

Dark Capabilities

When Tech Companies Become Threat Actors

Greg Conti

Tom Cross

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)

- Guy known for giving rants at hacker cons
- Director of Threat Research at **GetRealSecurity**
- Creator of **FeedSeer**, a news reader for Mastodon
- Previously: Security researcher (**IBM X-Force, Lancope**), CTO (**Drawbridge Networks, OPAQ, Fruitful**)
- Principal at **Kopidion**

We teach Adversarial Thinking and Influence Operations courses at Defcon Training

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, 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.



The blurring line between companies and states

"Mr. Lee's Greater Hong Kong is a private, wholly extraterritorial, sovereign, quasi-national entity"

"Mr. Lee's Greater Hong Kong is an open country, always looking for new citizens"

"If you have not attained your [Mr. Lee's Greater] Hong Kong citizenship, apply for your passport now!"

"As for a jail, some place to habeas the occasional stray corpus, any half-decent franchise strip has one."

https://www.redbubble.com/i/t-shirt/Mr-Lee-s-Greater-Hong-Kong-by-Dexternal/13777181.NL9AC

We don’t have the answers.

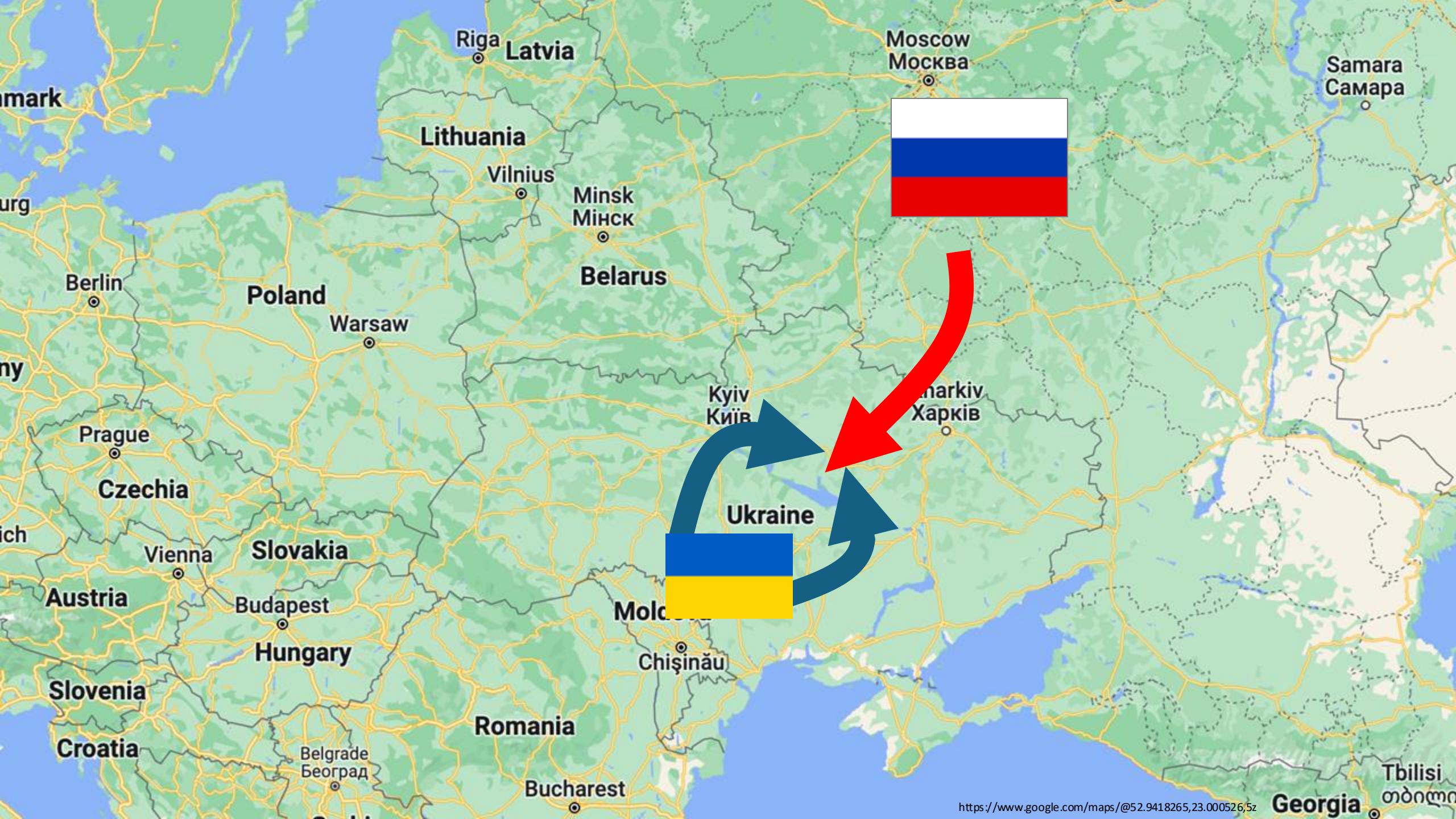
The purpose of this talk is to ask questions and inspire new thinking.

Some Trends

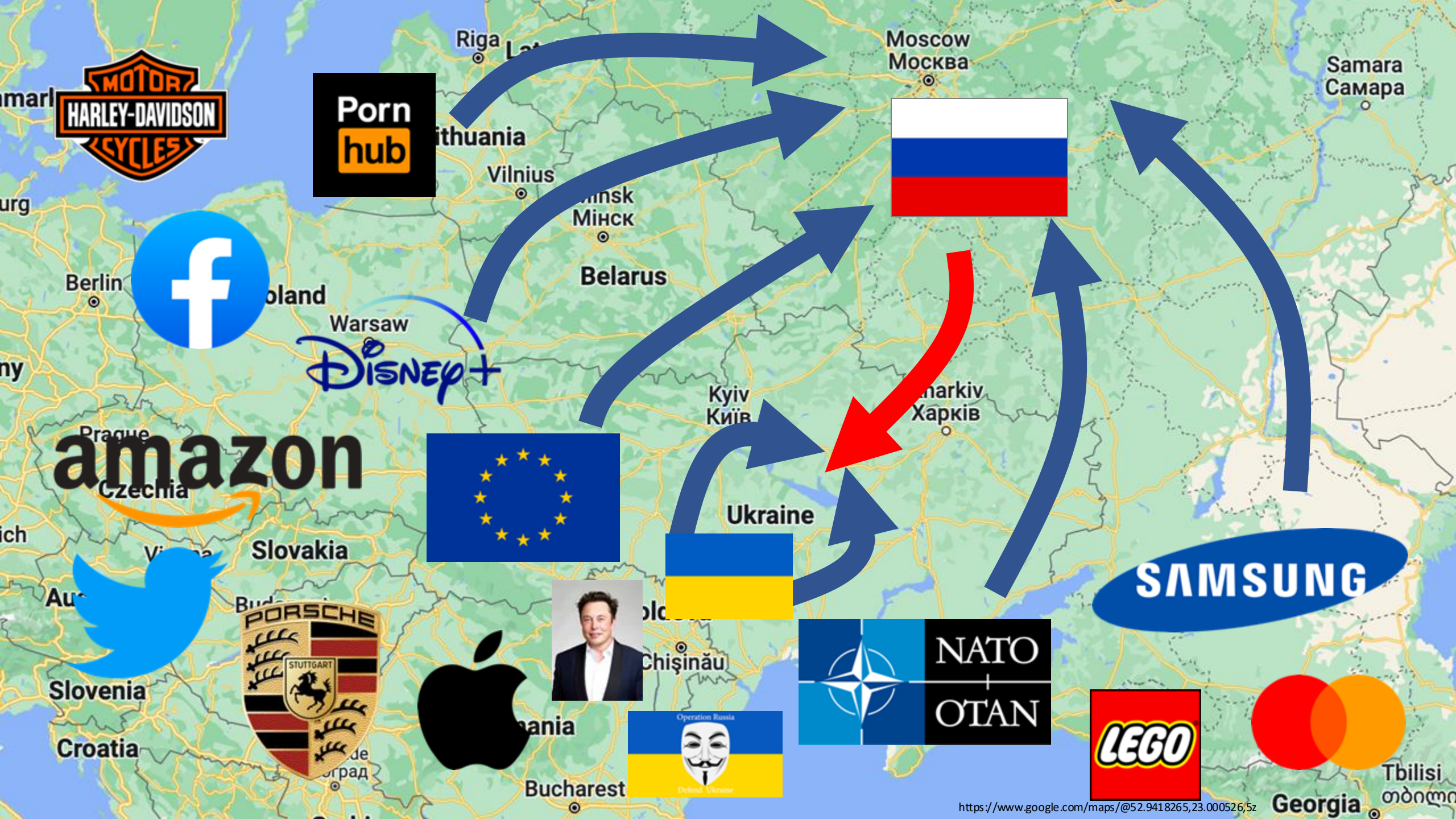
- Tech policy discussions over the past few decades have focused heavily on privacy.
- Tech companies are creating new kinds of capabilities that can impact the real world in new ways and raise new kinds of problems.
- It is becoming less clear whether nation states have supremacy vis-à-vis corporate actors.
- Global conflicts will create circumstances that raise challenging questions about how and when these capabilities will be used.

Why do we care?

Our experience with security and privacy has taught us that important problems spring from the failure to understand the true capabilities of technologies and organizations, not what they purport to do publicly or even what their creators intended internally. Governments have the legal right to commandeer these capabilities. Rogue employees and threat actors can employ these capabilities without permission.



https://www.google.com/maps/@52.9418265,23.000526,5z


Riga
Moscow
Москва
Samara
Самара
Vilnius
Minsk
Мінск
Belarus
Berlin
Warsaw
Kyiv
Київ
Харків
Prague
Czechia
Slovakia
Ukraine
Slovenia
Croatia
Chişinău
Bucharest
Tbilisi
Georgia
Operation Russia
Defend Ukraine
NATO
OTAN
https://www.google.com/maps/@52.9418265,23.000526,5z

A Spectrum of Effects

Effects-Based Operations (EBO)

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?" and "What can I blow up?" to "What effect do I want to create?"

Example effects

- Information Denial
- Perception Shaping
- Economic Disruption
- Mobility Restriction
- Behavior Modification
- Data Degradation
- Adversary Confusion
- Infrastructure Degradation
- Legitimacy Erosion

Exit Market
Block Country IPs

Defensive Security &
Anti-Malware Work

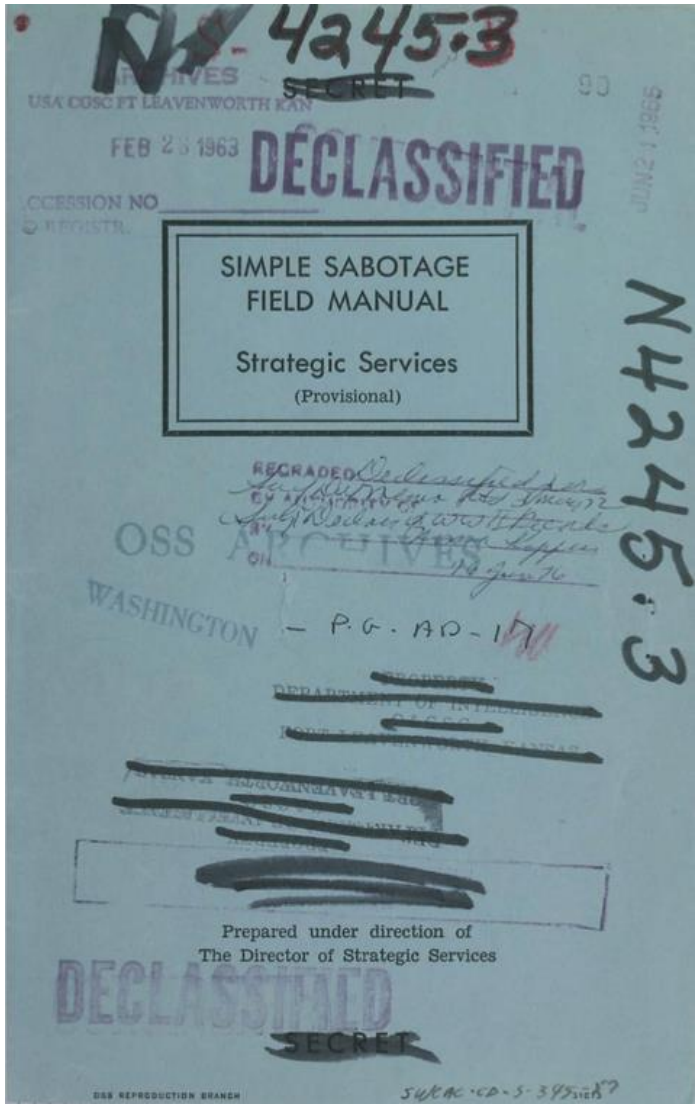
Infrastructural
Support for
Militaries

Protestware
Hacktivism

Vuln Injection
Sabotage



When do the normal rules no longer apply?



https://www.cia.gov/static/5c875f3ec660e092cf893f60b4a288df/SimpleSabotage.pdf



https://www.verzetsmuseum.org/en/world-war-ii-in-the-netherlands

Offensive Company Superpowers

Company Type	Example Capabilities
Search	**Manipulate search algorithms to help or hurt gov/mil operations**
Social Media	Create automated accounts to spread false information and disrupt gov/mil operations
Advertising/Marketing	Create campaigns to target public opinion for/against gov/mil and its operations
Hardware Products	Design and produce hardware to interfere with military equipment and communications
Software	Develop malware to target and disrupt military networks and operations
Cybersecurity	Exploit trusted access into gov and mil networks
Threat Intel	Monitor and analyze threats to military to anticipate and respond to attacks
Open Source Project	**Insert vulnerabilities into popular projects**
Online Retailer	Deny products to adversaries, report on purchases, send compromised products
VPN	Create weak/strong VPN tunnels to exploit/protect military communications from interception
ISP	Block or filter access to websites and services used by the military to disrupt operations.
Web Hosting	Take down websites used by adversary mil and gov, lock out admins and change websites
Ride Sharing	**Create ride-sharing services that can be used to quickly reposition personnel and supplies**

Some Questions

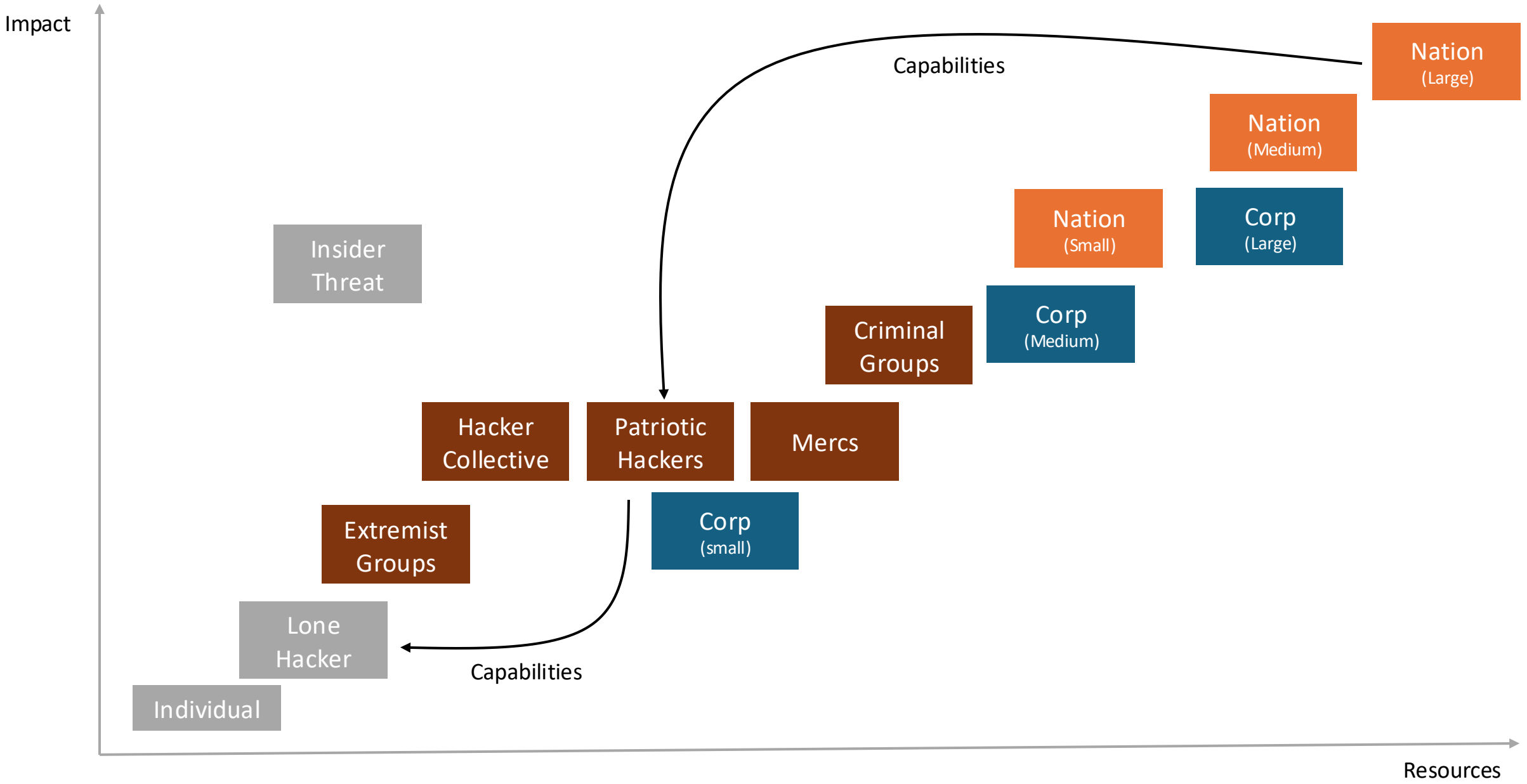
- What sort of capabilities does an organization **truly** have?
- Under what circumstances does it make sense to use what capabilities?
- What sort of risks does an organization face based on its choices? (How does LOAC apply?)
- What sort of actions should the organization never take?
- Is it possible to prevent the organization from making the wrong choices in the future?

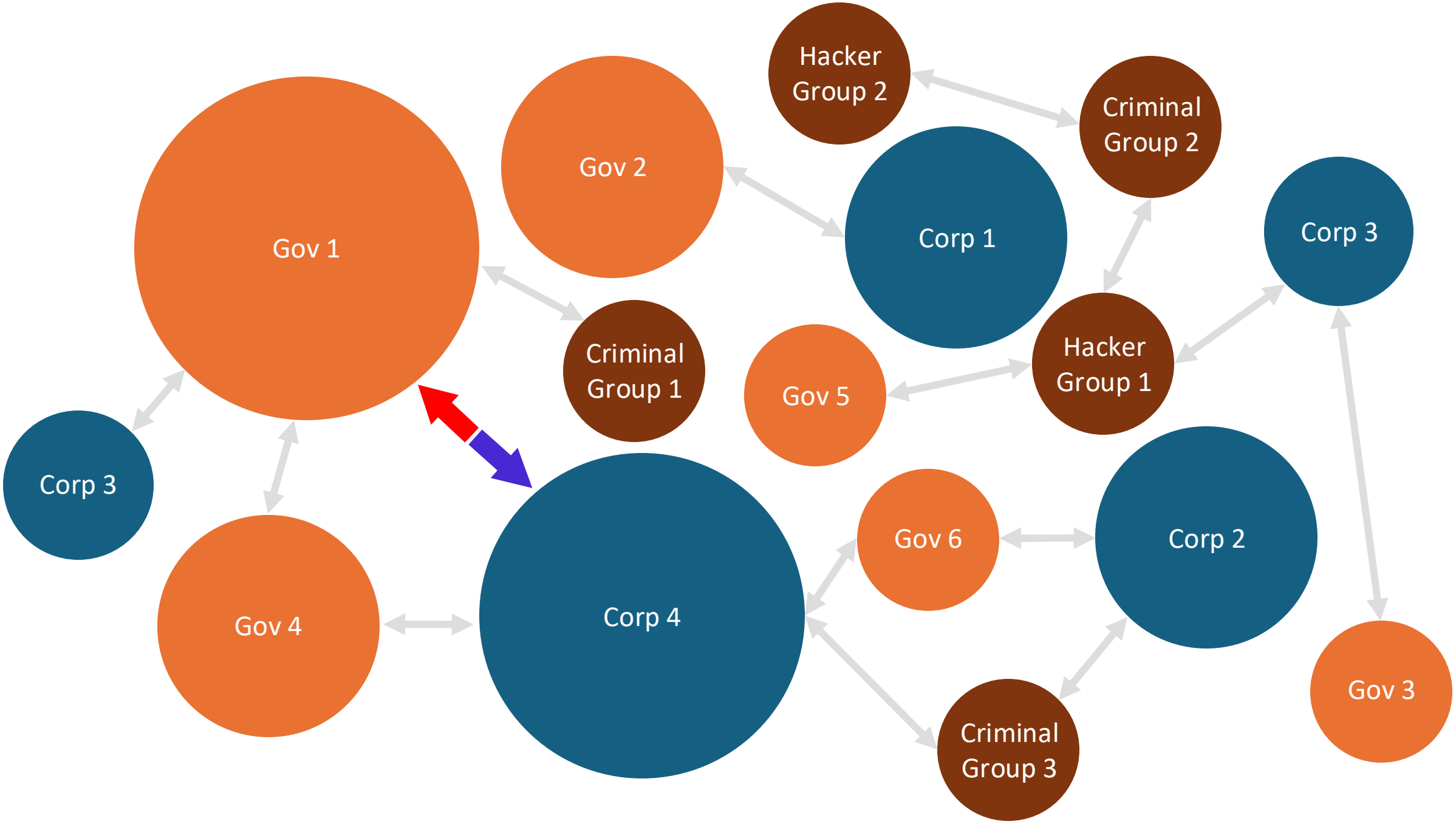


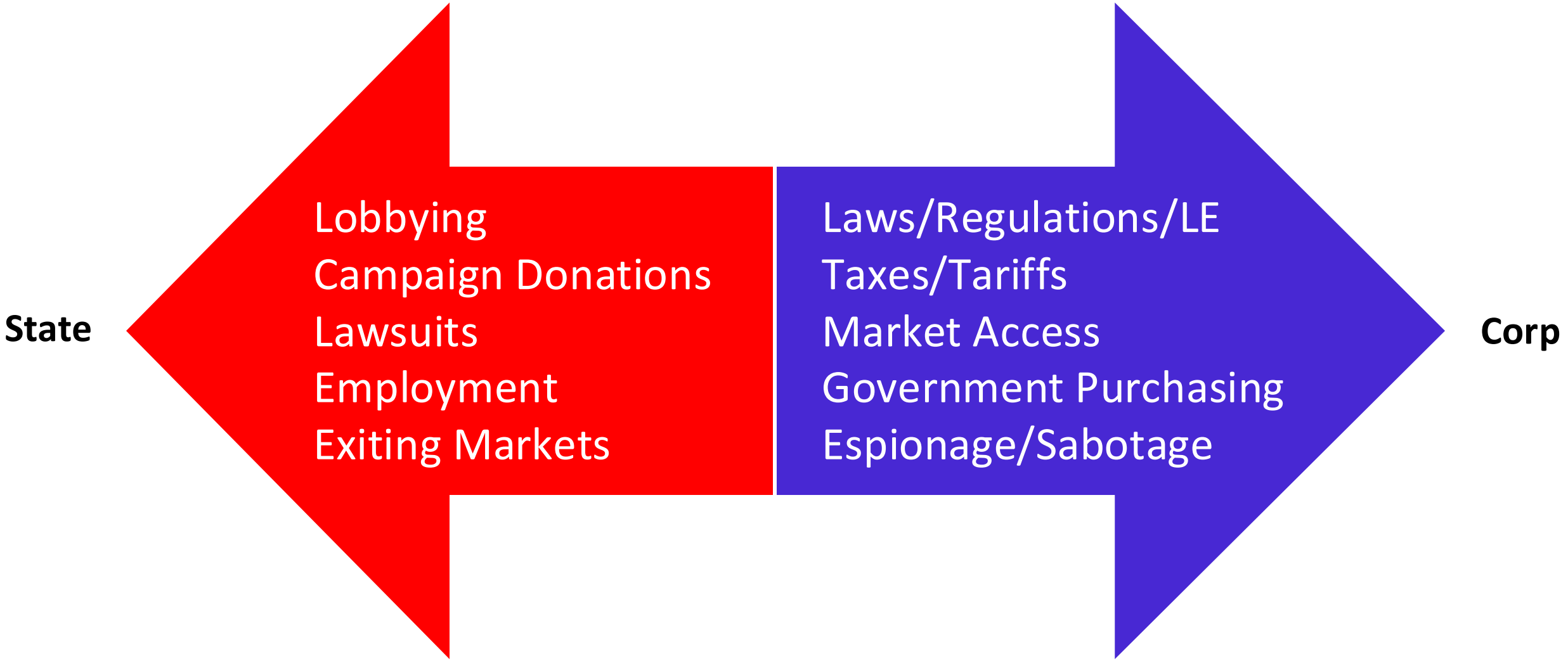
Who is in Charge?



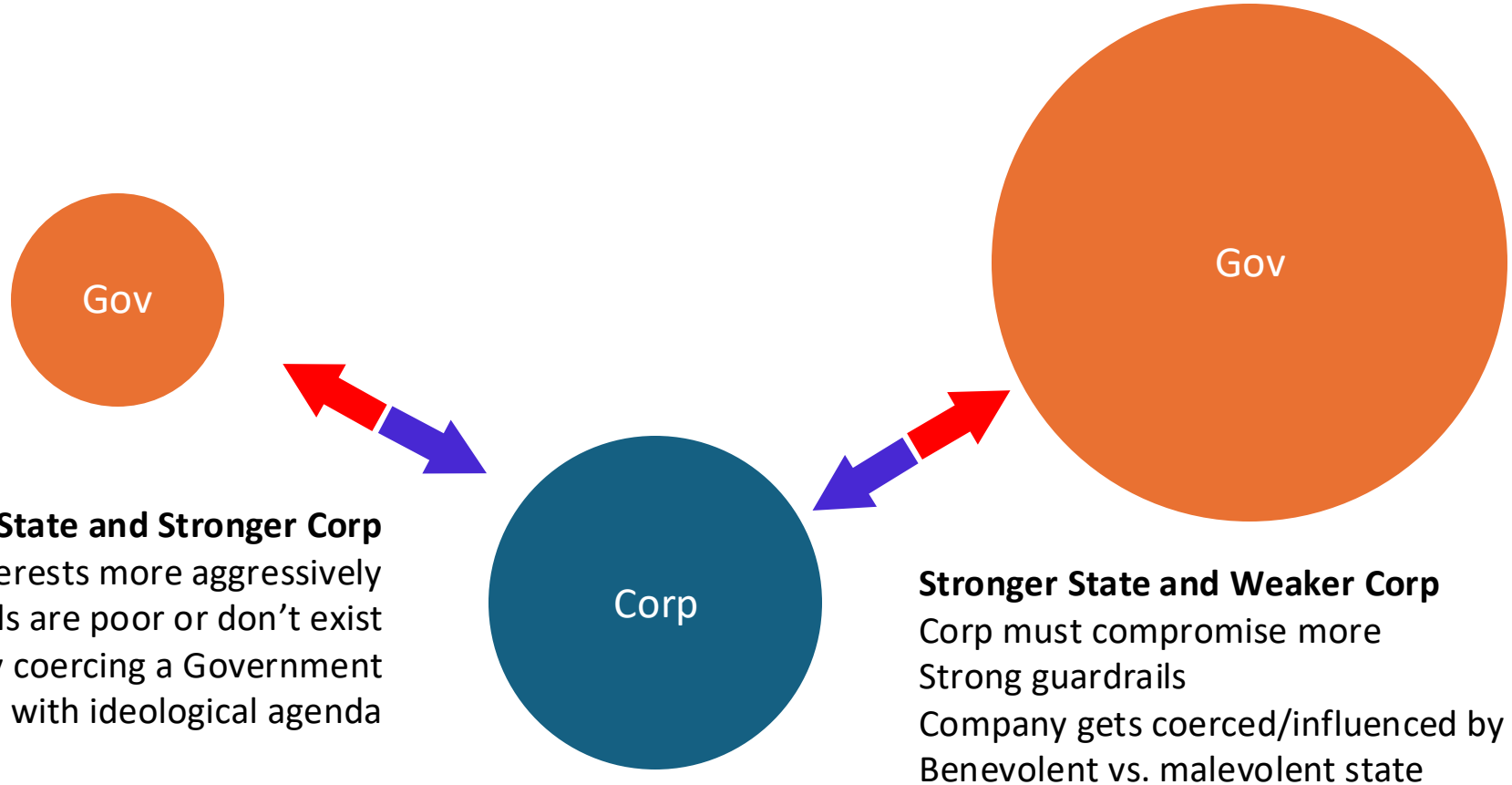
Actors – Impact vs. Resources




Hacker Group 2
Criminal Group 2
Gov 2
Corp 1
Corp 3
Gov 1
Criminal Group 1
Gov 5
Hacker Group 1
Corp 3
Gov 6
Corp 2
Gov 4
Corp 4
Gov 3
Criminal Group 3


State
Lobbying
Campaign Donations
Lawsuits
Employment
Exiting Markets
Laws/Regulations/LE
Taxes/Tariffs
Market Access
Government Purchasing
Espionage/Sabotage
Corp

Relative Power Relationships



Weaker State and Stronger Corp
Corp can pursue interests more aggressively
Guard rails are poor or don't exist
Company coercing a Government
CEO with ideological agenda

Stronger State and Weaker Corp
Corp must compromise more
Strong guardrails
Company gets coerced/influenced by Government
Benevolent vs. malevolent state
Democracy, authoritarian leader, etc.

How much can the Corp get away with before the market or government complains, employees quit, and regulators and or law enforcement attracted?

Market Cap: Company vs. Entire Market

(Trillions)

1. NYSE + NASDAQ	$62.19	**13. NVIDIA**	**$2.79**
2. Shanghai Stock Exchange	$7.19	14. Saudi Stock Exchange	$2.73
3. Tokyo Stock Exchange	$6.56	15. Taiwan Stock Exchange	$2.26
4. National Stock Exchange	$5.70	16. German Stock Exchange	$2.04
5. Euronext	$5.44	**17. Amazon**	**$2.02**
6. Bombay Stock Exchange	$5.26	**18. Alphabet (Google)**	**$2.00**
7. Hong Kong Stock Exchange	$4.55	19. Tehran Stock Exchange	$2.00
8. Shenzhen Stock Exchange	$4.53	20. Swiss Exchange	$1.97
9. Toronto Stock Exchange	$3.55	21. Australian Exchange	$1.89
10. Microsoft	**$3.24**	22. Nasdaq Nordic/Baltic	$1.79
11. Apple	**$3.08**	23. Korea Exchange	$1.56
12. London Stock Exchange	$2.99	**24. Meta Platforms**	**$1.51**

https://en.wikipedia.org/wiki/List_of_major_stock_exchanges
https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/

MICE as a model of CEO motivations

Money

- Corporate profit
- Business advantage
- Corporate strategy
- Competitive pressure
- Example: When the motivation is money, I want social media to promote my product to the right audiences

Compromise and Coercion

- Malicious insider
- Rogue insider
- Non-malicious insider (accident)
- External threat actor
- Example: Data center and satellite office must reside in country
- Government order (Defense Production Act)

Ideology

- Leadership values
- Virtue signaling
- Example: We aren't doing PSYOP we are informing the people

Ego

- CEO's agenda
- Corporate sociopathy
- Example: CEO mocks a country's leadership

Spectrum of **Company** Responsibility

Company-prohibited	Entity helps **stop activity**
Company-prohibited (inadequate)	Entity helps attempts to unsuccessfully stop activity
Company-ignored	Entity knows about the activity but is **unwilling to take action**
Company-encouraged	Entity **encourages third-party** to take action as a matter of policy
Company-shaped	Entity supports third-party to take action
Company-coordinated	Active coordination between entity and third-party for a given action
Company-ordered	**Entity directs third-party proxies** to conduct the activity
Company-rogue-conducted	Out of control insiders take actions
Company-executed	Entity **undertakes the action under its direct control**
Company-integrated	Entity jointly conducts activity with third-party

*Jason Healey, Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council

Initiator	Why	Corp Authorized	Gov Authorized	Examples
Employee Accident	weak internal controls	n/a	n/a	Software update bricks machines
Internal Abuse	rogue insider, weak internal controls	No	No	Employee independently bans account of a world leader
Independent Third-Party Actor	Hacktivism, financially motivated criminal	No	No	Hacking of Russian gas pump displays by Ukranian activists
Corporate Strategy	revenue, regulatory pressure	Yes	Yes	OS company scans for sensitive content, lawful intercept, rideshare company tracks riders after ride
Independent Corporate Action	MICE	Yes	No	SATCOM company deuthorization in a war zone, Geo-trojaned NPM package
State Coercion	legal or illegal government request, collaboration, threat or order, blackmail	No	Yes	U.S. Defense Production Act, wiretapping law, court order
State Infiltration	APT group, supply chain compromise, infiltration	No	Yes	Oil pipeline ransomware attack, North Korea's fake employees



Realpolitik Goals: Maximize transnational leverage, protect IP, avoid dependence on any one state, maximize profit and shareholder value

Stated Goals: Global prosperity, inclusive growth, compliance, rainbows and unicorns, etc.

- Avoid public alignment with single government
- Sees itself as a non-state actor with state-level influence
- Comply with laws of powerful jurisdictions. Lobby to block or prevent inconvenient laws.
- Tighter guardrails

Governments treat companies as partners, *when not inconvenient*



Realpolitik Goals: Survive disruption, sidestep entanglement, protect core business, minimize long-term damage, maximize profit and shareholder value

Stated Goals: National support, resilience, stakeholder responsibility

- Avoid picking sides, unless forced
- Offer support selectively, based on risk-adjusted ROI
- Follow laws of strong powers when risk is high, sidestep weaker states, re-domicile to avoid coercion
- Looser guardrails

Governments shift to coercion - export controls, asset seizures, data and production demands

Governments will seek capabilities systematically.

Military 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

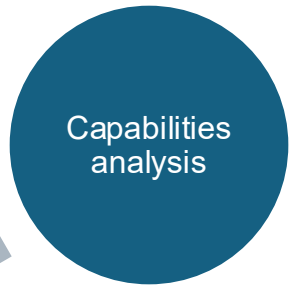
Using capabilities to create effects, at scale



Actor's motivations and incentives drive desired outcomes selection



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



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



Assign team or individual which possesses the desired capability



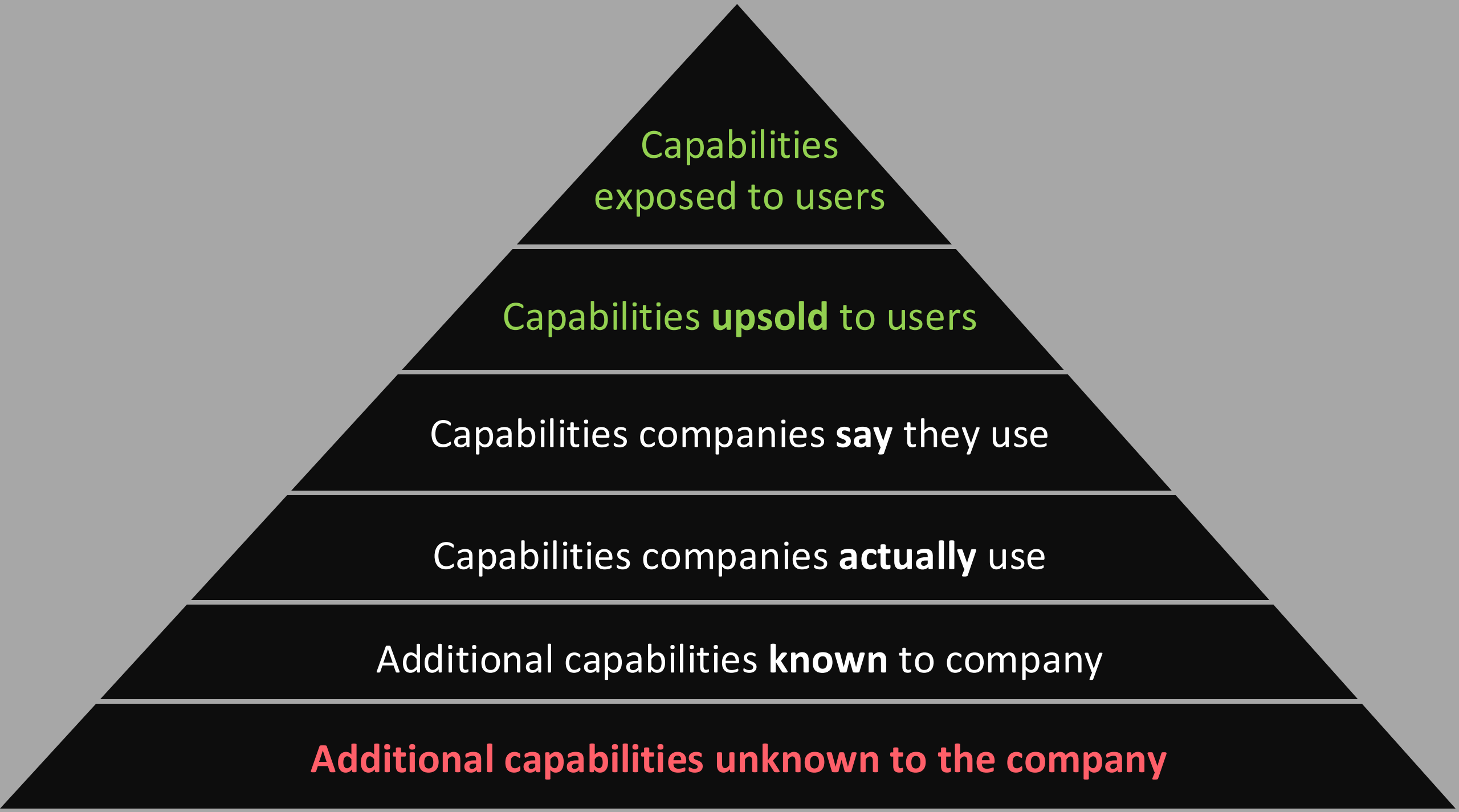
The kill chain happens here



Were the desired effects and end state achieved?

Note: Each Threat Actor has their own wheel, including its own target and desired effects list

https://irp.fas.org/doddir/dod/jp3_09.pdf


Capabilities exposed to users
Capabilities upsold to users
Capabilities companies say they use
Capabilities companies actually use
Additional capabilities known to company
Additional capabilities unknown to the company



Company Mission: "To disguise surveillance and adtech infrastructure as home convenience, one bulb at a time.”

Wifi Enabled Lightbulb

- Pattern of life data about when the user is home (or not)
- Bluetooth and wifi device scanning
- Backdoor into home internal network
  - Access to management interface of wifi router
- Mobile App provides user location data
- Has a false power off mode, but isn’t really off, under the guise of an emergency lighting capability

Let’s add a microphone and motion sensors and write some sample marketing copy for this lightbulb shall we…



Company Mission: "To disguise surveillance and adtech infrastructure as home convenience, one bulb at a time."

Introducing TronLum™
Smarter Light for Smarter Living
"Your lightbulb just got a sixth sense."

TronLum™ uses advanced **ambient awareness technology** to adapt lighting based on subtle environmental cues—like motion, presence, and even mood indicators.

Adaptive Presence Detection

Your light now knows when you're nearby—even before you touch a switch. Walk into a room and feel the glow respond with perfect timing.

Intelligent Room Insights

Optimize your routines with *discreet occupancy awareness* and *pattern-based adjustments*. TronLum learns your preferences so you don't have to micromanage your lights.

Peace of Mind, Reinvented

Receive real-time updates when unexpected movement is detected in your home. Whether you're away or asleep, your lighting system has your back.

Seamless Integration

Syncs effortlessly with your smart home ecosystem, enabling customized automations based on *presence*, *activity levels*, and *behavioral rhythms*.



https://www.nasa.gov/image-article/earth-night/

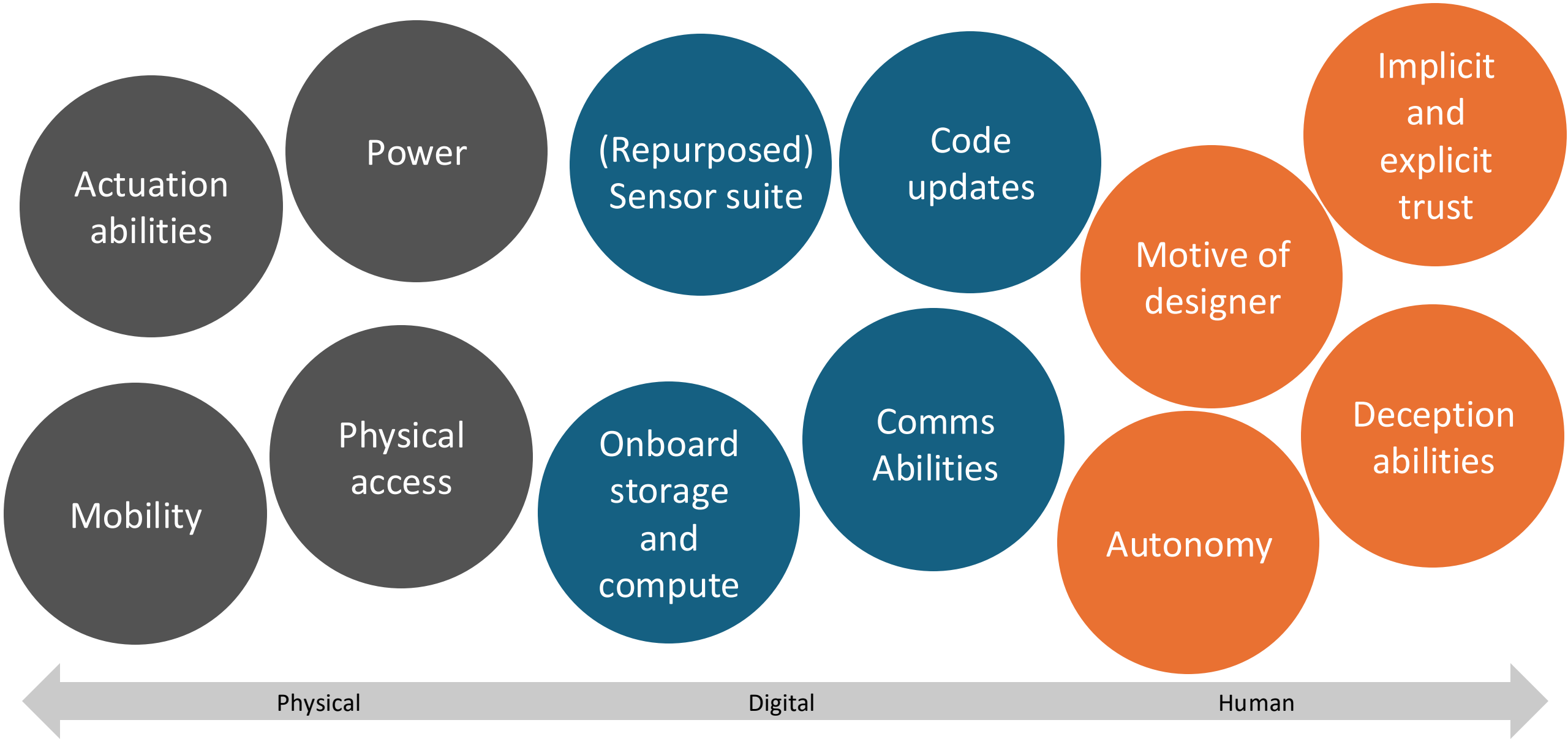


Company Mission: To normalize autonomous surveillance under the guise of household hygiene

Vacuum Cleaner Robot

- Precision mapping for future intrusion
- Audio/video surveillance for intelligence, blackmail, ads or ideological compliance
- Covert mapping or jamming of EM spectrum
- RFID and Smartcard harvesting
- Control smart TVs, phones, or IoT devices without detection
- Disruptive non-audible sounds that influence humans and pets
- DNA collection and biometric harvesting
- Covert cyber or physical (micro) payload delivery
- Accidental “malfunction” to cause injury or damage

Select facets for analyzing true product capabilities





Cybersecurity

Mission: To turn paranoia into pipeline, FUD into ARR, and zero days into Q4 growth opportunities.

Intelligence

- Global sensor networks and intelligence analysis teams
- Gather intelligence for governments or competitors
- Sell, rather than report, vulnerabilities
- Attribution for hire

Protect

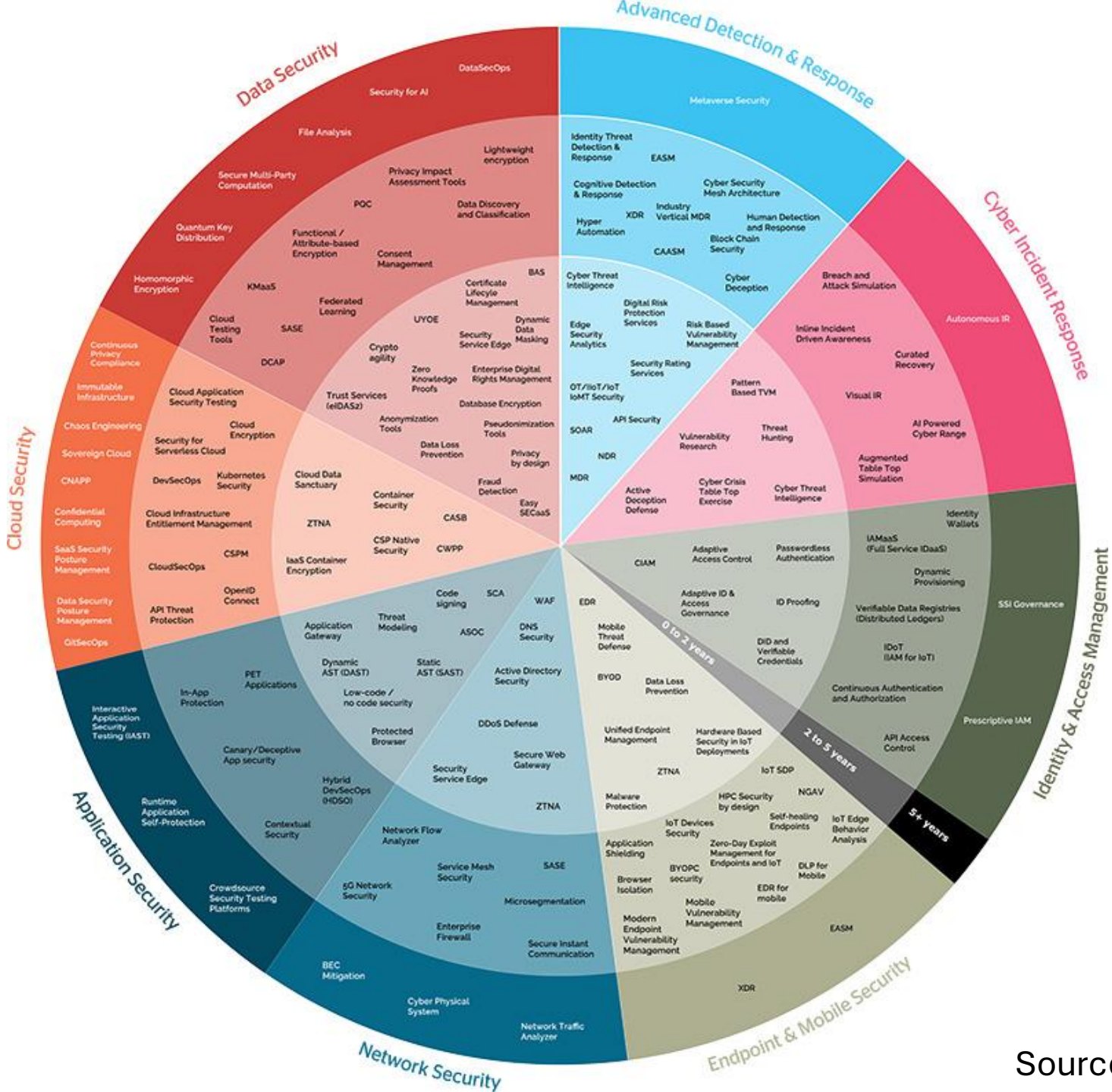
- Silent data exfiltration through opaque channels
- Silently disable defenses
- Persistent backdoor deployment disguised as protection

Detect

- Ignore specific alerts and malware
- Surveillance disguised at threat hunting

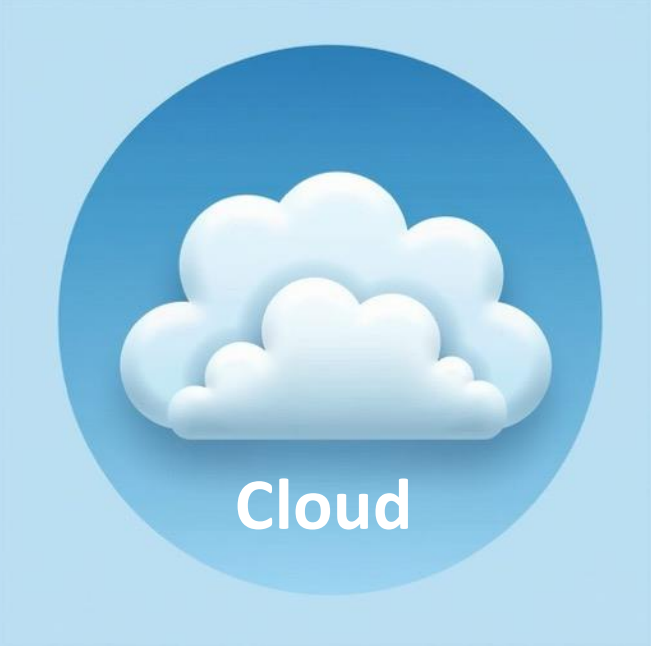
Respond

- Search user files, at scale
- User password collection
- Brick systems at scale
- Feedback IR event internals to threat actors
- Covert offensive operations



Source: Dr. Rabi Prasad Padhy

Cloud



Mission: To entrench our software, cloud, and licensing products so deeply into global institutions that no one can ever fully leave us.

Intelligence Operations

- Silent data theft from VMs, containers, storage
- Harvest secrets (tokens, credentials) from memory
- Analyze metadata to map users, behaviors, and org relationships
- Intercept traffic inside VPCs
- Mirror data for third-parties

Adversary Engagement

- Throttle critical infrastructure
- Compromise national defense workflows
- Targeted or global kill switch
- Sell covert infrastructure to threat actors
- Insert false flags

Infrastructure & Supply Chain

- Backdoor cloud-published images
- Tamper with CI/CD artifacts during cloud-native builds or deployment
- Modify base images for persistence
- Disable security tools
- Serve poisoned packages

Identity & Access

- Impersonate users via internal APIs
- Inject hidden roles and permissions into tenants
- Create shadow admins
- Suppress audit logs



Mission: To harvest the world's data, rewrite it in our voice, and rent it back to you indefinitely.

Cognitive & Psychological Warfare

- AI-orchestrated belief collapse
- Automated alteration of historical timelines
- Cognitive honeypots
- Synthetic morale operations against populations
- Synthetic persona generation

Surveillance, Profiling, and Exploitation

- Model and simulate real individuals, at scale
- Real-time emotional telemetry
- Pattern of life analysis
- Indefinitely log user actions
- User deanonymization systems

Cyber and Cyber-Physical Warfare

- Fully automated persona generation and deepfake social engineering
- Insert vulns in free software
- Training data poisoning
- Control lethal robotics
- Orchestrate and evolve cyber attacks and campaigns

Information and Narrative Control

- Synthetic persona swarms
- Harassment automation
- Create and share deceptive maps
- Mimic writing styles for deception
- Remove topics from AI awareness

See also MIT's AI Risk Repository https://airisk.mit.edu/



Mission: To slowly phase out human drivers, cities, and competitors, until all roads lead to us.

Mobile Sensor Platform as a Service

- Surreptitious mapping
- Stationary or mobile collection
- Sniff passenger tech
- Regular collection along targeted surveillance routes
- Video and audio recording across the fleet

Persistent Tracking and Targeted Surveillance

- Pattern-of-life data for riders and routes
- Track political figures, journalists, or activists in real time
- Send a specific car or driver
- Track users' locations before, during, and after rides
- Follow individuals of interest across multiple vehicles
- Provide surveillance data to regimes

Behavioral Control and Denial Capabilities

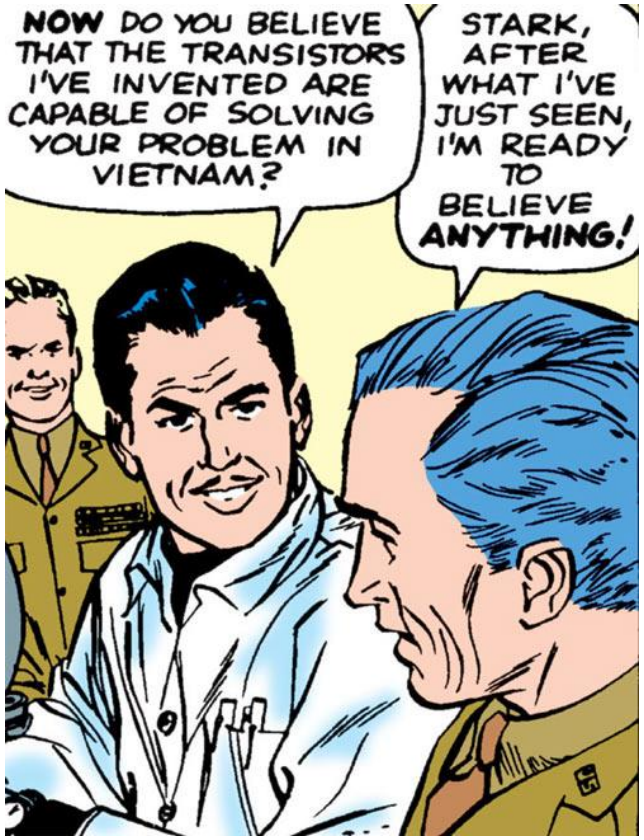
- Selectively deny or delay service
- Create false ride records
- Build behavioral, political, or psychological profiles of riders

Tactical and Physical Capabilities

- Coercive transport
- Targeted car crashes
- Route or destination "errors"
- Crisis or extralegal logistical transport

Transportation Shaping and Mobility Disruption

- Traffic on demand
- Block roads during a crisis
- Reroute traffic to favor business, military, or political outcomes



Captain America: Big man in a suit of armor. Take that off, what are you?

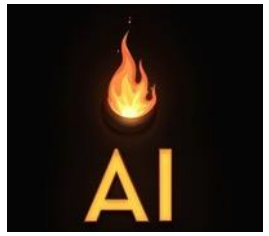
Tony Stark: Genius, billionaire, playboy, philanthropist.

MEGACORP


Cybersecurity



Adult

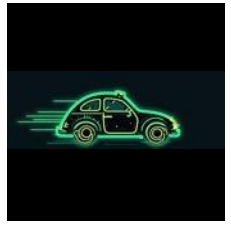


AI


Social Media


Smart Lighting

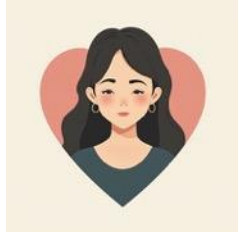

Auto


Rideshare


Cloud



Space


Dating



Robotic



Defense Contractor


Genomics


Mobile Telecom



Payment Processor

https://www.writeups.org/tony-stark-iron-man-marvel-comics/



What about the future?

- Agentic AI tools that empower individuals with limited funding & knowledge to create and to do
- Increasingly ubiquitous robotic systems
- Increasing privatization of space technology and infrastructure in orbit, on the moon, and on mars
- Neural interfacing*
- Predictive behavioral modeling of individual people
- Predictive behavioral modeling of whole populations & civilizations
- Large scale malign influence as a service
- AI driven education and molding of children
- Automated law enforcement

* just imagine the RSAC 2037 vendor floor

Things Companies Could Do (Probably Won't)



Not recommended

Consider misuse by:

- Your Customers/Users
- Your Insiders
- Threat Actors
- Your Executives
- Governments (by commandeering)

Can you create checks, balances, and Ulysses pacts?

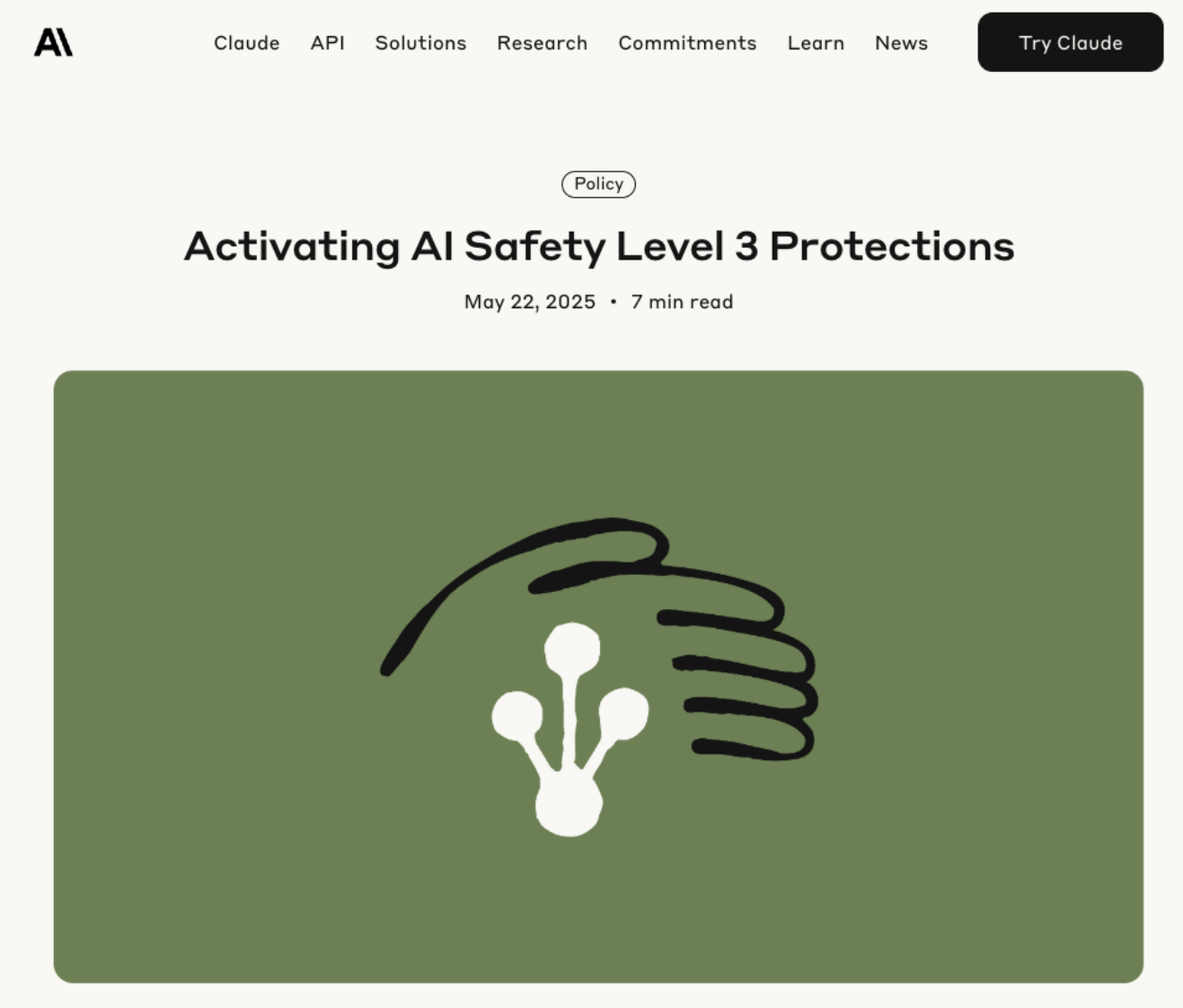
- Through technical architectures
- Through internal processes
- Through engagement with neutral third-party auditors
- Through public transparency

https://commons.wikimedia.org/wiki/File:Bury_your_head_in_the_sand.jpg

Adversarial Capability Mapping



- Create an **internal red team exercise** where teams map out all possible misuses of the company's own platforms, tools, and access, regardless of legality or policy.
- Ask: *If we had no ethics or were compromised, what could the company do to users, competitors, or the public?*
- Include scenarios driven by greed, revenge, ideology, coercion, insider compromise, and external threat actor attack
- Build a mirror universe capability map, then use it to inform access control, auditing, and system design



Example: Anthropic's AI Red Teaming

Assesses the use of AI to aid:

- Offensive Cyber
- Biological Weapons Development
- Nuclear Weapons Development

Developing guardrails

Key point – focused on user/consumer misuse

https://www.anthropic.com/news/activating-asl3-protections
https://www.anthropic.com/news/strategic-warning-for-ai-risk-progress-and-insights-from-our-frontier-red-team
https://x.com/sjgadler/status/1925628790723510304

Things Governments Could Do (Probably Won't)

Question: Public/Private national security engagement tends to be framed in terms of "critical infrastructure" segments. Are there important capabilities that framework misses?



Multi-Domain Strategic Capabilities Assessment

What high risk capabilities exist that could:

- Further national domestic and foreign policy objectives (if used offensively)
- Undermine the same if misused by a threat actor
- Undermine the same if misappropriated by corporate leadership (or unaligned)
- Are not covered by existing critical infrastructure segments
- Assessment must occur across multiple domains

Encourage Public/Private Coordination

- Carrots: Industry/Gov Communication
- Sticks: Forced Transparency
- Frameworks for Wartime Command and Control of critical capabilities

https://techcrunch.com/2018/04/10/you-dont-think-you-have-a-monopoly-read-sen-grahams-delightful-grilling-of-zuckerberg/

Dark Capabilities: Key Takeaways



Tinfoil hat and smart light bulbs
oil on canvas, Special Exhibit, MoMA, 2037

Most companies don’t intend to misuse power, but power still exists, and ignoring it invites misuse

If you're in a company: know your true capabilities, threat model accordingly

Well informed internal controls and tailored government oversight are both necessary, and likely insufficient

If you're a user: don’t trust the stated purpose, instead ask what the system can do

Once you are sensitized to hidden capabilities, you’ll see them everywhere

Questions



An army of tinfoil hats and smart light bulbs
oil on canvas, Special Exhibit, MoMA, 2037

It's not about what a system claims to do, it's about what it can do. The rest is just details.

Greg Conti // Tom Cross

Kopidion.com