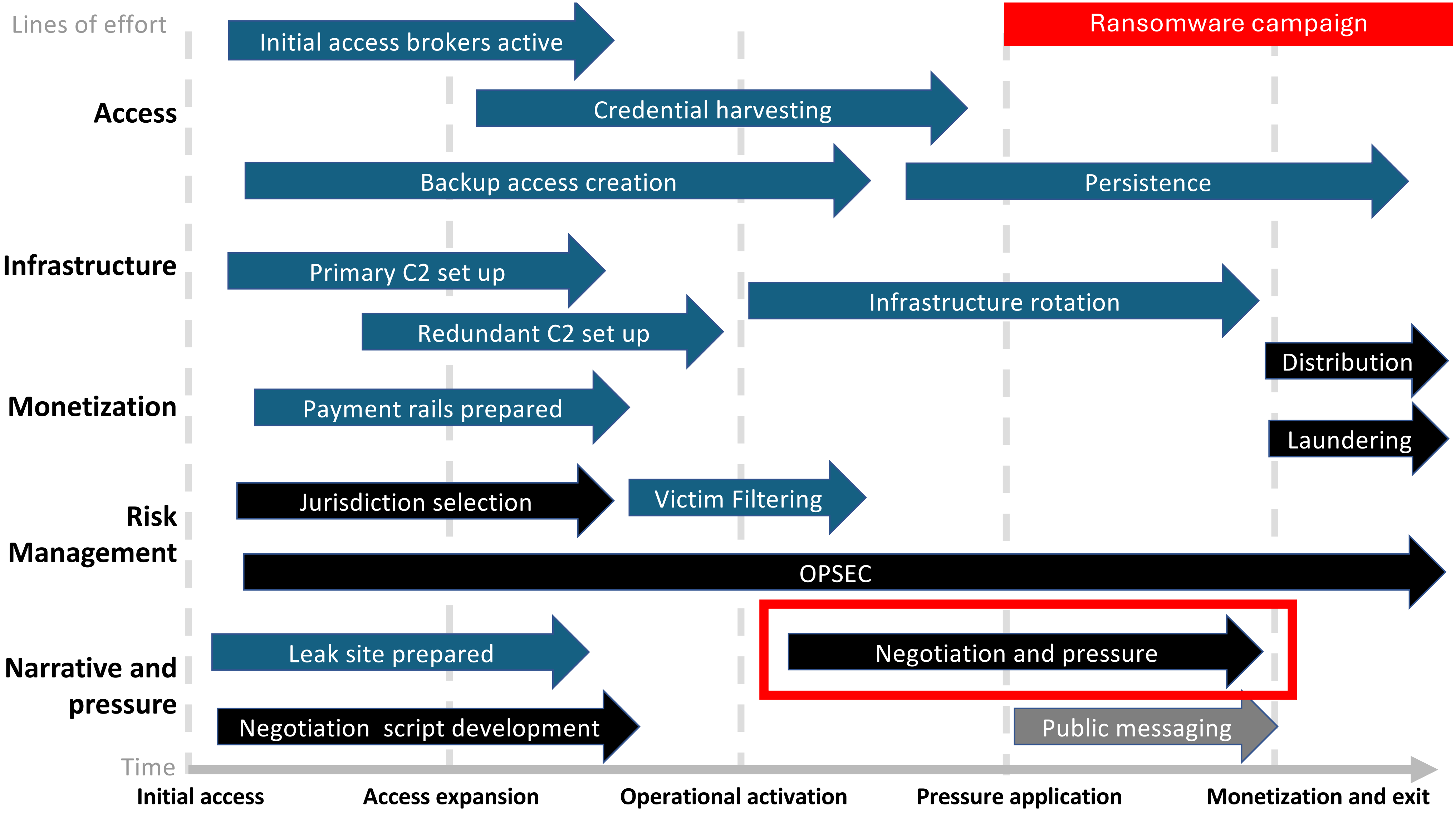
Cryptocurrency theft campaigns

Data theft and extortion

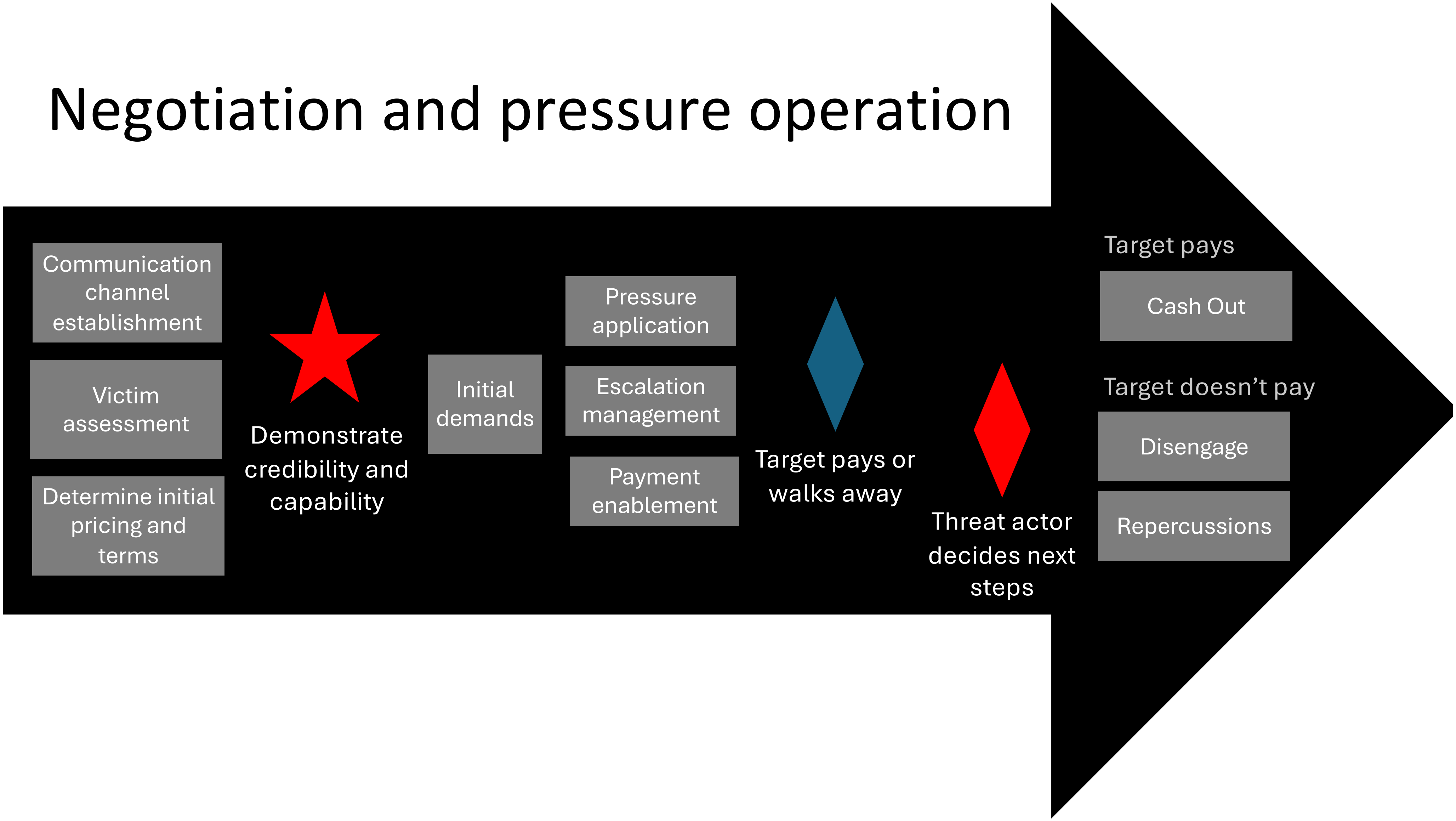
Malware distribution campaigns

Ad fraud campaigns

Credential harvesting campaigns


Lines of effort
Ransomware campaign
Access
Initial access brokers active
Credential harvesting
Backup access creation
Persistence
Infrastructure
Primary C2 set up
Infrastructure rotation
Redundant C2 set up
Distribution
Monetization
Payment rails prepared
Laundering
Risk Management
Jurisdiction selection
Victim Filtering
OPSEC
Narrative and pressure
Leak site prepared
Negotiation and pressure
Negotiation script development
Public messaging
Time
Initial access
Access expansion
Operational activation
Pressure application
Monetization and exit

Negotiation and pressure operation



Communication channel establishment

Victim assessment

Determine initial pricing and terms

Demonstrate credibility and capability

Initial demands

Pressure application

Escalation management

Payment enablement

Target pays or walks away

Threat actor decides next steps

Target pays

Cash Out

Target doesn’t pay

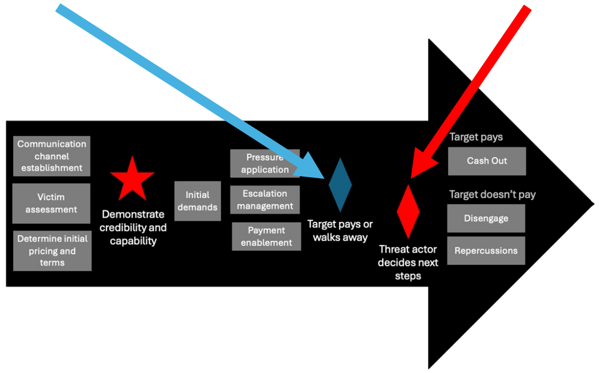
Disengage

Repercussions

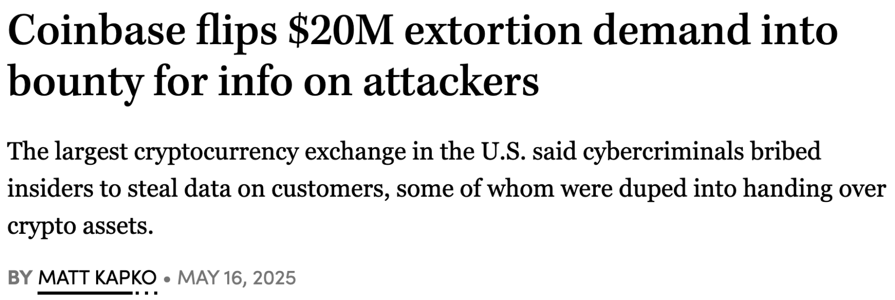
Decision points

Friendly decision point
pay or walk away

Threat actor decision point
decide next steps


Communication channel establishment
Victim assessment
Determine initial pricing and terms
Demonstrate credibility and capability
Initial demands
Pressure application
Escalation management
Payment enablement
Target pays or walks away
Threat actor decides next steps
Target pays
Cash Out
Target doesn't pay
Disengage
Repercussions

Decision point: A point where conditions force a critical choice that shapes the course of operations



Coinbase flips $20M extortion demand into bounty for info on attackers

The largest cryptocurrency exchange in the U.S. said cybercriminals bribed insiders to steal data on customers, some of whom were duped into handing over crypto assets.

BY MATT KAPKO • MAY 16, 2025

You want threat actor decision points to be dilemmas

- continue activity and accept higher exposure?
- shift infrastructure and incur cost?
- abandon access and lose investment?

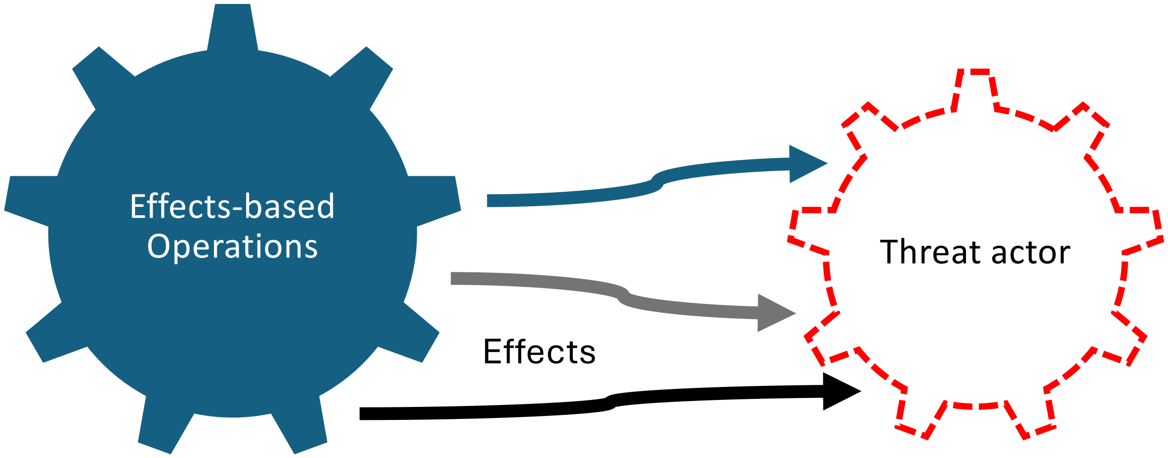
You want to consider your decision points in advance.

This reframes success away from **blocking** to **shaping**

Ransom (1996)

https://www.youtube.com/watch?v=haThIxPnYro

How can I put pressure on my adversary?



Why EBO?

Let’s say you had a date night with Kate Libby and wanted to impress.

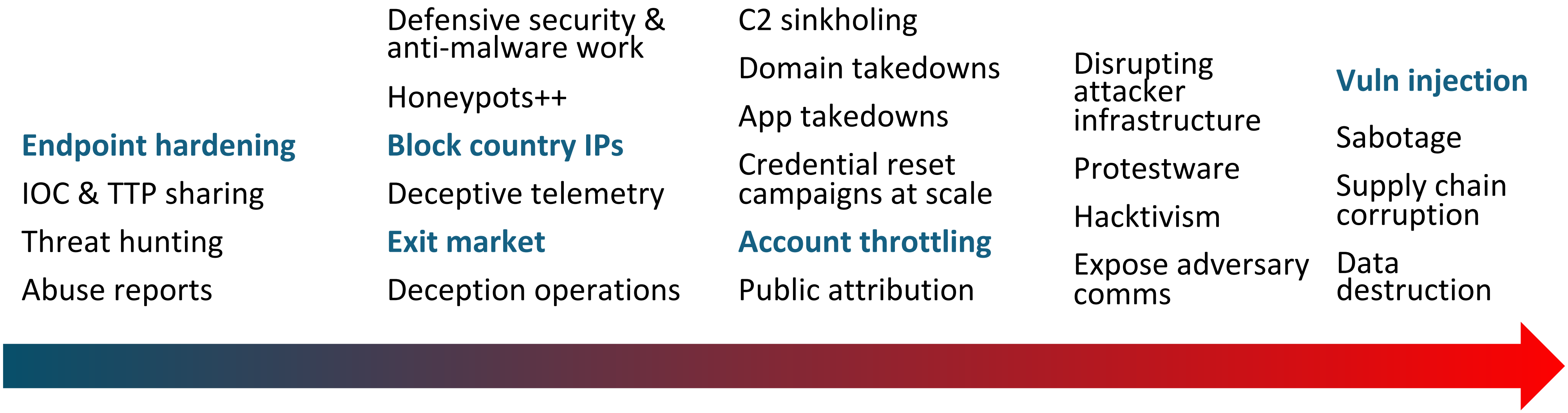
Effects-Based Operations

Taking actions designed to achieve specific outcomes on an adversary’s behavior, perception, or capabilities, rather than focusing only on tools or tactics.

It shifts the question from...
"What can I do?”
“What can I blow up?”
to...
“What effect do I want to create?”

- Force adversaries to **react on your terms**
- Create scalable advantage
- Multiply strength through **massed effects and collective operations with partners**
- Build lasting advantage by **shaping the threat environment**
- Provide options for reversible effects

A Spectrum of Effects



Endpoint hardening

IOC & TTP sharing

Threat hunting

Abuse reports

Defensive security & anti-malware work

Honeypots++

Block country IPs

Deceptive telemetry

Exit market

Deception operations

C2 sinkholing

Domain takedowns

App takedowns

Credential reset campaigns at scale

Account throttling

Public attribution

Disrupting attacker infrastructure

Protestware

Hacktivism

Expose adversary comms

Vuln injection

Sabotage

Supply chain corruption

Data destruction

What you do against financially motivated actor in **peacetime** differs from what you might do in **wartime**, and at **every stage in between**.

What tools do you have to apply pressure?

Capabilities
The tools, skills, access, infrastructure, and processes an actor can employ to produce effects.

Organic Company Capabilities (applied)
Actions a single enterprise can take using its own authority, assets, and decisions.

Example uses of capabilities
Identity-wide credential and token invalidation
Rapid revocation of trust relationships
Forced reauthentication at scale
Credible no-payment signaling and follow-through
Deliberate delay tactics to disrupt attacker tempo
Early, disciplined narrative control
Legal posture that reduces negotiation leverage
Hardening signals that reduce future targeting
Post-incident access pattern hunting across the environment

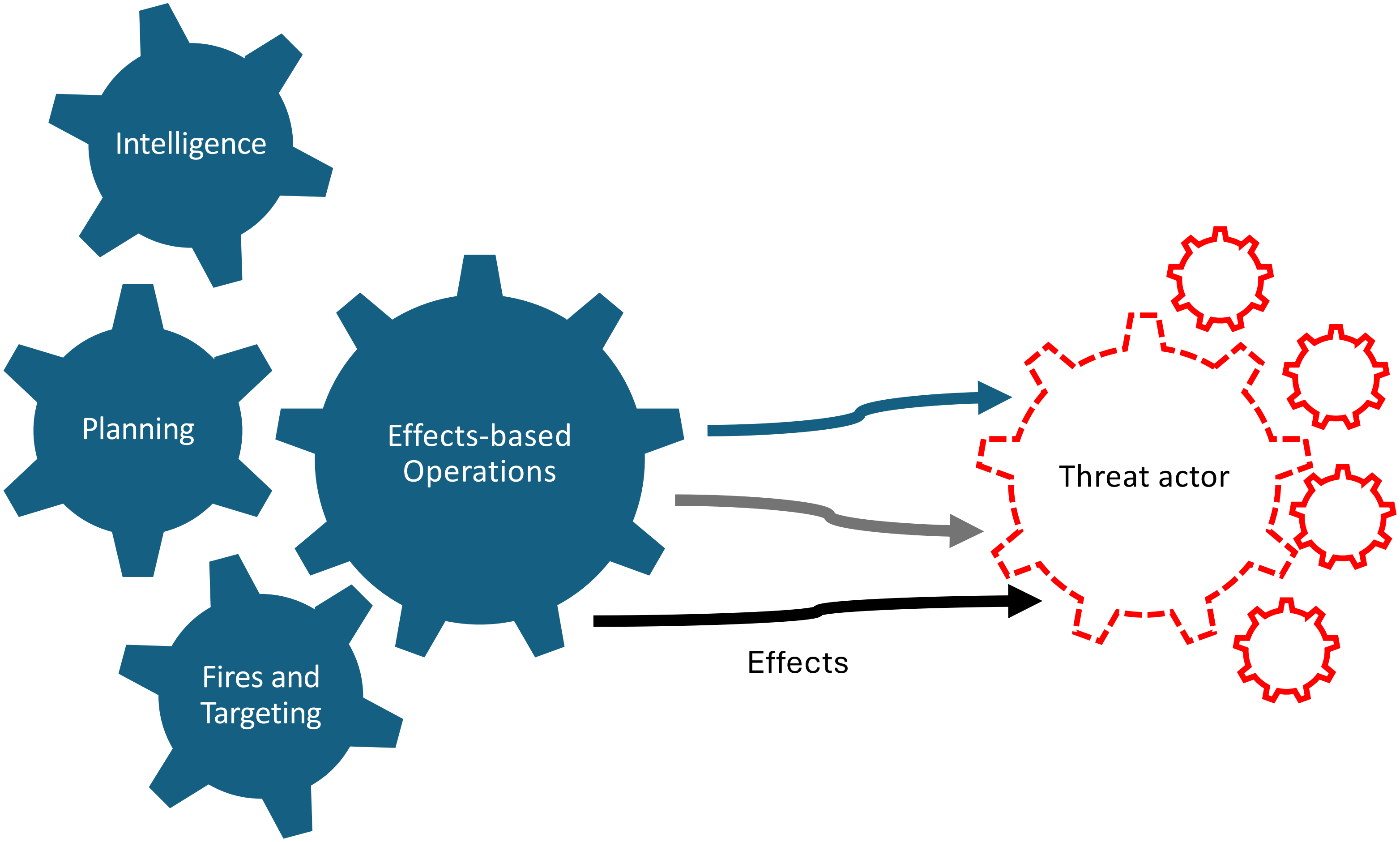
Example Adversary Decision Points (Ransomware)

	Defender EBO levers	Desired effect
DP1 Escalate privileges or maintain current foothold?	Visible containment actions that create uncertainty, rapid account resets and token invalidation, public signaling the IR is underway, coordinated LE engagement signals	Increase perceived detection probability. Cause adversary to abort early or avoid exfiltration
DP2 Exfiltrate or encrypt-only?	Strong DLP adoption across sectors, publicized failed exfiltration cases, rapid detection of suspect outbound traffic, aggressive data recovery posture	Make exfiltration unreliable and risk heavy
DP3 Increase campaign tempo or go quiet?	Coordinated infrastructure disruption, attribution pressure, sanctions and indictments, multi-organization/multi-country collaboration signals	Force adversary to slow down which reduces revenue and threat actor brand dominance
DP4 Target high-profile, high-risk firms?	Industry-wide detection sharing, publicized arrests and indictments, visible rapid response playbooks, increase LE cooperation	Shift adversary to lower-yield, lower-impact targets which reduces revenue and weakens brand signaling
DP5 Publicly name victim, extend negotiation, or quietly drop victim	Coordinated victim non-payment posture, public declarations of refusal to negotiate, rapid transparency from victim organizations, infrastructure disruption of leak sites	Make early publication of victim less economically useful and more operationally risky

What **full spectrum** capabilities do companies possess?

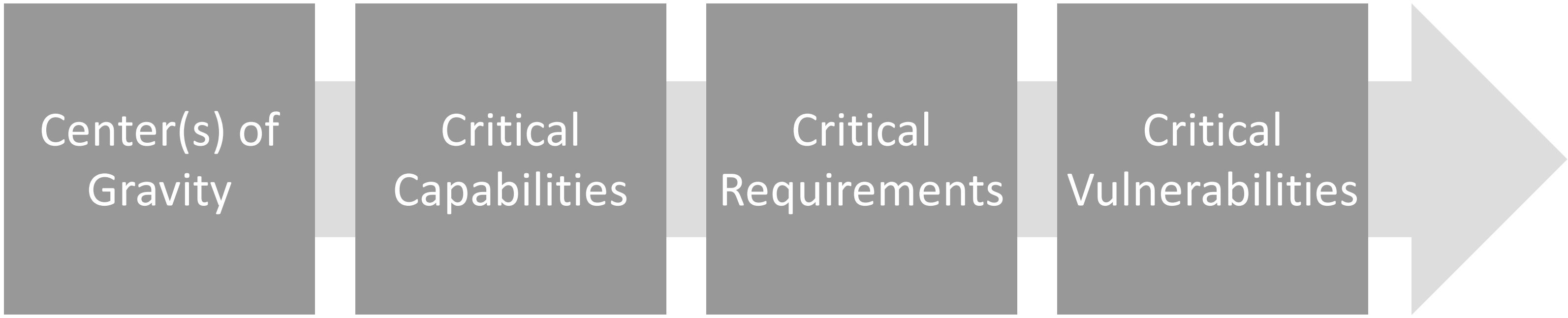
Offensive Capability	Corporate Superpower	Example Technologies & Services
Spying/Intelligence Collection	Access to Full Email Cleartext	Large Email Services
	Scanning of Computer Files	Anti-Virus, Operating Systems
	Devices with Microphones and Location Tracking	Mobile Phones, Cars
	Mapping of People's Relationships	Social Media, Mobile Phones
Real World Mapping and Reconnaissance	Devices with Cameras	Laptops, Mobile Phones (including citizen reporting via apps), Cars, Drones, Vacuums
	Infrastructural Cameras	CCTV, Smart Cities Infrastructure
	Robots that Map Physical Spaces	Vacuums, Cars, Delivery Drones
Influence Operations	Prioritizing Content that People See	Search Engines, Social Media
Gaining Access to Networks/Infrastructure	Backdoors Deployed Inside Networks	Lightbulbs, IOT, Infrastructure & Software
Denying Access to Services/Infrastructure	Selective/Targeted Outages	Satellite Internet Services, and everything else
Supply and Logistics	Moving People and Objects	Rideshare Services, Delivery Drones
	Manipulate Supply Chains (Deny or Modify Items)	Online Retailer, Shipping Company
Arresting People	Capturing and Moving People	Robot Taxis, also vulnerable CAN bus in cars?
Destroying Things	Destroying Data	Backdoored Open Source Project
	Destroying Real World Objects	Robot Taxis, Drones

How can I put pressure on my adversary?



Choosing where to hit

Center of Gravity (COG) Analysis



what provides the actor freedom of action or strength

what the COG must be able to do to function

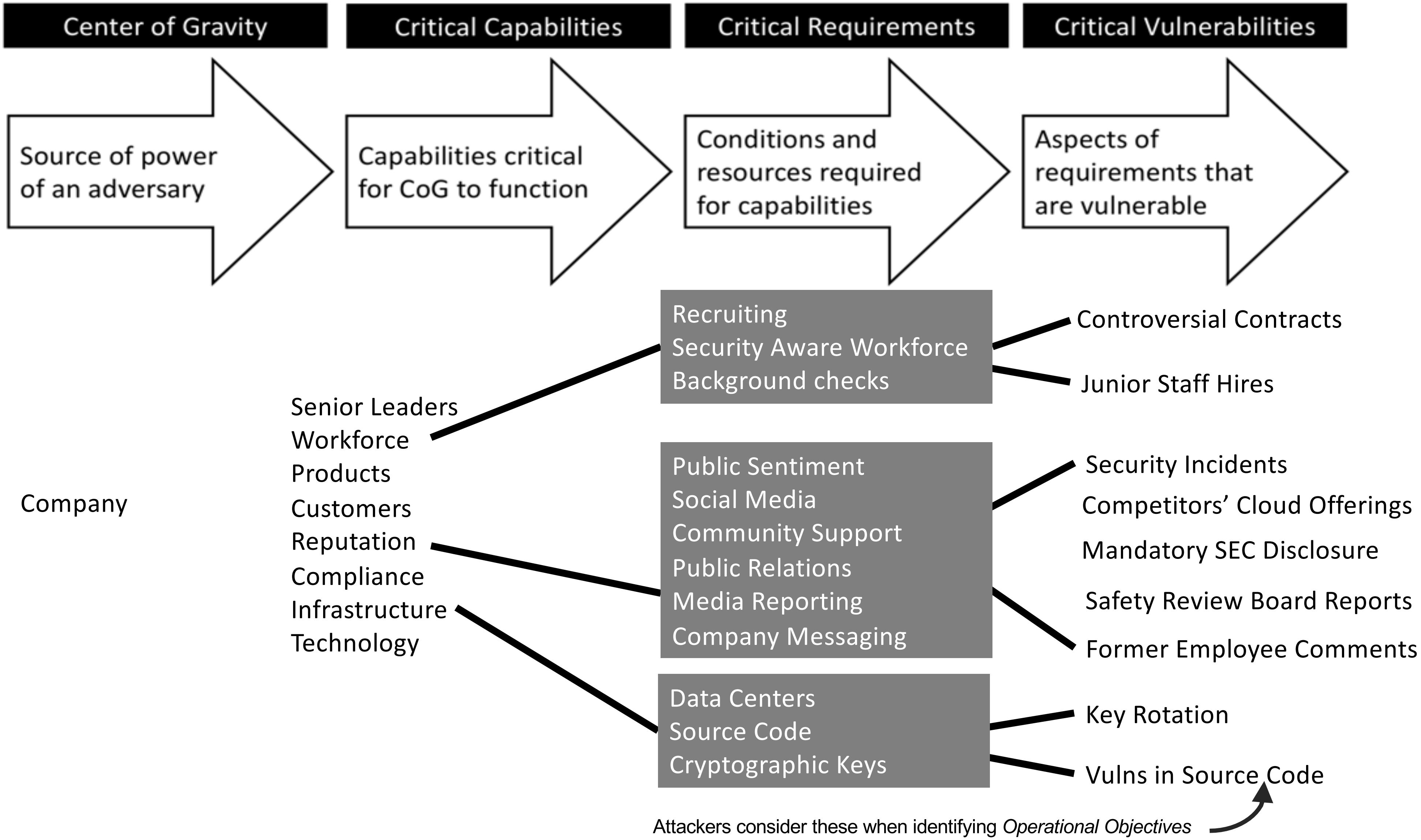
what those capabilities depend on to exist or operate

requirements that are fragile, exposed, or exploitable

Yields a structured understanding of what sustains an actor's ability to operate and where it is vulnerable.

- High value and high payoff targets
- Points where pressure could force choice or tradeoffs
- Friendly opportunities for leverage

See also, Rock Stevens - The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level, USENIX Security



Center of Gravity

Source of power of an adversary

Critical Capabilities

Capabilities critical for CoG to function

Critical Requirements

Conditions and resources required for capabilities

Critical Vulnerabilities

Aspects of requirements that are vulnerable

Company

Senior Leaders
Workforce
Products
Customers
Reputation
Compliance
Infrastructure
Technology

Recruiting
Security Aware Workforce
Background checks

Public Sentiment
Social Media
Community Support
Public Relations
Media Reporting
Company Messaging

Data Centers
Source Code
Cryptographic Keys

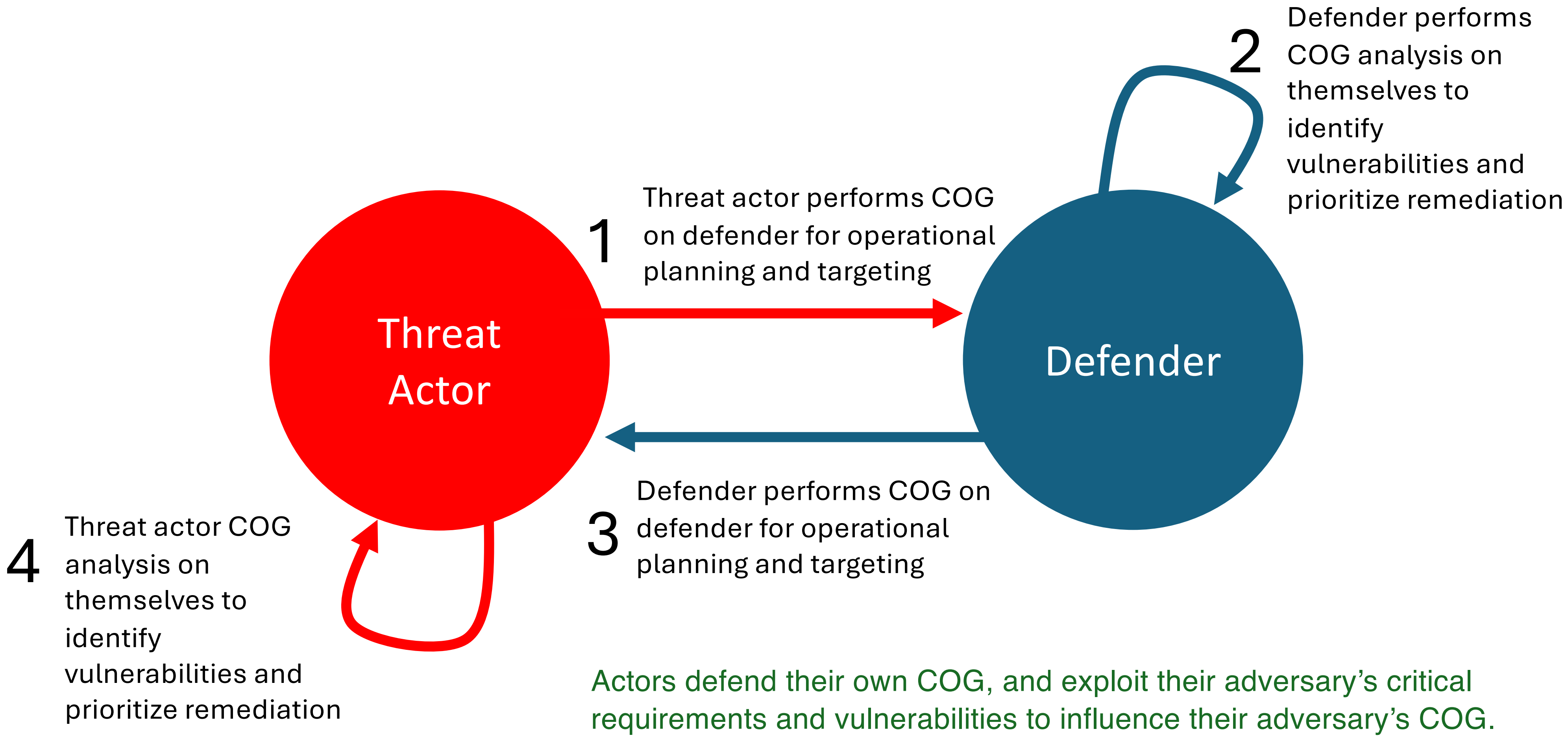
Controversial Contracts
Junior Staff Hires

Security Incidents
Competitors’ Cloud Offerings
Mandatory SEC Disclosure
Safety Review Board Reports
Former Employee Comments

Key Rotation
Vulns in Source Code

Attackers consider these when identifying *Operational Objectives*

COG Applications



1 Threat actor performs COG on defender for operational planning and targeting

2 Defender performs COG analysis on themselves to identify vulnerabilities and prioritize remediation

3 Defender performs COG on defender for operational planning and targeting

4 Threat actor COG analysis on themselves to identify vulnerabilities and prioritize remediation

Actors defend their own COG, and exploit their adversary’s critical requirements and vulnerabilities to influence their adversary’s COG.

Choose your COG

Brand dominance and market reputation (LockBit)

BlackCat / ALPHV – Candidate COGs

Technical Sophistication and Tooling Architecture
BlackCat's Rust-based ransomware and technical differentiation support its reputation.

Affiliate Ecosystem
Like others, its RaaS structure sustains reach and attack volume.

Reputation and Public Signaling
Public attribution, retaliation, and branding reinforce coercive leverage.

Core Leadership and Strategic Direction
Central coordination shapes targeting, messaging, and adaptation.

LockBit – Candidate COGs

Ransomware-as-a-Service Platform
LockBit's scalable affiliate model is central to its operational power.

Brand Dominance and Market Reputation
LockBit cultivated a strong brand identity to attract affiliates and pressure victims.

Leadership Stability and Adaptability
LockBit has shown resilience and rapid reconstitution after law enforcement disruption.

Automated Tooling and Operational Efficiency
Technical refinement and process maturity sustain speed and scale.

Conti – Candidate COGs

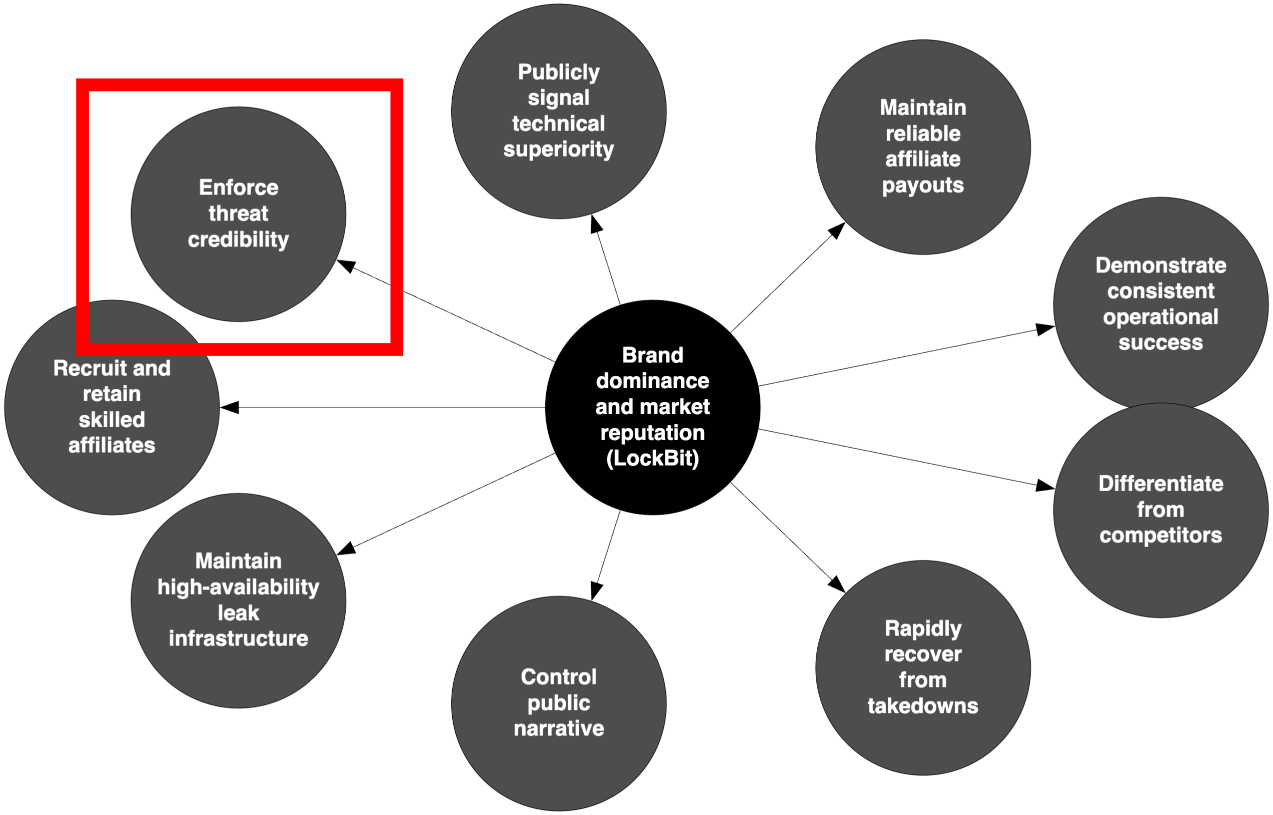
Centralized Leadership and Management Core
Conti exhibited strong internal leadership and structured management, especially revealed through the Conti leaks.

Affiliate Network and Operational Workforce
The group's ability to recruit, manage, and incentivize affiliates under a RaaS model sustained operations.

Brand Reputation and Negotiation Credibility
Conti's public presence, leak site, and retaliation behavior reinforced coercive leverage.

Internal Coordination Infrastructure
Communication platforms, tooling, and training materials enabled disciplined operations.

Develop Critical Capabilities (CCs) Required to sustain the selected COG


Brand dominance and market reputation (LockBit)
Publicly signal technical superiority
Maintain reliable affiliate payouts
Enforce threat credibility
Demonstrate consistent operational success
Recruit and retain skilled affiliates
Differentiate from competitors
Maintain high-availability leak infrastructure
Control public narrative
Rapidly recover from takedowns

These CCs sustain actor's ability to function as a dominant and trusted brand within the ransomware ecosystem.

COG: Brand dominance and market reputation

CC1 - Demonstrate Consistent Operational Success
Regularly compromise high-profile victims and publish proof.

CC2 - Maintain Reliable Affiliate Payouts
Honor revenue-sharing agreements to reinforce trust within the ecosystem.

CC3 - Publicly Signal Technical Superiority
Market tooling speed, automation, and innovation.

CC4 - Enforce Threat Credibility
Consistently leak data or escalate when ransoms are not paid.

CC5 - Recruit and Retain Skilled Affiliates
Attract capable operators who amplify brand visibility.

CC6 - Maintain High-Availability Leak Infrastructure
Ensure public-facing sites remain accessible and visible.

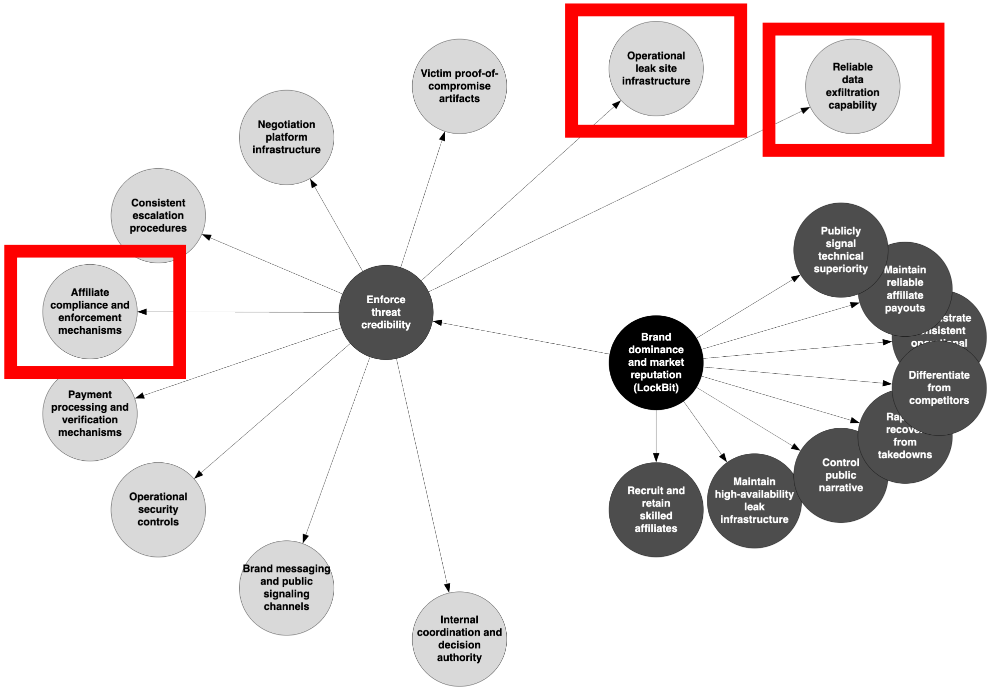
CC7 - Control Public Narrative
Shape messaging around law enforcement actions, breaches, and disruptions.

CC8 - Rapidly Recover From Takedowns
Reconstitute infrastructure and brand presence after disruption.

CC9 - Differentiate From Competitors
Promote distinctive features or policies to stand out in the RaaS marketplace.

COG → CCs → CRs → CVs

Critical Requirements (CRs) of Enforce Threat Credibility


Operational leak site infrastructure
Reliable data exfiltration capability
Victim proof-of-compromise artifacts
Negotiation platform infrastructure
Consistent escalation procedures
Affiliate compliance and enforcement mechanisms
Enforce threat credibility
Payment processing and verification mechanisms
Operational security controls
Brand messaging and public signaling channels
Internal coordination and decision authority
Brand dominance and market reputation (LockBit)
Publicly signal technical superiority
Maintain reliable affiliate payouts
strate nsistent
Differentiate from competitors
Rap recove from takedowns
Control public narrative
Maintain high-availability leak infrastructure
Recruit and retain skilled affiliates

Candidate CRs that must exist for actor to enforce threat credibility

COG: Brand dominance and market reputation
CC4: Enforce threat credibility

CR1 - Reliable Data Exfiltration Capability
The ability to extract sensitive data before encryption to enable double extortion.

CR2- Operational Leak Site Infrastructure
Hosting, maintaining, and defending public-facing leak portals.

CR3- Victim Proof-of-Compromise Artifacts
Ability to publish screenshots, sample files, or internal documents as evidence.

CR4 - Negotiation Platform Infrastructure
Secure victim communication portals for ransom negotiation.

CR5 - Consistent Escalation Procedures
Defined timelines and processes for publishing data when payment is refused.

CR6 - Affiliate Compliance and Enforcement
Mechanisms to ensure affiliates follow through on publication and don't privately settle.

CR7 - Payment Processing and Verification Mechanisms
Cryptocurrency wallets, escrow logic, and confirmation workflows.

CR8 - Operational Security Controls
Infrastructure obfuscation, anonymity, and counter–law enforcement protections.

CR9 - Brand Messaging and Public Signaling Channels
Forums, statements, or retaliatory messaging reinforcing seriousness.

CR10 - Internal Coordination and Decision Authority
Leadership oversight to approve leaks, escalations, and public messaging.

COG → CCs → CRs → CVs

Critical Vulnerabilities (CVs) of Reliable Data Exfiltration, Leak Site Infrastructure, Affiliate Compliance and Enforcement

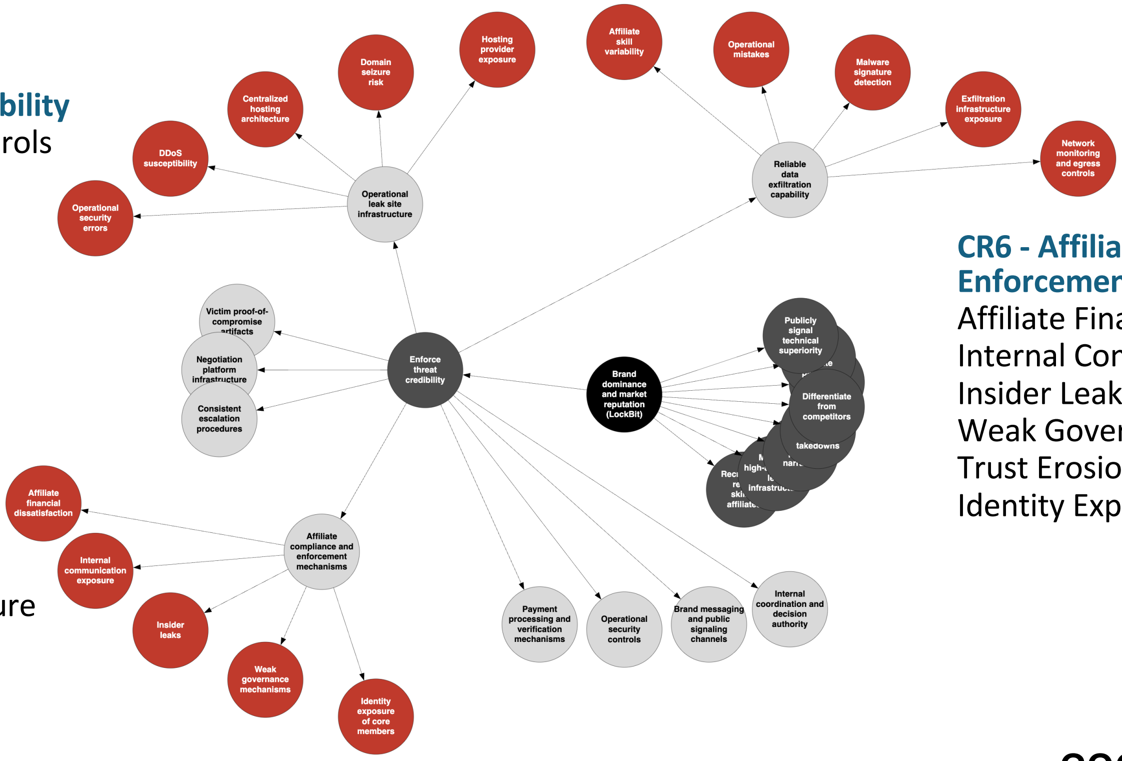
COG: Brand dominance and market reputation
CC4: Enforce threat credibility

CR1 - Reliable Data Exfiltration Capability

Network Monitoring and Egress Controls
Encryption Key Mismanagement
Exfiltration Infrastructure Exposure
Malware Signature Detection
Operational Mistakes
Affiliate Skill Variability

CR2 - Operational Leak Site Infrastructure

Hosting Provider Exposure
Domain Seizure Risk
Centralized Hosting Architecture
DDoS Susceptibility
Operational Security Errors
Payment Traceability


Hosting provider exposure
Affiliate skill variability
Operational mistakes
Domain seizure risk
Malware signature detection
Centralized hosting architecture
Exfiltration infrastructure exposure
DDoS susceptibility
Network monitoring and egress controls
Reliable data exfiltration capability
Operational leak site infrastructure
Operational security errors
Victim proof-of-compromise artifacts
Publicly signal technical superiority
Negotiation platform infrastructure
Enforce threat credibility
Brand dominance and market reputation (LockBit)
Differentiate from competitors
Consistent escalation procedures
takedowns
Affiliate financial dissatisfaction
Affiliate compliance and enforcement mechanisms
Internal communication exposure
Insider leaks
Internal coordination and decision authority
Payment processing and verification mechanisms
Operational security controls
Brand messaging and public signaling channels
Weak governance mechanisms
Identity exposure of core members

CR6 - Affiliate Compliance and Enforcement

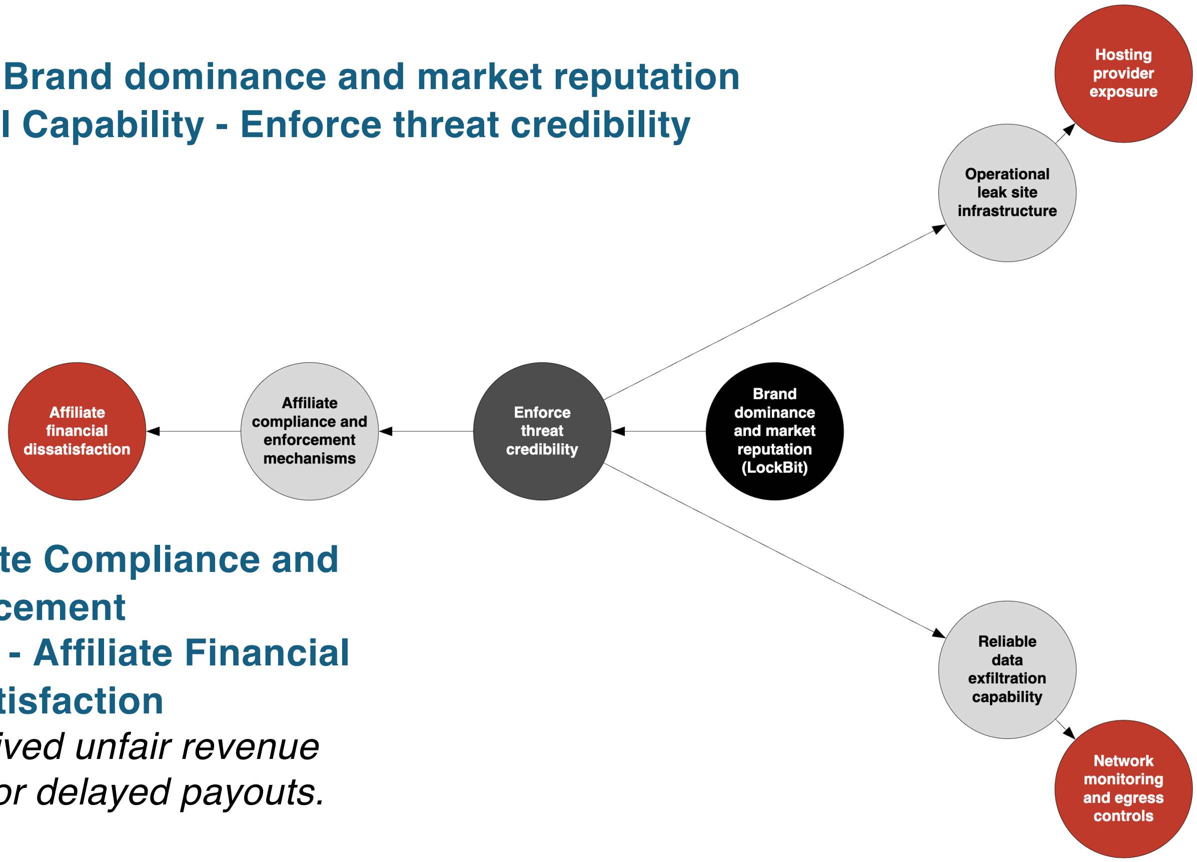
Affiliate Financial Dissatisfaction
Internal Communication Exposure
Insider Leaks
Weak Governance Mechanisms
Trust Erosion After LE Disruption
Identity Exposure of Core Members

COG → CCs → CRs → CVs

Okay, the graph is starting to get big let’s prune it to three CVs

COG - Brand dominance and market reputation
Critical Capability - Enforce threat credibility

Operational Leak Site Infrastructure
CV2.1 - Hosting Provider Exposure
Dependence on identifiable infrastructure providers vulnerable to legal pressure or seizure.
…


Hosting provider exposure
Operational leak site infrastructure
Affiliate financial dissatisfaction
Affiliate compliance and enforcement mechanisms
Enforce threat credibility
Brand dominance and market reputation (LockBit)
Reliable data exfiltration capability
Network monitoring and egress controls

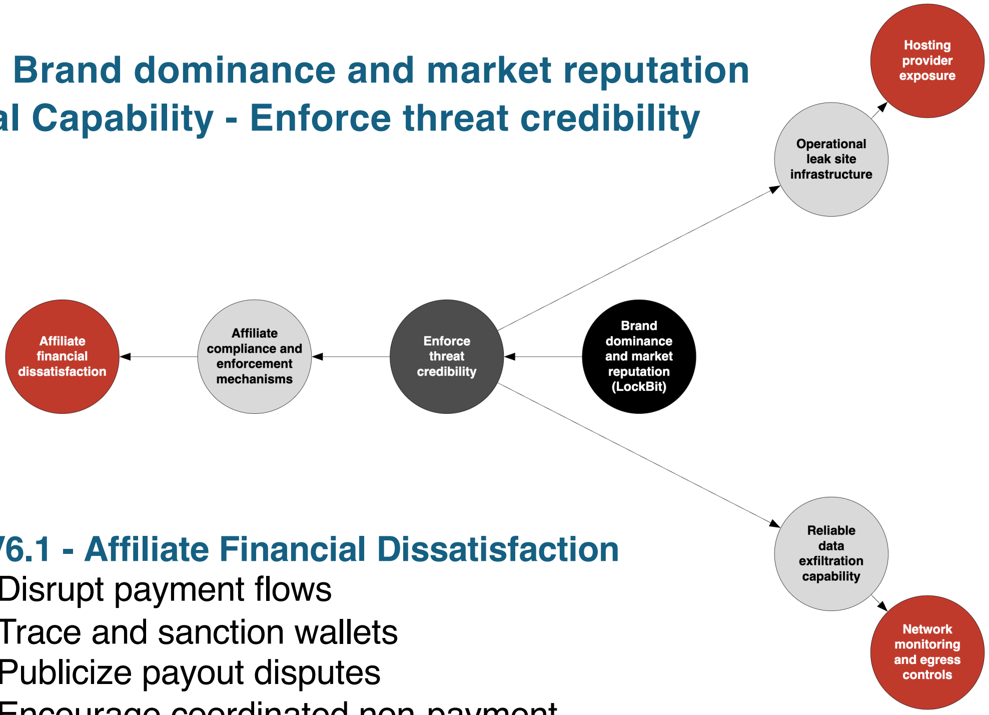
Reliable Data Exfiltration Capability
CV1.1 - Network Monitoring and Egress Controls
Strong DLP or traffic anomaly detection blocking exfiltration.
…

Affiliate Compliance and Enforcement
CV6.1 - Affiliate Financial Dissatisfaction
Perceived unfair revenue splits or delayed payouts.
…

COG → CCs → CRs → CVs

Add Actions that Target those Vulnerabilities

COG - Brand dominance and market reputation
Critical Capability - Enforce threat credibility


Hosting provider exposure
Operational leak site infrastructure
Affiliate financial dissatisfaction
Affiliate compliance and enforcement mechanisms
Enforce threat credibility
Brand dominance and market reputation (LockBit)
Reliable data exfiltration capability
Network monitoring and egress controls

CV2.1 - Hosting Provider Exposure

Targets / Actions:

1. Coordinate hosting takedowns
2. Registrar cooperation and domain seizure
3. Sinkhole or seize exposed infrastructure
4. Collective DDoS pressure
5. Exploit OPSEC mistakes for attribution

Intended effect:

Decision Point: Should operators rebuild, relocate or suspend leak site infrastructure?

CV1.1 - Network Monitoring and Egress Controls

1. Harden outbound inspection and DLP
2. Share behavioral detection analytics
3. Identify and seize cloud drop servers
4. Publicize failed exfiltration attempts
5. Increase operational friction

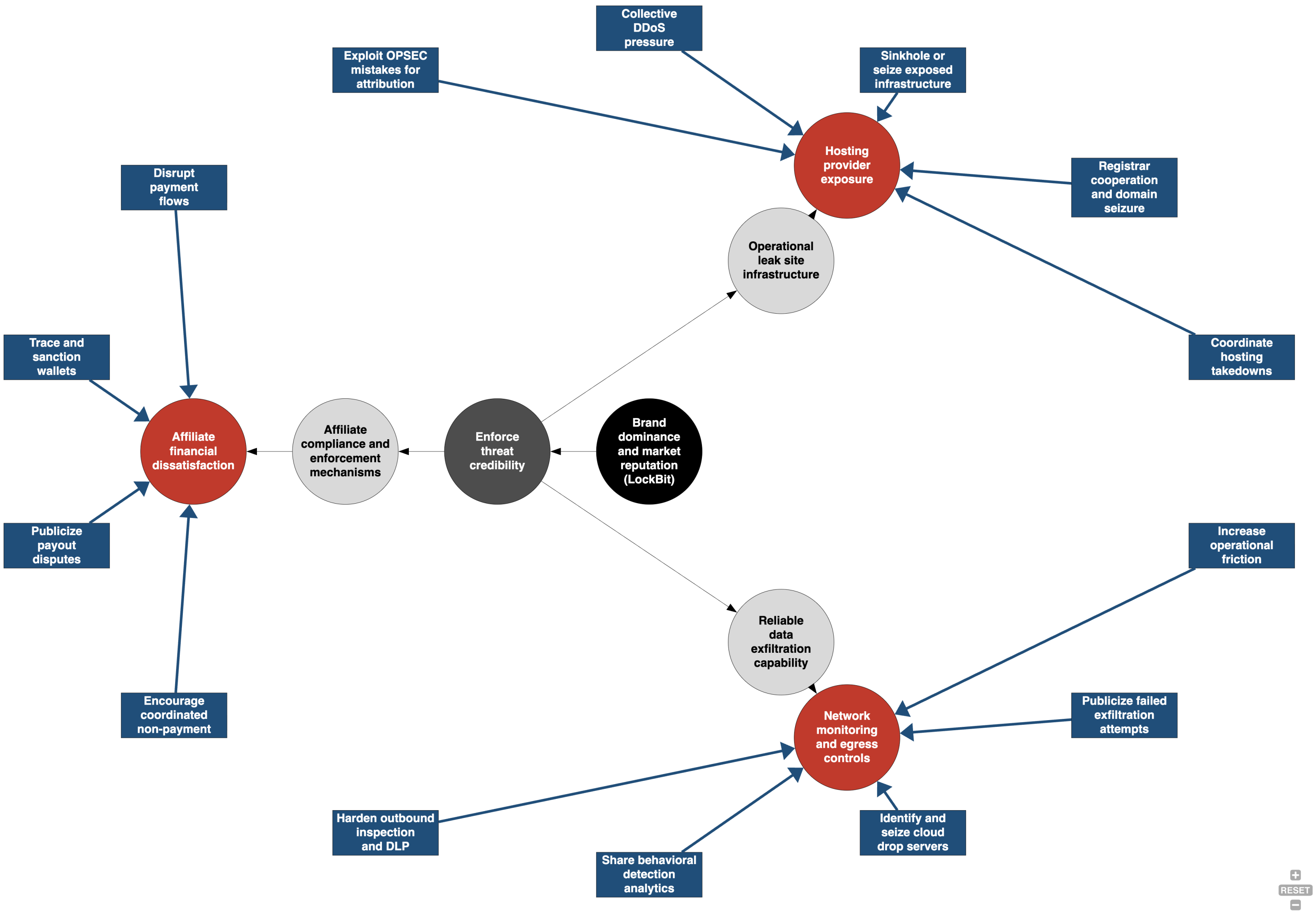
Decision Point: Should the operators continue relying on double extortion tactics or shift to alternative pressure mechanisms?

CV6.1 - Affiliate Financial Dissatisfaction

1. Disrupt payment flows
2. Trace and sanction wallets
3. Publicize payout disputes
4. Encourage coordinated non-payment

Decision Point: Should affiliates continue operating under the LockBit platform or migrate to another ransomware operation?

COG → CCs → CRs → CVs



Brand dominance and market reputation (LockBit)

Enforce threat credibility

Affiliate compliance and enforcement mechanisms

Operational leak site infrastructure

Reliable data exfiltration capability

Affiliate financial dissatisfaction

Hosting provider exposure

Network monitoring and egress controls

Disrupt payment flows

Trace and sanction wallets

Publicize payout disputes

Encourage coordinated non-payment

Exploit OPSEC mistakes for attribution

Collective DDoS pressure

Sinkhole or seize exposed infrastructure

Registrar cooperation and domain seizure

Coordinate hosting takedowns

Increase operational friction

Publicize failed exfiltration attempts

Harden outbound inspection and DLP

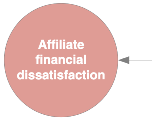
Share behavioral detection analytics

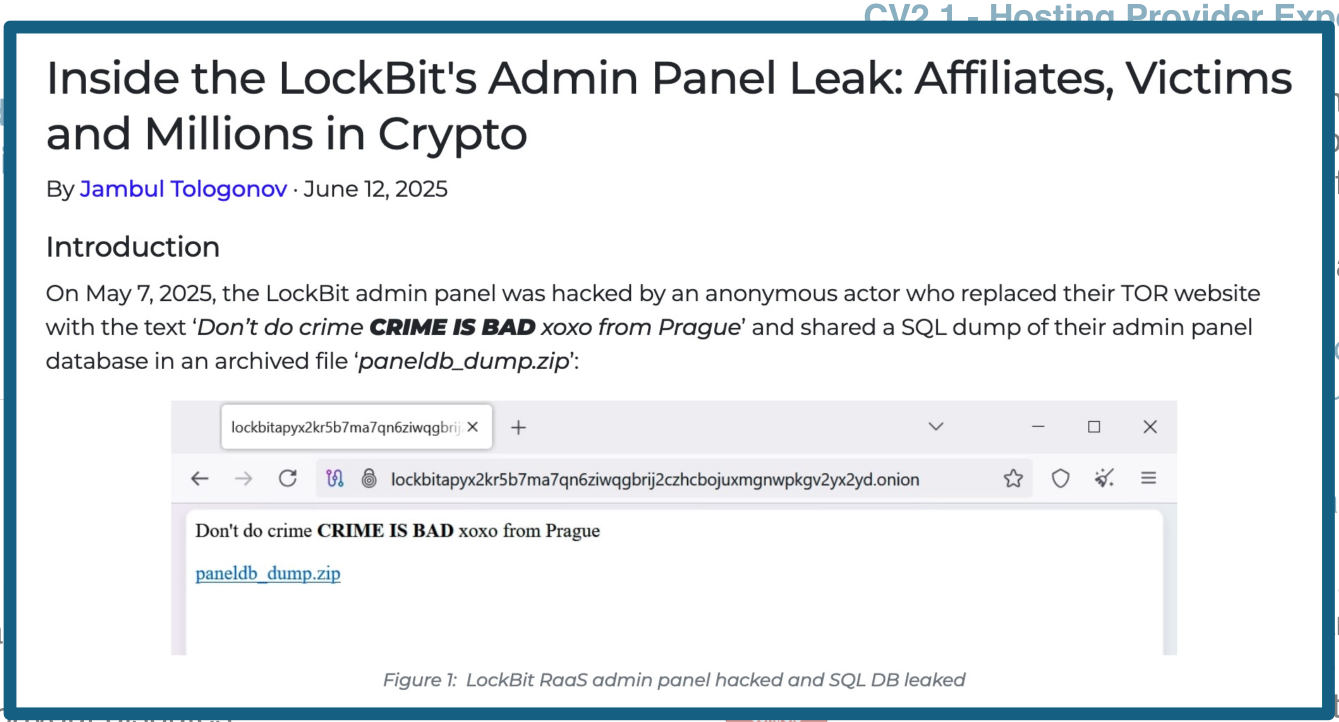
Identify and seize cloud drop servers

COG → CCs → CRs → CVs ← Targeting the vulnerabilities

Add Actions that Target those Vulnerabilities

COG - Brand d
Critical Capabi





Inside the LockBit's Admin Panel Leak: Affiliates, Victims and Millions in Crypto

By Jambul Tologonov · June 12, 2025

Introduction

On May 7, 2025, the LockBit admin panel was hacked by an anonymous actor who replaced their TOR website with the text '*Don't do crime **CRIME IS BAD** xoxo from Prague*' and shared a SQL dump of their admin panel database in an archived file '*paneldb_dump.zip*':

lockbitapyx2kr5b7ma7qn6ziwqgbrij
lockbitapyx2kr5b7ma7qn6ziwqgbrij2czhcbojuxmgnwpkgv2yx2yd.onion

Don't do crime **CRIME IS BAD** xoxo from Prague

paneldb_dump.zip

Figure 1: LockBit RaaS admin panel hacked and SQL DB leaked

CV6.1 - Affil
1. Disrupt pa
2. Trace and
3. Publicize payout disputes
4. Encourage coordinated non-payment

Decision Point: Should affiliates continue operating under the LockBit platform or migrate to another ransomware operation?

CV2.1 - Hosting Provider Exposure

ns
omain seizure
frastructure

attribution

ors rebuild, relocate
ure?

nd Egress

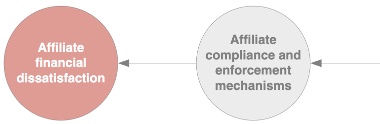
and DLP
nalytics
servers
tempts
5. Increase operational friction

Decision Point: Should the operators continue relying on double extortion tactics or shift to alternative pressure mechanisms?

COG → CCs → CRs → CVs

Add Actions that Target those Vulnerabilities

COG - Brand dominance ar
Critical Capability - Enforce


Affiliate financial dissatisfaction
Affiliate compliance and enforcement mechanisms

CV6.1 - Affiliate Financial
1. Disrupt payment flows
2. Trace and sanction wallet
3. Publicize payout disputes
4. Encourage coordinated n

Decision Point: Should affi continue operating under the LockBit platform or migrate to another ransomware operation?

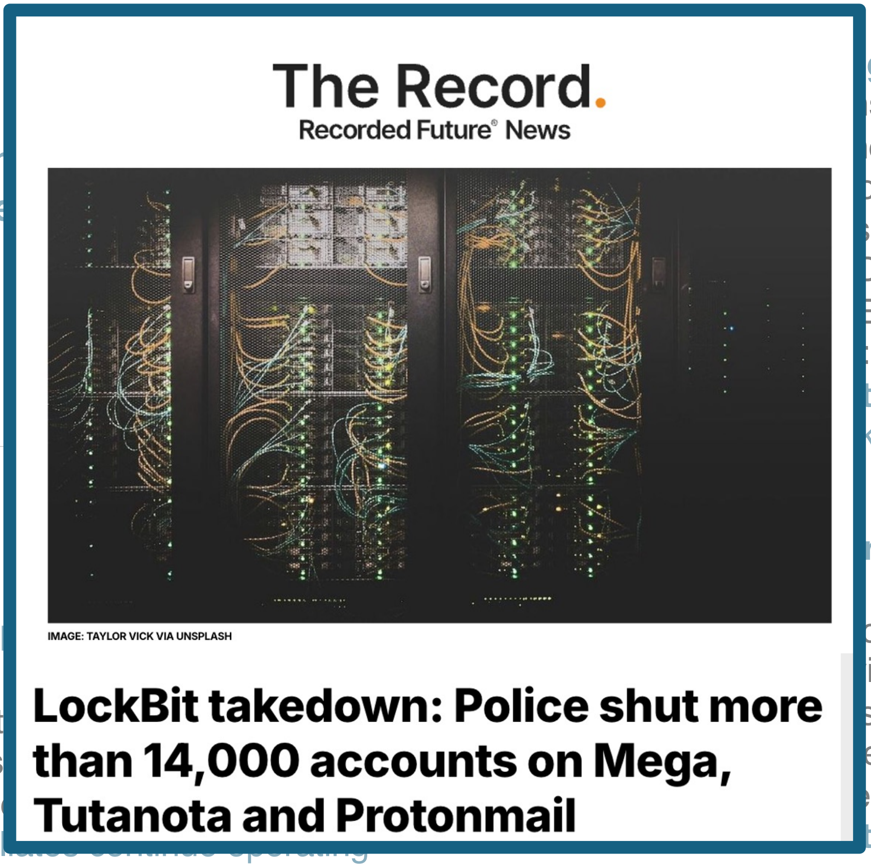

The Record.
Recorded Future® News

IMAGE: TAYLOR VICK VIA UNSPLASH

LockBit takedown: Police shut more than 14,000 accounts on Mega, Tutanota and Protonmail

g Provider Exposure
s:
osting takedowns
operation and domain seizure
seize exposed infrastructure
DoS pressure
EC mistakes for attribution
:
t: Should operators rebuild, relocate
k site infrastructure?

rk Monitoring and Egress

ound inspection and DLP
ioral detection analytics
seize cloud drop servers
ed exfiltration attempts
erational friction
t: Should the operators continue relying on double extortion tactics or shift to alternative pressure mechanisms?

COG → CCs → CRs → CVs

Comparing Military COG and Infosec

In military COG doctrine, targets are selected because they exploit critical vulnerabilities tied to the center of gravity.

In infosec, vulnerabilities are selected because exploiting them produces decisive operational effects.

Structurally, they are equivalent, but not every vulnerability is strategically critical.

COG thinking filters adversary weaknesses by their impact on what actually sustains power.

COG-informed security reframes the question:
Not "Where are the vulnerabilities?"
But "Which vulnerabilities, if exploited, collapse what actually matters?"

We only explored ~3% of the potential vulnerability space (14/450)

Future work: explore shared dependencies e.g. a critical vulnerability may undermine multiple critical requirements

Mitigations the **threat actor** could employ

Affiliate financial dissatisfaction

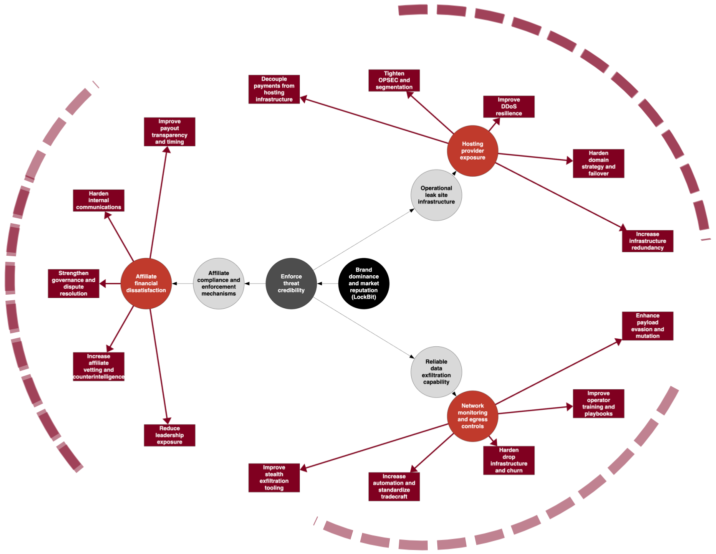
Improve Revenue Transparency
Provide reliable dashboards for affiliate payouts. Ensure timely, predictable revenue distribution.

Strengthen Internal Communications Security
Move to hardened, private communication platforms. Enforce compartmentalization.

Increase Governance Discipline
Formalize rules for enforcement escalation. Implement clearer dispute resolution processes.

Strengthen Counterintelligence
Vet affiliates more aggressively. Monitor for insider threat indicators.

Reduce Leadership Exposure
Further anonymize core operators. Rotate public-facing handles. Reduce centralized decision visibility.



Brand dominance and market reputation (LockBit)
Enforce threat credibility
Affiliate compliance and enforcement mechanisms
Affiliate financial dissatisfaction
Improve payout transparency and timing
Harden internal communications
Strengthen governance and dispute resolution
Increase affiliate vetting and counterintelligence
Reduce leadership exposure
Operational leak site infrastructure
Hosting provider exposure
Decouple payments from hosting infrastructure
Tighten OPSEC and segmentation
Improve DDoS resilience
Harden domain strategy and failover
Increase infrastructure redundancy
Reliable data exfiltration capability
Network monitoring and egress controls
Enhance payload evasion and mutation
Improve operator training and playbooks
Harden drop infrastructure and churn
Increase automation and standardize tradecraft
Improve stealth exfiltration tooling

Hosting provider exposure mitigations

Increase Infrastructure Redundancy
Deploy distributed, multi-jurisdiction hosting. Use layered reverse proxies and rotating infrastructure.

Harden Domain Strategy
Pre-register backup domains. Use automated failover between onion services and clearnet mirrors.

Improve DDoS Resilience
Use distributed hosting and traffic scrubbing services. Maintain rapid redeployment playbooks.

Tighten OPSEC
Separate infrastructure management identities. Improve metadata hygiene. Conduct internal OPSEC audits.

Decouple Payment Infrastructure
Avoid wallet-hosting correlation. Rotate wallet clusters more aggressively.

Network monitoring and egress control mitigations

Improve Exfiltration Tooling
Encrypt and fragment outbound traffic.
Blend exfiltration with legitimate protocols.

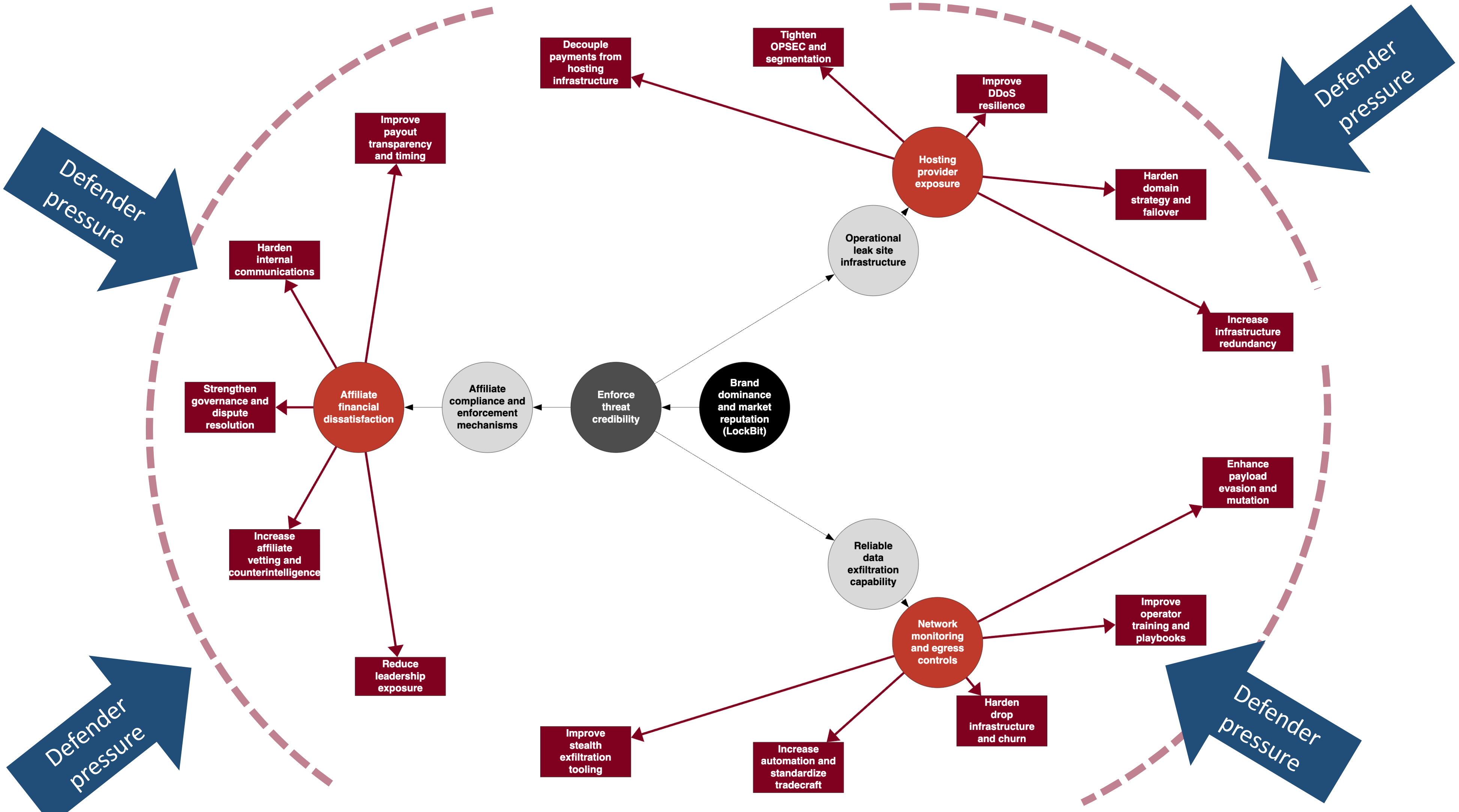
Increase Automation
Reduce affiliate execution variability with standardized tooling.

Harden Drop Infrastructure
Use short-lived cloud storage accounts. Increase infrastructure churn rate.

Improve Operator Training
Provide playbooks for stealth exfiltration. Reduce operational mistakes through process standardization.

Enhance Malware Evasion
Frequent payload mutation. Behavioral evasion against EDR.

COG → CCs → CRs → CVs ← **Mitigate the vulnerabilities**



Brand dominance and market reputation (LockBit)

Enforce threat credibility

Affiliate compliance and enforcement mechanisms

Operational leak site infrastructure

Reliable data exfiltration capability

Affiliate financial dissatisfaction

Hosting provider exposure

Network monitoring and egress controls

Improve payout transparency and timing

Harden internal communications

Strengthen governance and dispute resolution

Increase affiliate vetting and counterintelligence

Reduce leadership exposure

Decouple payments from hosting infrastructure

Tighten OPSEC and segmentation

Improve DDoS resilience

Harden domain strategy and failover

Increase infrastructure redundancy

Enhance payload evasion and mutation

Improve operator training and playbooks

Harden drop infrastructure and churn

Increase automation and standardize tradecraft

Improve stealth exfiltration tooling

Defender pressure

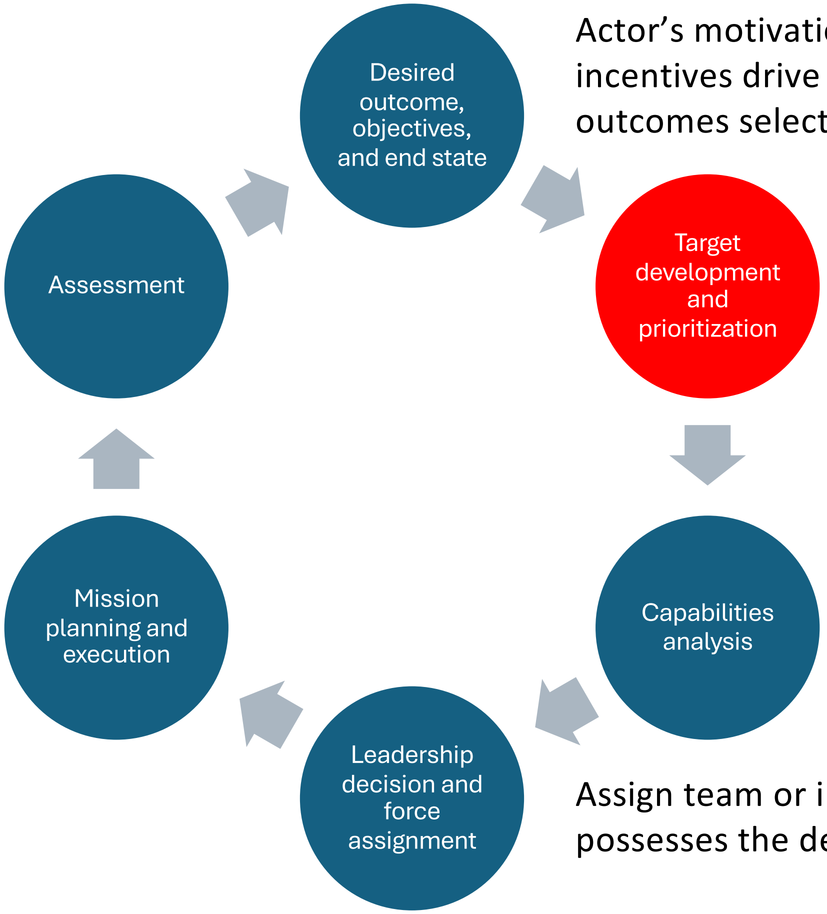
Defender pressure

Defender pressure

Defender pressure

COG → CCs → CRs → CVs ← Mitigate the vulnerabilities

COG reveals dependencies, targeting applies pressure



Desired outcome, objectives, and end state

Actor’s motivations and incentives drive desired outcomes selection

Target development and prioritization

Actor collects necessary intelligence, decides which entities to target and their priority

Capabilities analysis

Choose from existing capabilities. Actors can create desired capabilities, if necessary.

Leadership decision and force assignment

Assign team or individual which possesses the desired capability

Mission planning and execution

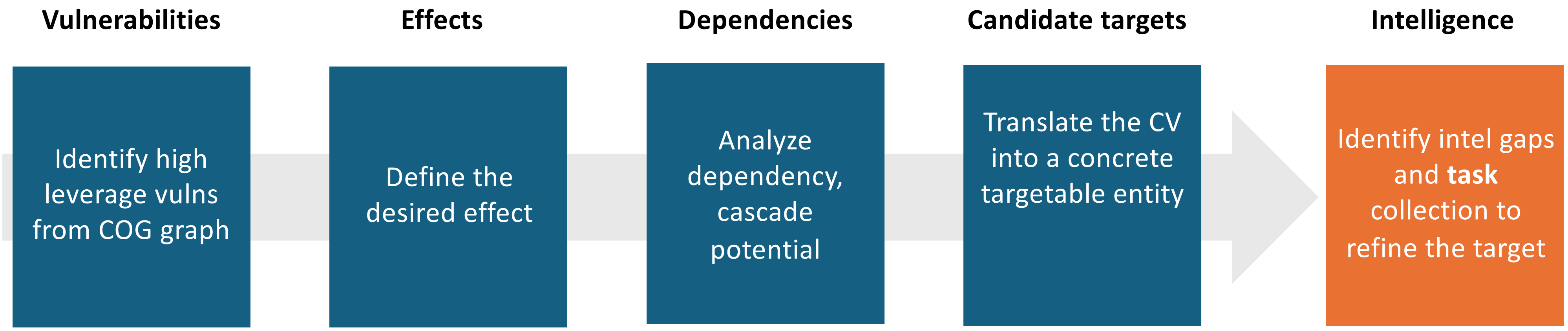
The kill chain happens here

Assessment

Were the desired effects and end state achieved?

Based on the Joint Targeting Cycle, see https://irp.fas.org/doddir/dod/jp3_09.pdf

From Critical Vulnerability to Target Intelligence



Vulnerabilities

Identify high leverage vulns from COG graph

Affiliate financial dissatisfaction undermines the CR “Affiliate compliance and enforcement mechanisms,” which undermines “Enforce threat credibility.”

Effects

Define the desired effect

Increase internal distrust, reduce affiliate willingness to deploy ransomware under the actor’s brand.

Dependencies

Analyze dependency, cascade potential

High cascade potential: affiliate dissatisfaction degrades compliance, weakens threat follow-through, and erodes brand dominance.

Candidate targets

Translate the CV into a concrete targetable entity

- *Cryptocurrency payout wallets*
- *Affiliate communication channels*
- *Public proof-of-payment claims*
- *Recruitment and promotion forums*

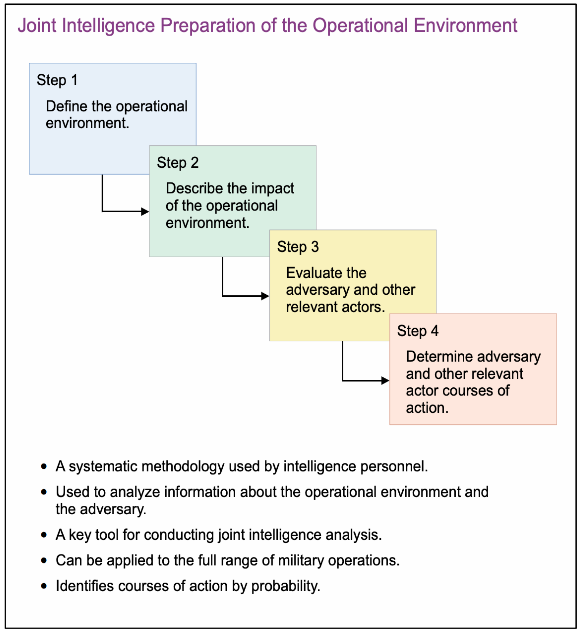
Intelligence

Identify intel gaps and **task** collection to refine the target

- *Map wallet clusters and payment flows*
- *Monitor affiliate complaints and dispute signals*
- *Track payout delays or inconsistencies*
- *Identify key affiliate influencers*

Planning and Execution

Intelligence



Joint Intelligence Preparation of the Operational Environment

Step 1
Define the operational environment.

Step 2
Describe the impact of the operational environment.

Step 3
Evaluate the adversary and other relevant actors.

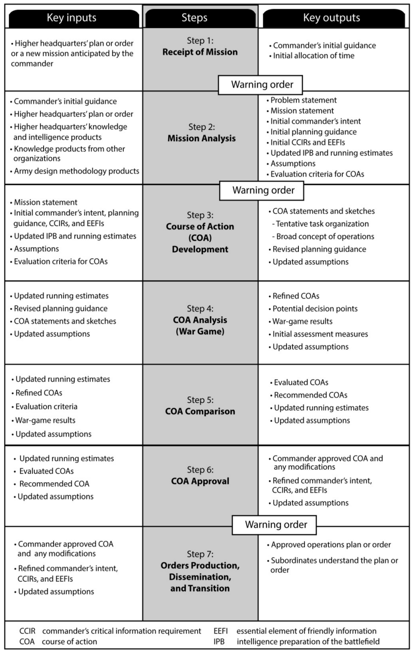
Step 4
Determine adversary and other relevant actor courses of action.

- A systematic methodology used by intelligence personnel.
- Used to analyze information about the operational environment and the adversary.
- A key tool for conducting joint intelligence analysis.
- Can be applied to the full range of military operations.
- Identifies courses of action by probability.

Figure I-5. Joint Intelligence Preparation of the Operational Environment

[Joint Intelligence Preparation of the Operational Environment (JIPOE)]

Operations



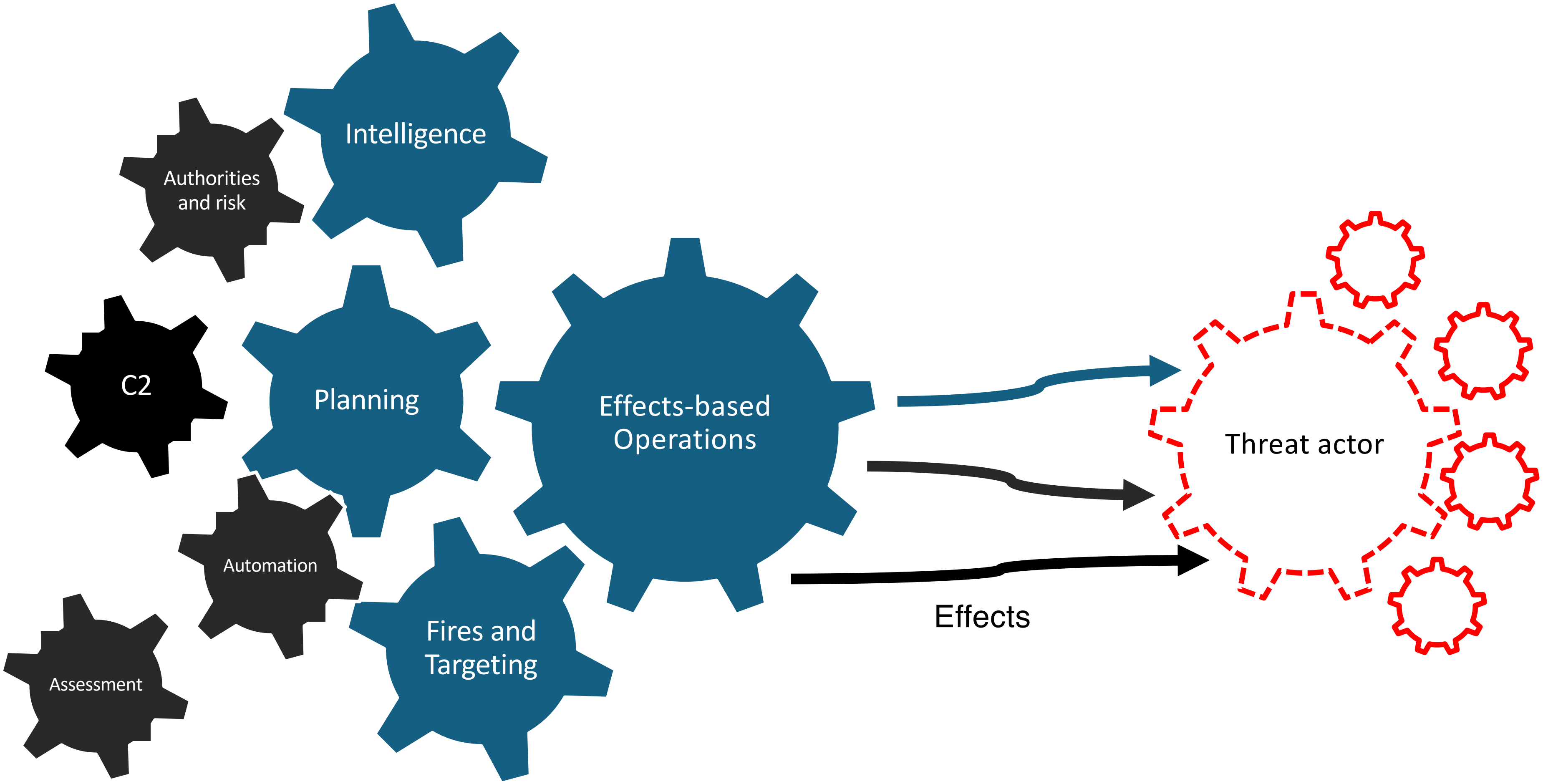
Key inputs	Steps	Key outputs
• Higher headquarters' plan or order or a new mission anticipated by the commander	Step 1: **Receipt of Mission**	• Commander's initial guidance • Initial allocation of time
		Warning order
• Commander's initial guidance • Higher headquarters' plan or order • Higher headquarters' knowledge and intelligence products • Knowledge products from other organizations • Army design methodology products	Step 2: **Mission Analysis**	• Problem statement • Mission statement • Initial commander's intent • Initial planning guidance • Initial CCIRs and EEFIs • Updated IPB and running estimates • Assumptions • Evaluation criteria for COAs
		Warning order
• Mission statement • Initial commander's intent, planning guidance, CCIRs, and EEFIs • Updated IPB and running estimates • Assumptions • Evaluation criteria for COAs	Step 3: **Course of Action (COA) Development**	• COA statements and sketches - Tentative task organization - Broad concept of operations • Revised planning guidance • Updated assumptions
• Updated running estimates • Revised planning guidance • COA statements and sketches • Updated assumptions	Step 4: **COA Analysis (War Game)**	• Refined COAs • Potential decision points • War-game results • Initial assessment measures • Updated assumptions
• Updated running estimates • Refined COAs • Evaluation criteria • War-game results • Updated assumptions	Step 5: **COA Comparison**	• Evaluated COAs • Recommended COAs • Updated running estimates • Updated assumptions
• Updated running estimates • Evaluated COAs • Recommended COA • Updated assumptions	Step 6: **COA Approval**	• Commander approved COA and any modifications • Refined commander's intent, CCIRs, and EEFIs • Updated assumptions
		Warning order
• Commander approved COA and any modifications • Refined commander's intent, CCIRs, and EEFIs • Updated assumptions	Step 7: **Orders Production, Dissemination, and Transition**	• Approved operations plan or order • Subordinates understand the plan or order

CCIR commander's critical information requirement
COA course of action
EEFI essential element of friendly information
IPB intelligence preparation of the battlefield

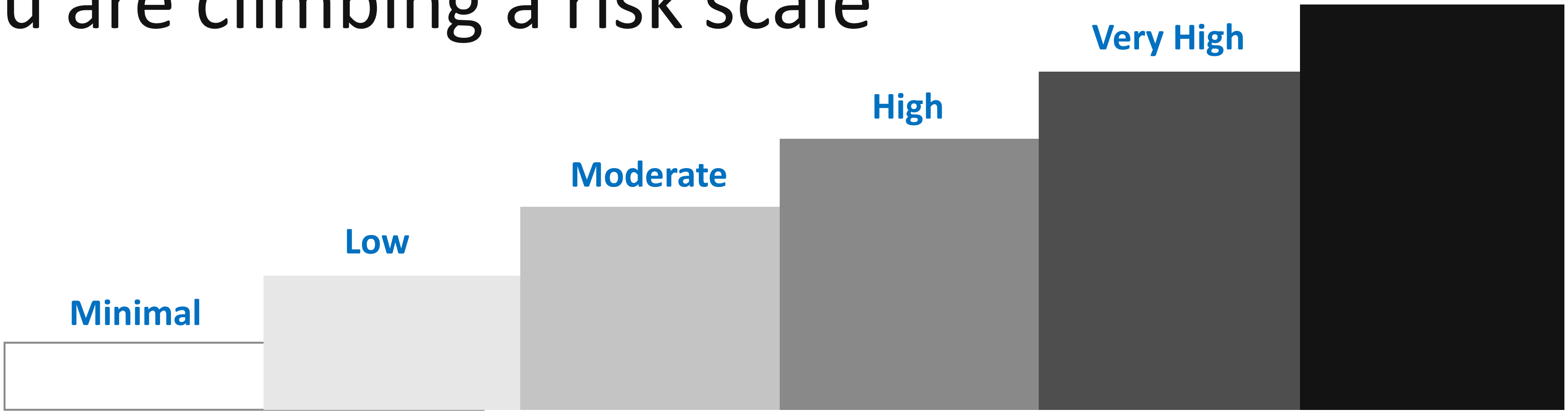
[Military Decision Making Process (MDMP)]

1. Receive the task or problem
2. Understand the mission and constraints
3. Develop viable courses of action
4. Analyze and wargame the options
5. Compare outcomes and tradeoffs
6. Decide and approve a course of action
7. Issue execution guidance

How can I put pressure on my adversary?



You are climbing a risk scale



Minimal	Low	Moderate	High	Very High	Extreme
Internal, reversible actions on own systems	Internal actions that touch external dependencies or partners	Targeted disruptions under clear authority	Coordinated multi-party operations with legal process	Public attribution with punitive actions	Strategic campaign imposing major costs on adversaries
Negligible external impact or visibility	Reversible and narrowly scoped	Limited public exposure	Sizable external impact	Cross-border complexity	High likelihood of escalation
	Minimal exposure	Some operational and reputational risk	Meaningful escalation risk	Significant political and collateral risk	Potentially irreversible effects

Risk: Becoming a Combatant

Two things that can make you a legitimate target in an armed conflict:

1. Hacking in support of a party to an armed conflict and to the detriment of an adversary

- Such activities, if conducted, must not target civilian, medical, or humanitarian infrastructure

2. Collecting militarily relevant information for a belligerent

- Could include?
  - Sharing photos of military activity with your government
  - Sharing cyber threat intelligence about military threat actors with your government

“**Civilianization of the Digital Battlefield**” is a serious global concern!

https://blogs.icrc.org/law-and-policy/2025/11/04/from-hackers-to-tech-companies-ihl-and-the-involvement-of-civilians-in-ict-activities-in-armed-conflict/

Example Risk Management TTPs

Governance and Planning

Structures and processes that guide decision-making

Governance playbooks

Multi-disciplinary planning teams

Risk assessments before action

Define escalation thresholds and stop conditions

Legal and Compliance

Anchoring operations in law, regulation, and policy

Route actions through lawful authorities

Use compliance frameworks as shields

Document decisions

Transfer risk through insurance

Allocate liability via contracts, partnerships, or outsourcing

Precision and Safeguards

Applying effects in a controlled and technically sound way

Apply precision in targeting

Separate EBO from production systems

Pre-mitigate retaliation risk

Test in sandboxes

Validate with red teams

Pre-mission rehearsals

Messaging and Attribution

Shaping perceptions through narrative

Frame actions as defensive

Maintain comms discipline

Use controlled ambiguity

Calibrate attribution and disclosure

Employ attribution deception if needed

Resilience and Intelligence

Maintaining continuity, adapting, and learning from operations

Monitor ops in real time

Preposition recovery resources

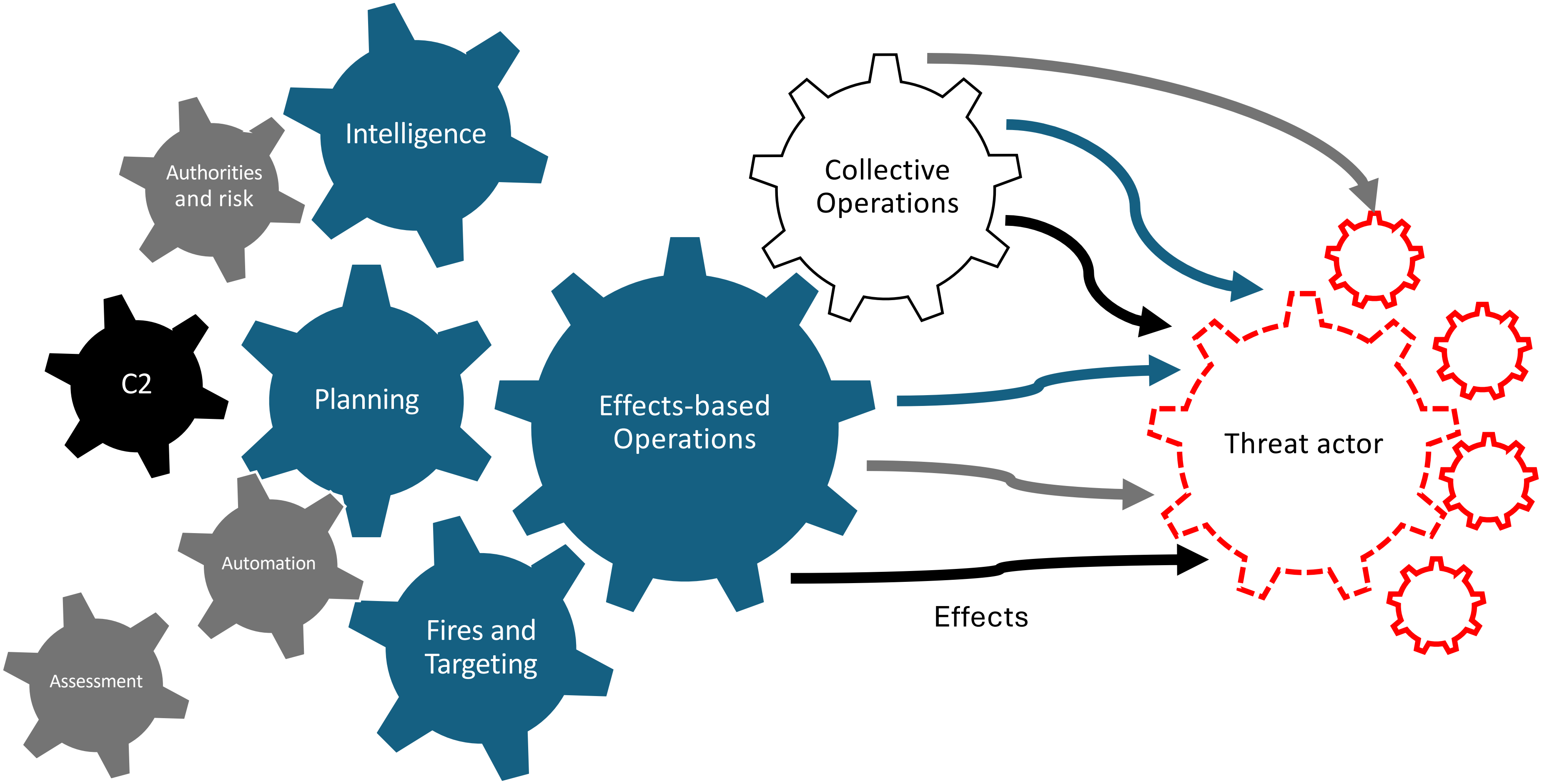
Assess intelligence gain/loss

Model adversaries

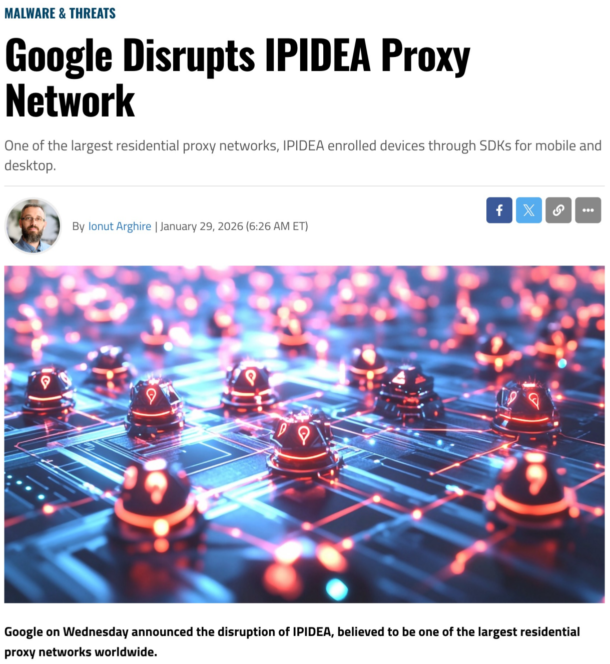
Leverage partnerships

Synchronize with allies

How can I put pressure on my adversary?



~~Collective Defense~~ Collective Operations



MALWARE & THREATS

Google Disrupts IPIDEA Proxy Network

One of the largest residential proxy networks, IPIDEA enrolled devices through SDKs for mobile and desktop.

By Ionut Arghire | January 29, 2026 (6:26 AM ET)

Google on Wednesday announced the disruption of IPIDEA, believed to be one of the largest residential proxy networks worldwide.

Collective operations are conducted by multiple organizations that share situational awareness and coordinate actions to align and reinforce effects.

Leverage collective's **capabilities, legal authorities**, and risk appetites

Share situational awareness to coordinate timing and pressure

Apply pressure beyond networks: infrastructure, money, identity, and narrative

Leverage partners to expand options and constrain adversaries

Applying Collective Pressure

Collective Operations can create **disproportionate payoff** but require coordination.

Collective operations can be **unexpected** because they:

- multiple targeted organizations can amplify pressure
- attack the campaign, not the incident
- ideally raise risk faster than attackers can adapt

Examples

Repeated infrastructure and hosting disruption
Payment-path friction through platforms and exchanges
Repeatedly degrading the market that supplies initial access
Coordinated identity and platform abuse reporting
Multi-victim disruption that breaks campaign tempo
Collective refusal signaling within a sector
Shared intelligence focused on campaign behavior
Coordinated disclosure timing to raise exposure risk
Law enforcement actions aligned to counter-campaign milestones

https://samuraiwr.com/movie/seven-samurai

Opportunity: Doctrinal Templates

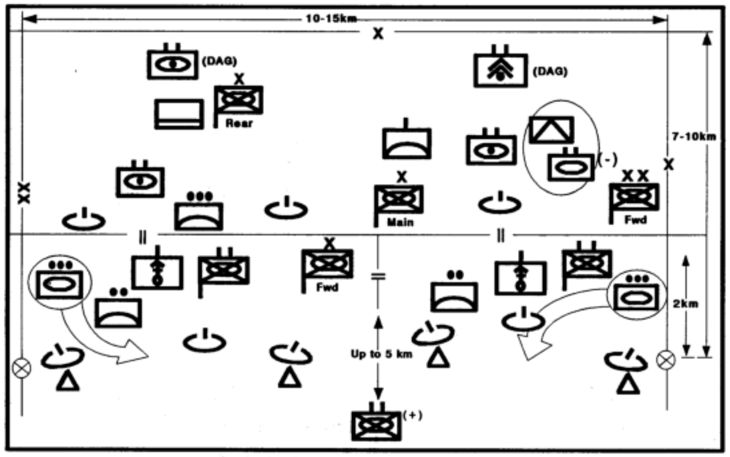
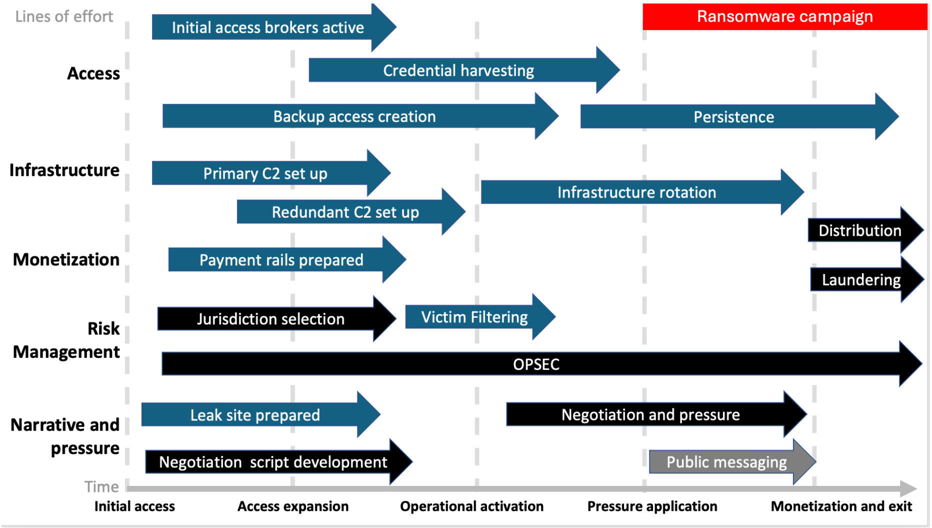


Figure 3-1-19. Doctrinal template for a defending brigade.



Lines of effort

Access

Initial access brokers active

Credential harvesting

Backup access creation

Persistence

Infrastructure

Primary C2 set up

Redundant C2 set up

Infrastructure rotation

Monetization

Payment rails prepared

Distribution

Laundering

Risk Management

Jurisdiction selection

Victim Filtering

OPSEC

Narrative and pressure

Leak site prepared

Negotiation script development

Negotiation and pressure

Public messaging

Ransomware campaign

Time

Initial access

Access expansion

Operational activation

Pressure application

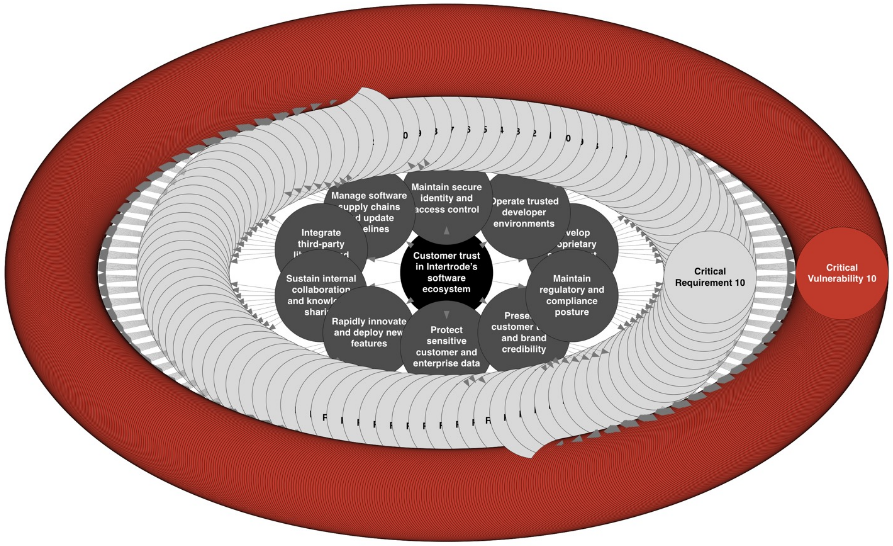
Monetization and exit

Doctrinal template
A baseline model of how an adversary typically organizes and conducts operations, used to anticipate behavior and identify leverage.

Doctrinal templates let us recognize campaigns, not just incidents.

At **high zoom**, the template shows campaign structure and intent.
At **medium zoom**, it shows LOOs, LOEs, and decision points.
At **low zoom**, it maps to kill chains, techniques, and tasks.

Opportunity: Continuous COG Analysis, at scale


Manage software supply chains d update elines
Maintain secure identity and access control
Operate trusted developer environments
Integrate third-party
velop oprietary
Customer trust in Intertrode's software ecosystem
Sustain internal collaboration and knowl shari
Maintain regulatory and compliance posture
Rapidly innovate and deploy new features
Protect sensitive customer and enterprise data
Prese customer and brand credibility
Critical Requirement 10
Critical Vulnerability 10

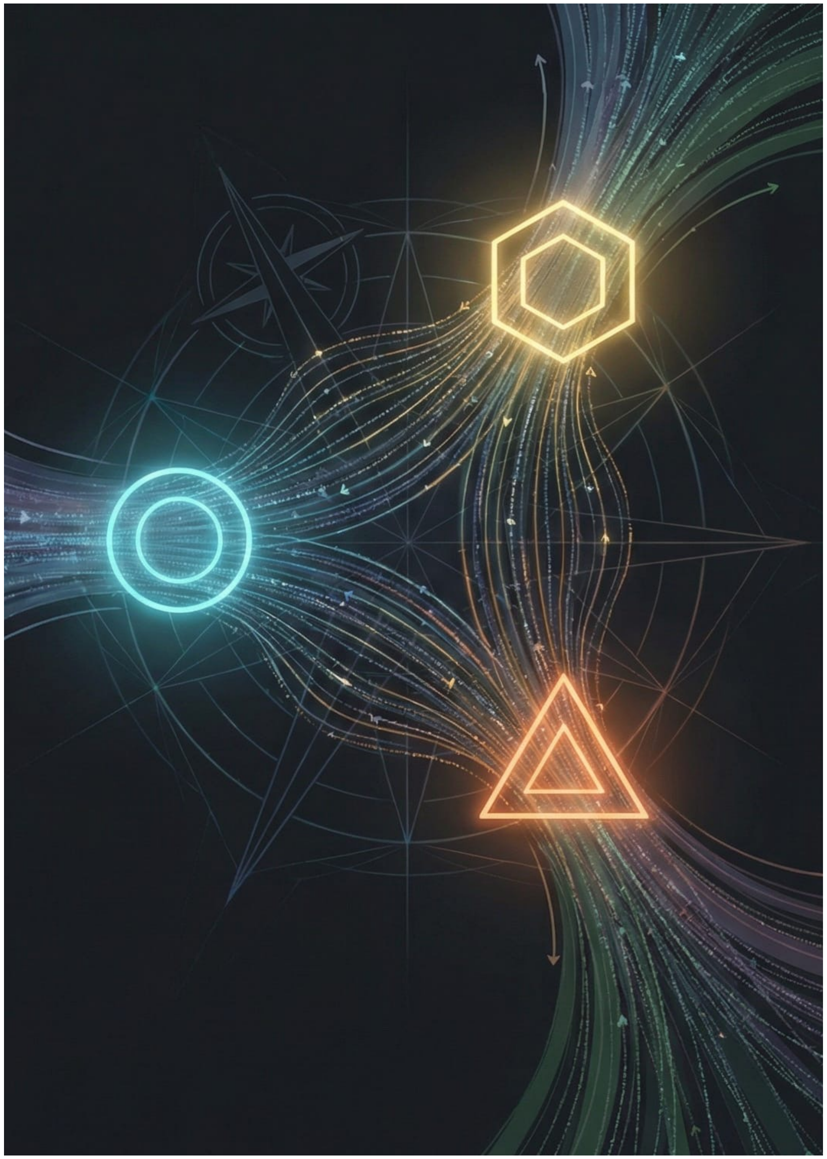
COG Node = 1
Critical Capabilities =10
Critical Requirements = 10^2
Critical vulnerabilities = 10^3
Total 1111 nodes / 1110 edges

At scale, visualizations quickly become **analytically meaningless** to humans.

However the underlying graph is ideal for machines.

AI, telemetry, threat intel can help generate and enrich the **COG Graph** and keep it current.

This would make a badass infosec product



Key Takeaways

Attackers act rationally within constraints **defenders can affect**

You do not need to win, only **make campaigns unprofitable**

Adversary campaigns contain **decision points** that defenders can deliberately shape

Operational art applies deliberate pressure by **targeting centers of gravity** and employing effects based operations

Much of this can be **precompiled and scaled** through automation and AI

Where to go for more information…

Dark Capabilities: Effects Based Operations for Tech Companies

Greg Conti
Tom Cross

Effects Based Operations

BSides Augusta

Dark Capabilities
When Tech Companies Become Threat Actors

Greg Conti
Tom Cross

Enterprise Capabilities

DEFCON

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

Greg Conti
Bob Fanelli

Collective Defense

Black Hat

Pen Testing a City

Defending Cities

Black Hat

War Planning for Tech Companies

Greg Conti
Tom Cross

Conflict Preparedness

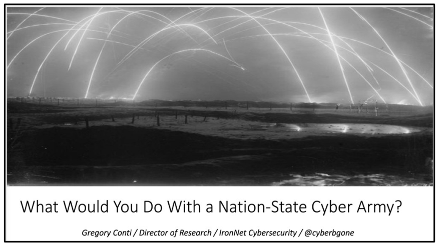
ShmooCon / RSAC

The Library of Sparta

David Raymond
Greg Conti
Tom Cross

Military Doctrine

Black Hat / RSA


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

Gregory Conti / Director of Research / IronNet Cybersecurity / @cyberbgone

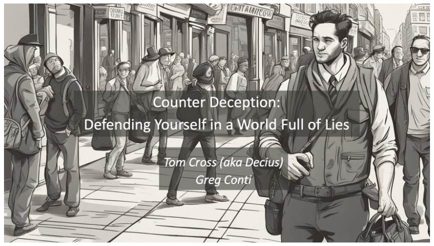
Cyber Armies

USENIX Enigma

ON CYBER
TOWARDS AN OPERATIONAL ART FOR CYBER CONFLICT

Deep Dive

Kopidion Press


Counter Deception:
Defending Yourself in a World Full of Lies

Tom Cross (aka Decius)
Greg Conti

Deception

DEFCON

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

Gregory Conti / Robert Fanelli

Strategic Vulnerabilities

BSides Long Island

Choosing Where to Hit
How Defenders Can Shape Adversary Behavior

Greg Conti
Tom Cross

Operational Targeting

CypherCon

Training and Consulting

Discussion

Cyber defense fails when defenders try to stop attacks.

It succeeds when defenders shape attacker behavior.

Greg Conti // Tom Cross

info@kopidion.com

Kopidion.com **<< slides are available here (under war planning)**

KOPIDION