War Planning for Tech Companies

Greg Conti
Tom Cross

https://d1ldvf68ux039x.cloudfront.net/thumbs/photos/1502/1752886/1000w_q95.jpg

Bios

Greg Conti

Tom Cross

The views expressed in this talk are those of the authors and do not reflect the official policy or position of Kopidion, the US Government, or any of our other current or past employers. We are not lawyers, and nothing in this talk constitutes legal advice. Consult with an attorney if you are uncertain of the legality of any action you might take.

AP U.S. WORLD POLITICS VIDEO SPOTLIGHT ENTERTAINMENT SPORTS BUSINESS SCIENCE FACT CHECK CLIMATE H

Russell Brand UAW strike Dallas Cowboys Travis Hunter injury Drew Barrymore

WORLD NEWS

The Taliban have detained 18 staff, including a foreigner, from an Afghanistan-based NGO, it says

Cisco Systems pulled out of russia and destroyed $23.42m worth of equipment

By: Maksim Panasovskyi | 05.04.2023, 13:50

BBC NEWS

Ukraine war: The Russian ships accused of North Sea sabotage

By Gordon Corera
Security correspondent, BBC News

19 April 2023

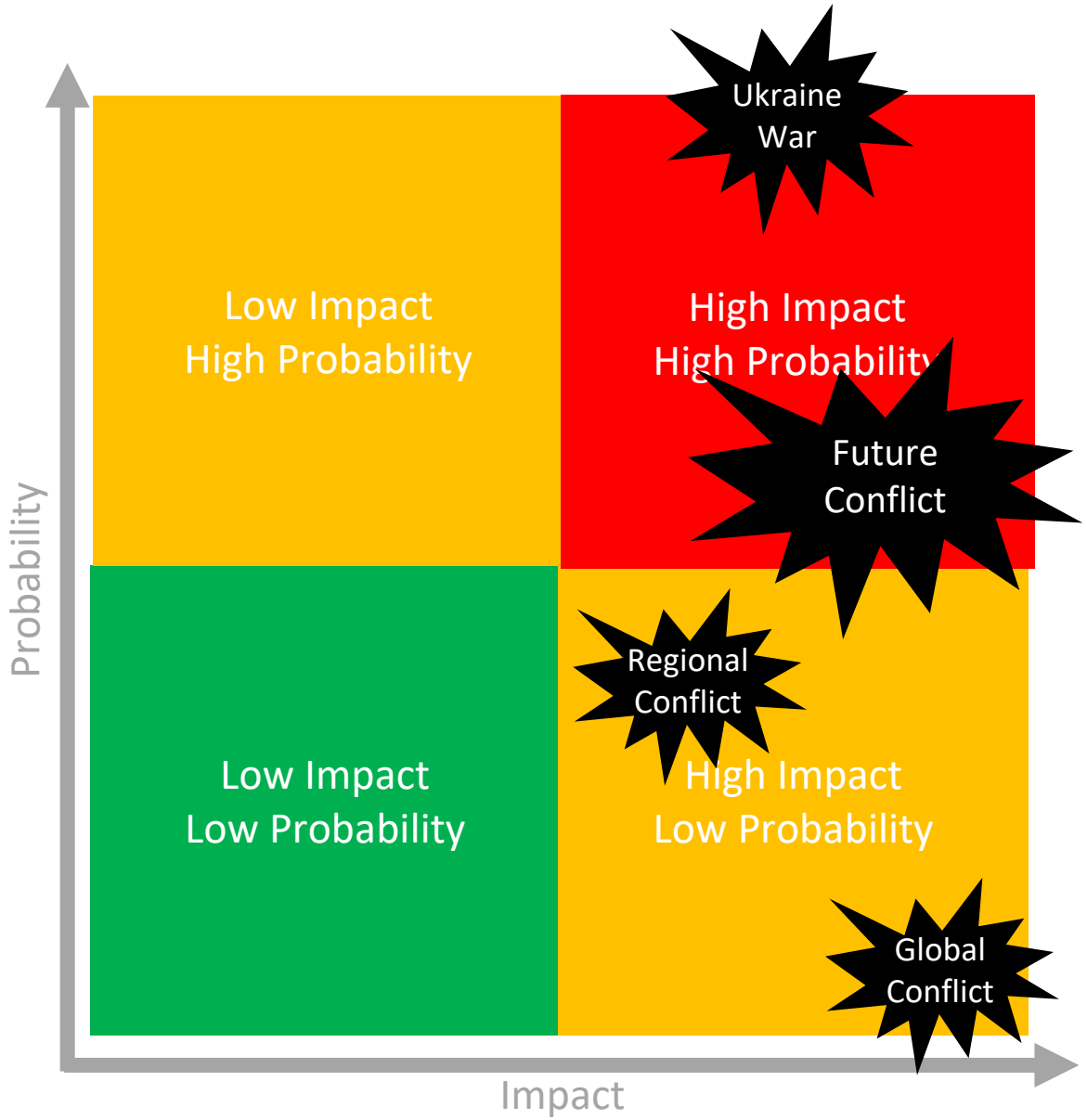
FP news | analysis | podcasts | the magazine | newsletter

Companies Thought They Could Ignore Geopolitics. Not Anymore.

Deglobalization is changing corporate behavior as boardrooms start paying attention to war.

By **Elisabeth Braw**, a columnist at *Foreign Policy* and a fellow at the American Enterprise Institute. FP subscribers can now receive alerts when new stories written by this author are published. Subscribe now | Sign in

The Problem: Future Conflict Preparedness



- We are focusing on Kinetic War and Multi-Domain Conflict
  - Not exclusively cyber conflict or influence operations
- A Great Power conflict is no longer an unimaginable threat
- The probability is high enough that we should be planning now
- Serious consequences of not planning
- **How would your organization respond?**

BREAKING DEFENSE

Special Features

AIR LAND NAVAL SPACE NETWORKS / CYBER ALL DOMAIN CONGRESS PENTAGON GLOBAL

FEATURED: Space Symposium » Sea-Air-Space » 2024 Budget » Indo-Pacific »

GLOBAL, NETWORKS / CYBER

US tech firms should wargame response if China invades Taiwan, warns NSA cybersecurity chief

"You don't want to be starting that planning the week before an invasion, when you're starting to see the White House saying it's coming," said NSA's Rob Joyce. "You want to be doing that now."

By SYDNEY J. FREEDBERG JR. on April 11, 2023 at 2:08 PM

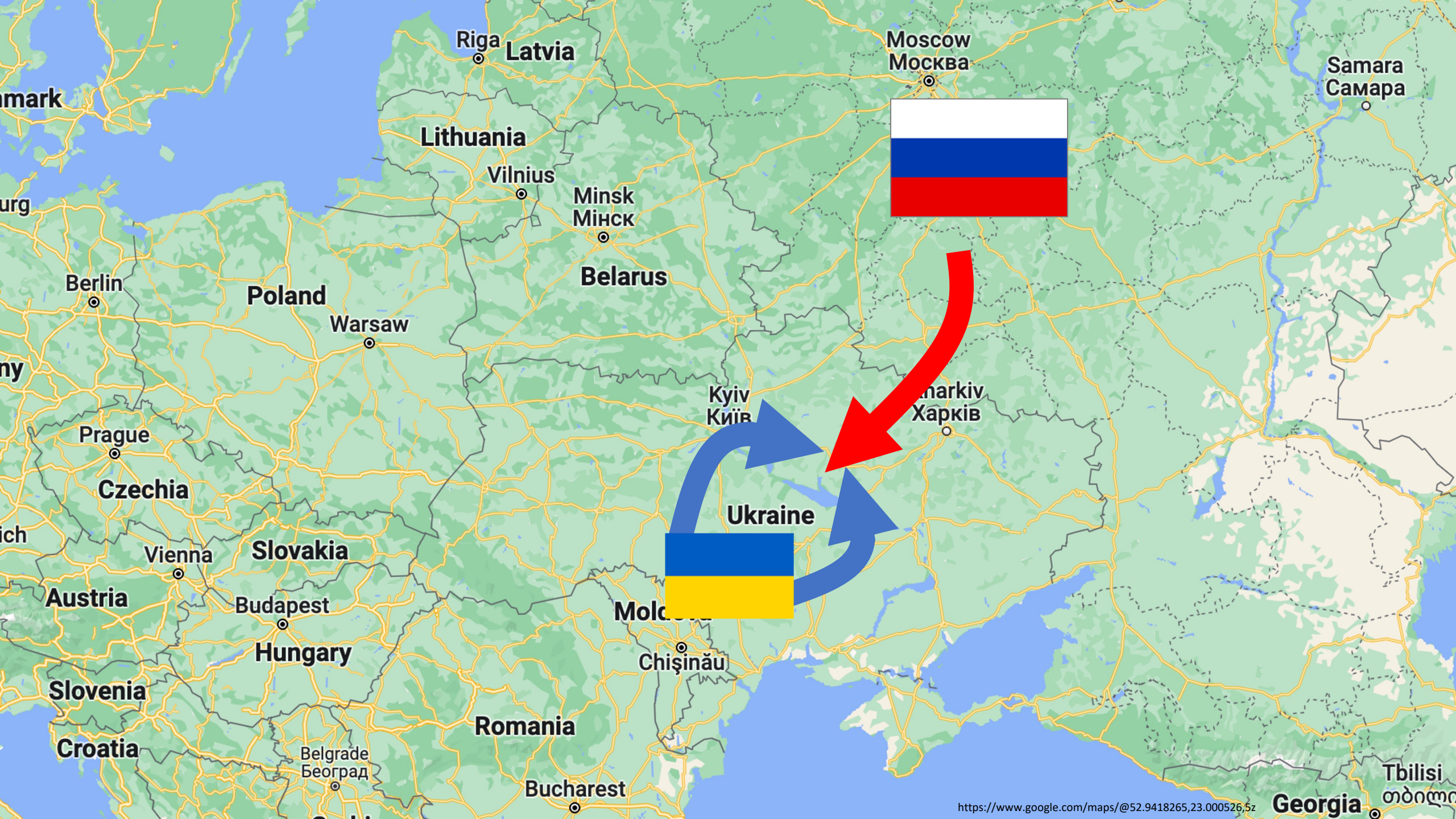
Robert Joyce, director of cybersecurity at the National Security Agency (NSA), speaks during a Senate Armed Services Subcommittee hearing in Washington, D.C., U.S., on Wednesday, April 14, 2021. (Al Drago/Bloomberg via Getty Images)

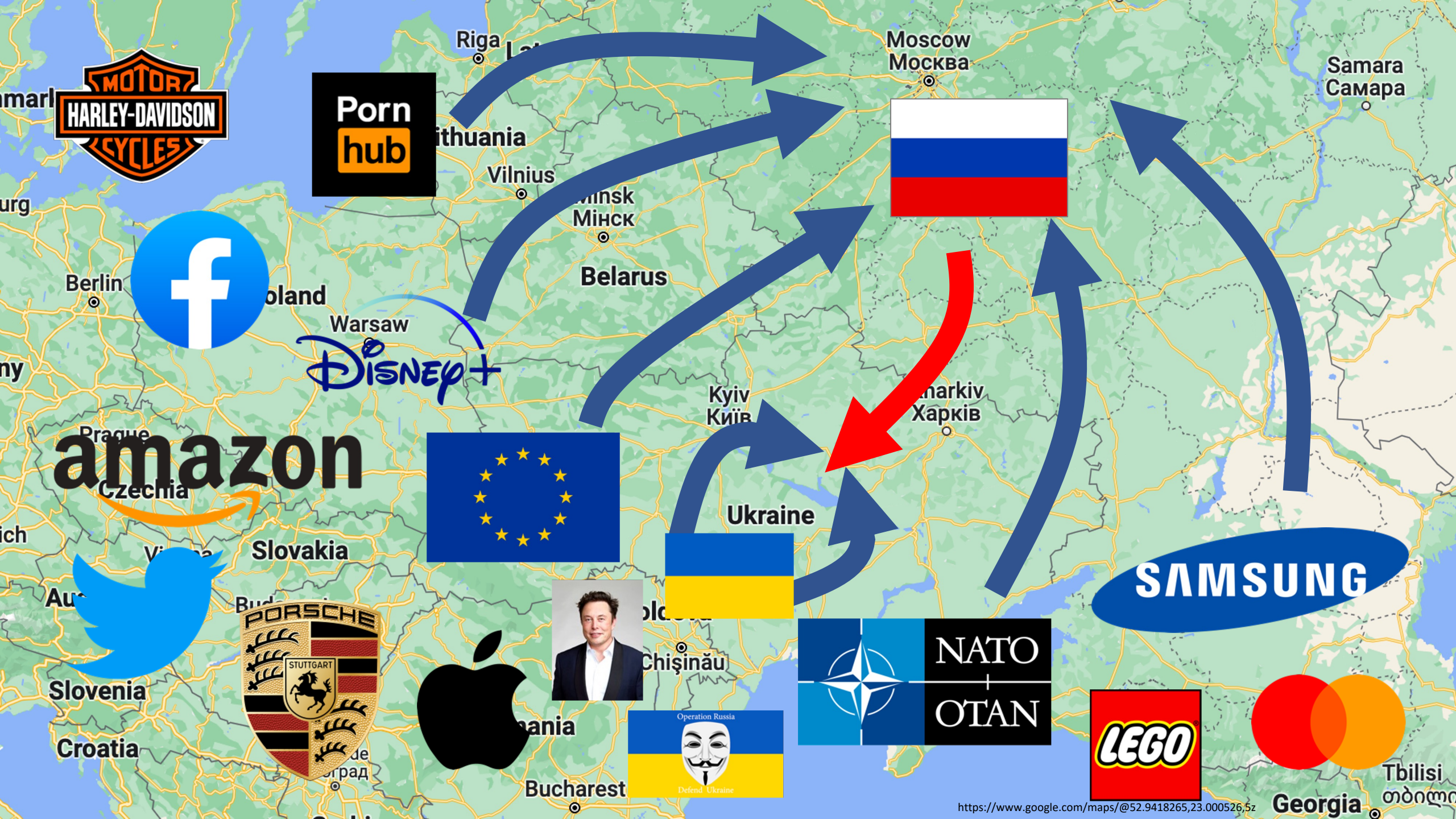
"You don't want to start planning the week before an invasion, when you see the White House saying it's coming"

"You want to be planning now."

Checklist

https://breakingdefense.com/2023/04/us-tech-firms-should-wargame-response-if-china-invades-taiwan-warns-nsa-cybersecurity-chief/

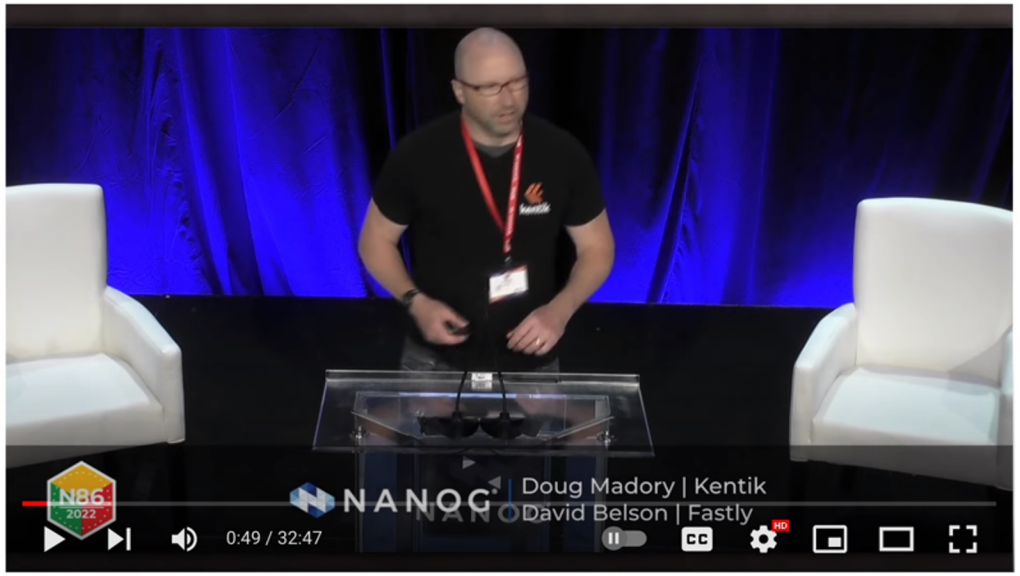

Riga
Latvia
Moscow
Москва
Samara
Самара
Lithuania
Vilnius
Minsk
Мінск
Belarus
Berlin
Poland
Warsaw
Kyiv
Київ
Харків
Prague
Czechia
Ukraine
Vienna
Slovakia
Austria
Budapest
Hungary
Chişinău
Slovenia
Romania
Croatia
Belgrade
Београд
Bucharest
Tbilisi
Georgia
https://www.google.com/maps/@52.9418265,23.000526,5z


Riga
Moscow
Москва
Samara
Самара
Vilnius
Minsk
Мінск
Belarus
Berlin
Warsaw
Kyiv
Київ
Kharkiv
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

https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain

Source: **Politiken** (Based on Our Yale List)

Lessons from Ukraine



Internet Impacts Due to the War in Ukraine

Internet Impacts Due to the War in Ukraine (Video)

Ukraine's Wartime Internet from the Inside

The Russification of Ukrainian IP Registration

Tactical

- **Using credentials from captured technicians**
- Employment of destructive malware
- **Deliberate and accidentally severed fiber**
- Kinetic attacks destroy infrastructure and disrupt utilities
- Heroic efforts by in-country technicians to make repairs

Operational

- **Wholesale cutoff of network transit in an occupied city**
- BGP Hijacking
- Disruption of satellite and ISP operations
- DDOS prior to kinetic attacks
- Switchover to Russian transit in occupied regions
- **Shift to US-based cloud and satellite comms providers**

Strategic

- Request to ICANN and RIPE that Russia be disconnected
- **Meta declared extremist org**
- Backbone providers threaten disconnecting Russia from internet
- 8.2M refugees (include techs) left country

Hot Spots

War in Ukraine Escalates

?

Something Else

Taiwan

North Korea

Iran

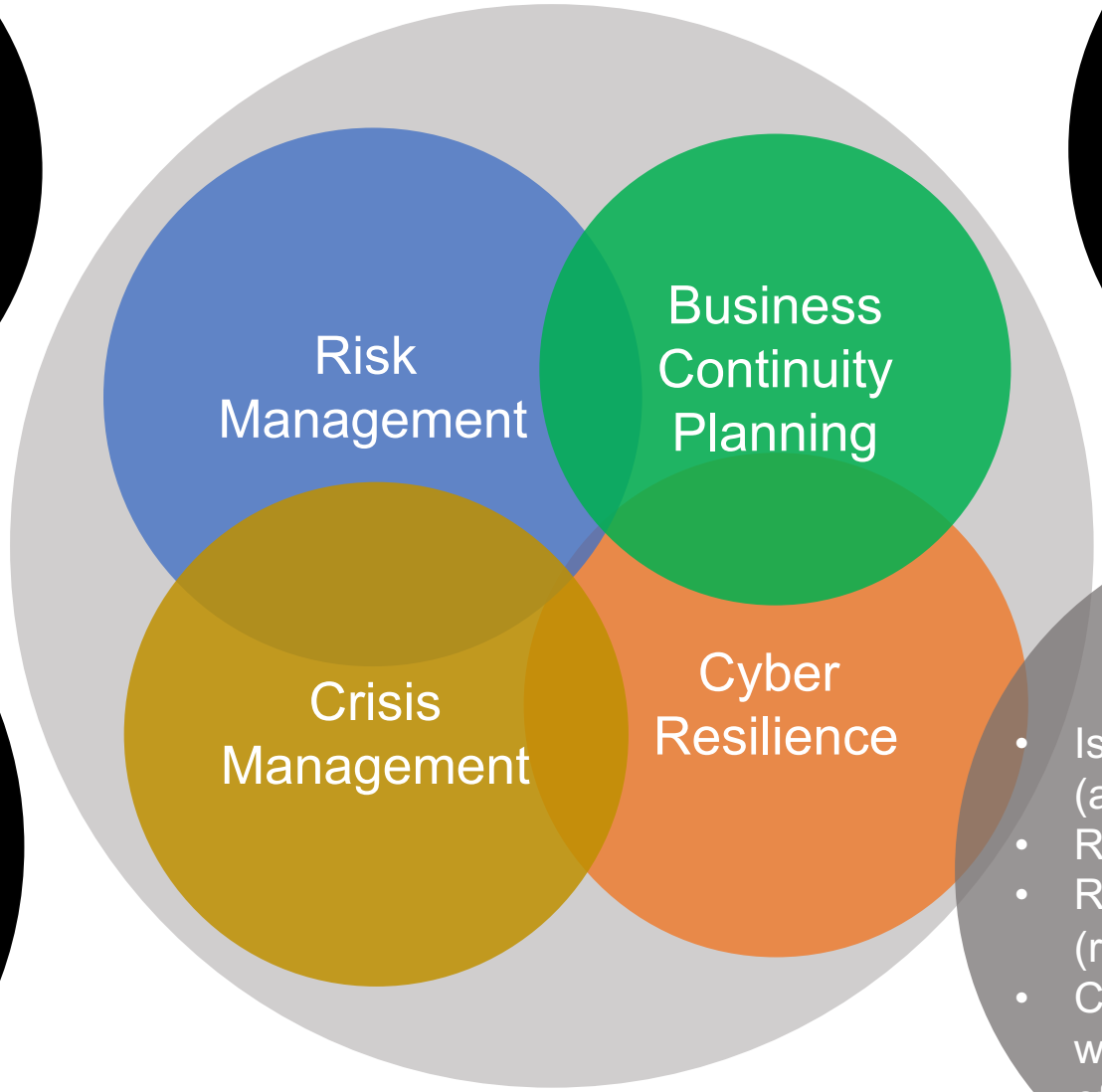
What is the chance of a superpower conflict in the next ten years? ____%

Strategic Scenario Gaps

- Invasion of countries
- Company/Org becoming a lawful target
- Sanctions & Boycotts

Tactical Situation Gaps

- Physical takeover of office facilities
- Employees moonlight in a cyber army



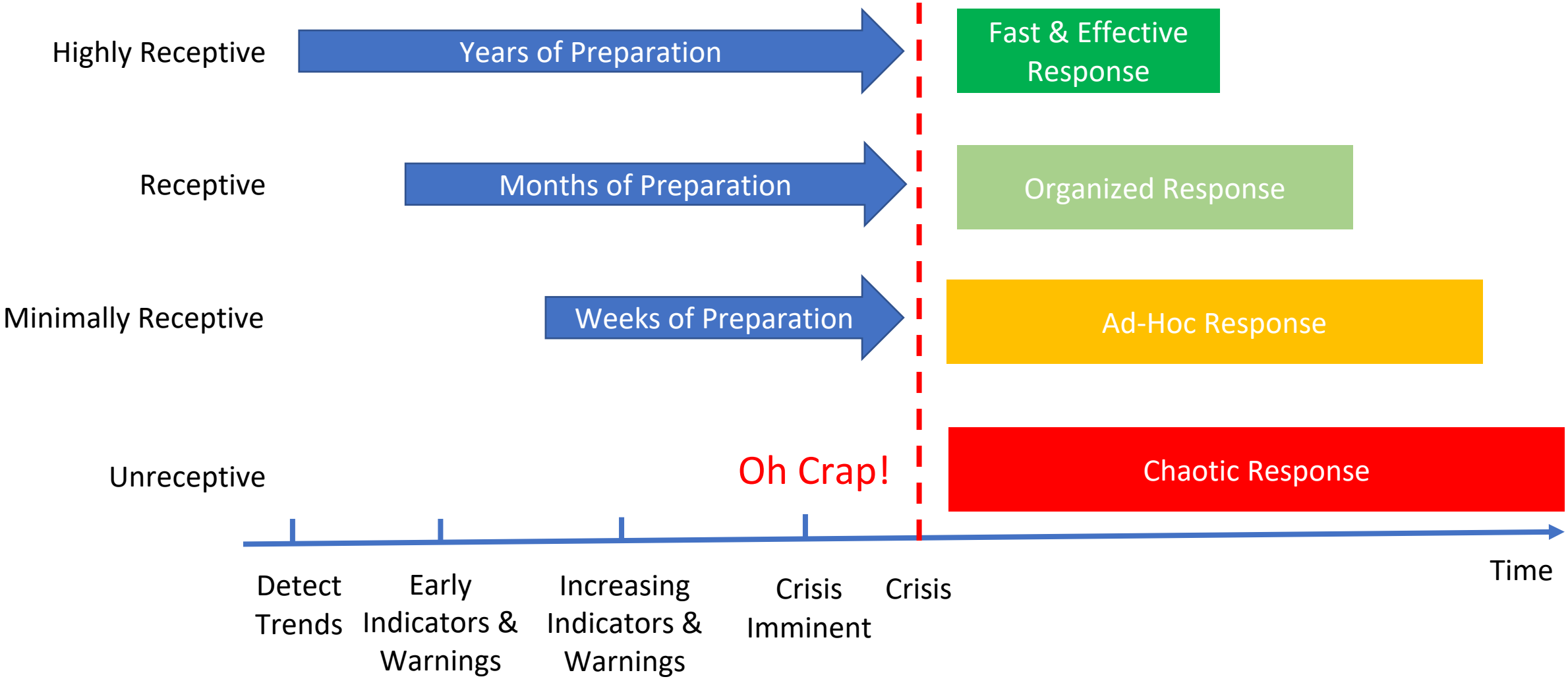
Action Gaps

- Intentional destruction of data/infrastructure
- Exiting markets
- Evacuating your people out of a combat zone
- Denying access to products and services from markets
- Offensive actions

Partial Overlap

- Isolation (after malware outbreak)
- Repair
- Retaking infrastructure (ransomware recovery)
- Communication w/stakeholders about loss of infrastructure

Receptiveness of Organizations



Convincing the Reluctant Organization

- OSINT
- ISACs
- Commercial Threat Intelligence
- Government Information Sharing
- Collective Defense
- **Your People**

Risk = Probability X Impact

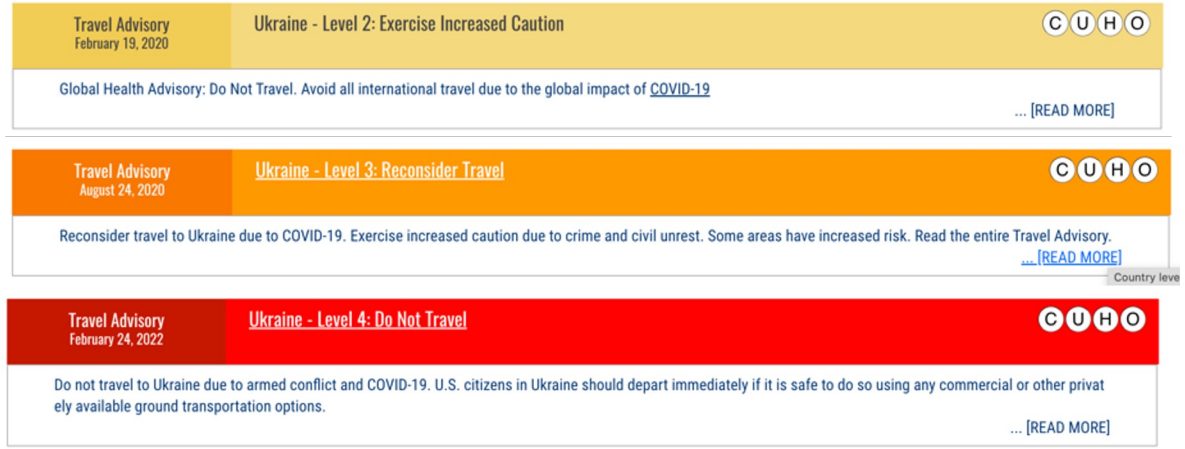
Developing Indications and Warnings (I&W)

"How did you go bankrupt?"
"Two ways. Gradually, then suddenly."
- Ernest Hemingway's
The Sun Also Rises

Examples
- Troops massing at the border
  - "It's just a training exercise"
- Preparatory DDOS attacks
- Suspicious network "outages"
- Air Defense systems go down
- Local national staff don't come to work
- …

Declassified Example: Evaluation of U.S. European Command's Warning Intelligence Capabilities

See also: Applying Indications and Warning Frameworks to Cyber Incidents, CyCon 2019.



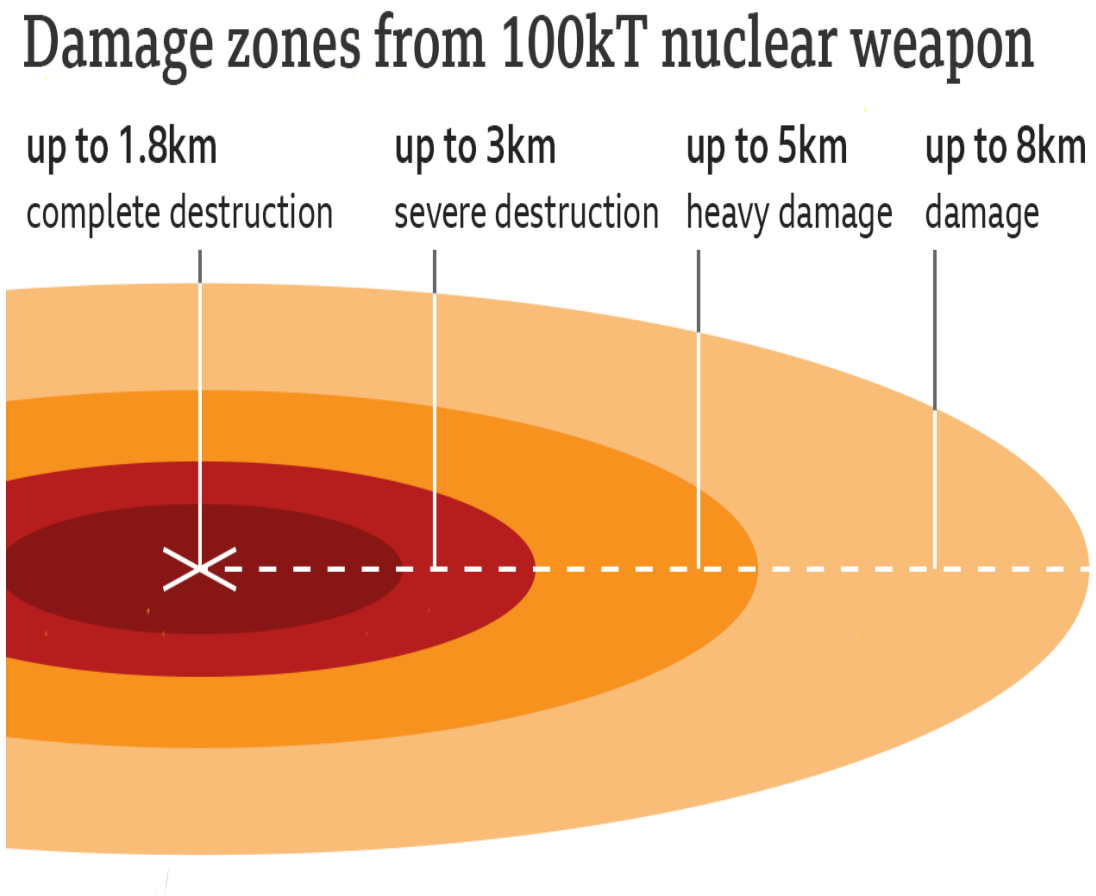
NEWS | Nov. 28, 2022

Before the Invasion: Hunt Forward Operations in Ukraine

By Cyber National Mission Force Public Affairs

FORT GEORGE G. MEADE, Md. – U.S. joint forces, in close cooperation with the government of Ukraine, conducted defensive cyber operations alongside Ukrainian Cyber Command personnel from December 2021 to March 2022, as part of a wider effort to contribute to enhancing the cyber resiliency in national critical networks.

“Blast Radius” – How Exposed Are We?



Exploitation Disclosure Virus Bulletin Article

- Direct Exposure
  - Organizations with offices in location
  - Organizations that may be targeted because they support organizations in the region
  - Organizations that may be targeted symbolically
- Secondary Exposure
  - Organizations with dependencies on third parties with any direct exposure
- Collateral Exposure
  - Global organizations may experience collateral effects (i.e. Stuxnet)

Business Down (Permanently)

Business not possible for foreseeable future

Partially In Scope

Civilization Down

Head to your compound. Fight for survival.

Read [When Sysadmins Ruled the Earth]

Out of Scope

Operations Up and Down

Staggering along

In Scope

Business Down (Temporarily)

Wait and see. Problems massive but temporary.

In Scope

Business as Usual

Stable environment for operations

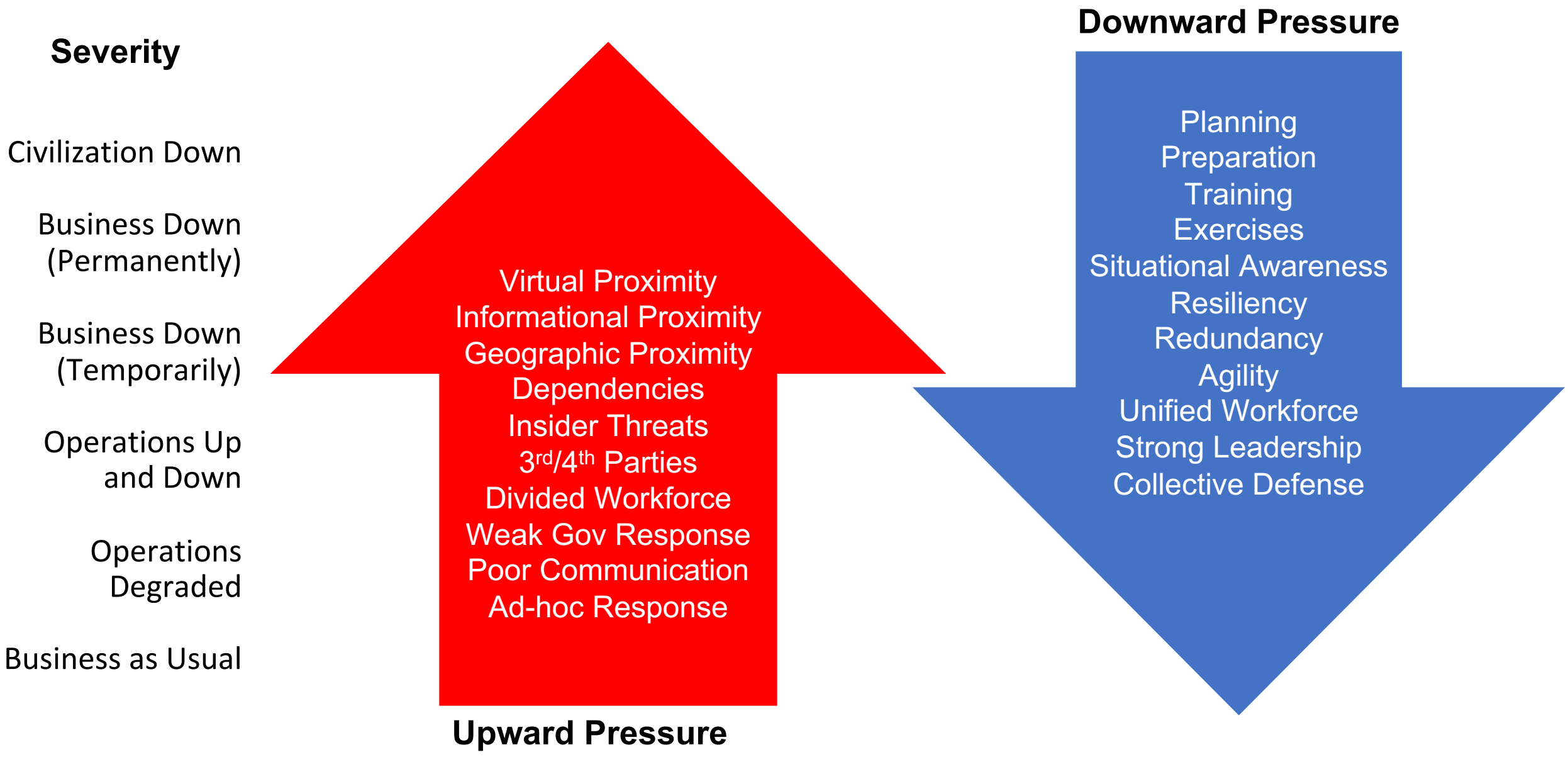
In Scope

Operations Degraded

Business still possible.

In Scope

Scoping the Problem: Stairway to Armageddon


Severity
Civilization Down
Business Down (Permanently)
Business Down (Temporarily)
Operations Up and Down
Operations Degraded
Business as Usual
Virtual Proximity
Informational Proximity
Geographic Proximity
Dependencies
Insider Threats
3rd/4th Parties
Divided Workforce
Weak Gov Response
Poor Communication
Ad-hoc Response
Upward Pressure
Downward Pressure
Planning
Preparation
Training
Exercises
Situational Awareness
Resiliency
Redundancy
Agility
Unified Workforce
Strong Leadership
Collective Defense

What is a War Plan?

2 CENTS PAY NO MORE!

Chicago Daily Tribune

THE WORLD'S GREATEST NEWSPAPER

FINAL

VOLUME C.—NO. 290 C THURSDAY, DECEMBER 4, 1941.—46 PAGES PRICE TWO CENTS

F. D. R.'S WAR PLANS!

REDS BEGIN NEW DRIVE TO BREAK VISE ON MOSCOW

Strike at Nazi Line South of Leningrad.

LEIBER TRADED TO GIANTS; CUBS GET BOWMAN

NEWS SUMMARY of The Tribune

WAR SITUATION.

HOUSE ADOPTS DRASTIC BILL TO BLOCK STRIKES

Goes to Senate on 252-136 Vote.

THE STRONGHOLD OF PEACE

WAR PROPAGANDA

THE MIDDLE WEST

ILL.

CHICAGO

OHIO

GOAL IS 10 MILLION ARMED MEN; HALF TO FIGHT IN AEF

Proposes Land Drive by July 1, 1943, to Smash Nazis; President Told of Equipment Shortage.

BY CHESLY MANLY.

"A war plan develops a concept to win a war militarily and politically; it is the detailed ways and means of an overarching strategy."

"The Department of Defense has no definition of 'war plan' according to its own doctrine. There are the Unified Command Plan, campaign plans, theaters of war, and regional theater strategies."

https://warroom.armywarcollege.edu/articles/war-plan/

Organizational War Plan

- Develops a concept to protect an organization's people, infrastructure and data while continuing business operations in the event of a major conflict.
- Plans may be a single generalized plan or multiple tailored plans based on projected scenarios.
- Should include analysis of allegiance during the conflict.

Examples of How to Prepare

- Build public-private partnerships in advance of conflict
- Put in place wartime legal authorities and liability protection
- Share threat intelligence
- Organize sector- and national-level wartime exercises

- Assess capabilities
- Determine vulnerabilities
- Enumerate & war game scenarios
- **Develop generic war plan and test**
- Develop situational awareness
- Develop counter-insider threat programs
- **(Develop scenario-specific plans)**

- Maintain situational awareness
- Task threat intelligence sources for I&W reporting
- Continually assess threat probabilities
- Track locations of people, infrastructure, data

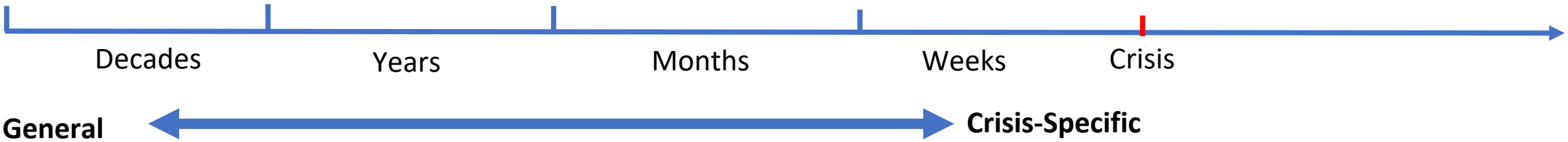
Attacker Planning and Preparation

- Long term planning
- Infiltrate sleepers

- Probe infrastructure
- Identify vulnerabilities
- Develop exploits
- Gain and maintain access
- Steal IP
- Surveil
- Develop leverage over employees
- Create dependencies whilst reducing their own
- Divide alliances
- Amass resources

- Maintain exploit database
- Activate sleepers
- Attempt to *create* insider threats
- Attempt to steal copies of company crisis plans
- Exercise leverage over employees
- Conduct influence campaigns
- Develop prioritized target lists

- Capture targets
- Exploit dependencies
- Degrade connectivity
- Conduct cyber, physical, and kinetic operations



Organizational Planning and Preparation

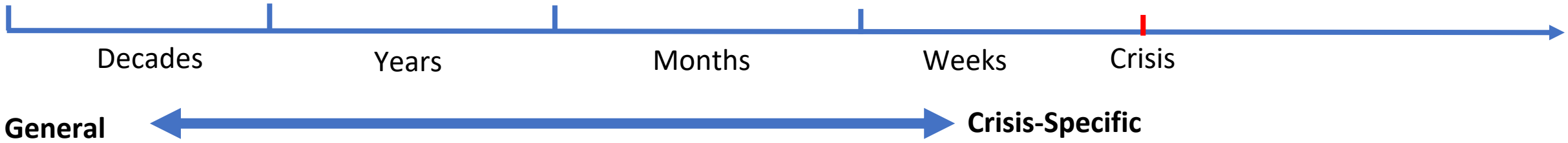
- Build resilient programs
- Create talented workforce

- Vet employees
- Train and Exercise
- Patch Vulnerabilities
- Conduct planning
- Build relationships
- Minimize dependencies

- Update war plan
- Tailored hunt operations
- Tailored training

- Disable/harden infrastructure
- Evacuate people
- Move, encrypt or wipe data
- Pivot to more secure infrastructure

- Continue operations
- Recover from attacks
- Leverage organizational capabilities to support war effort



Who should lead War Planning efforts?

In most organizations, no single function has a comprehensive perspective.

Core Team
- Business Continuity Planning
- Business Risk Management
- Cybersecurity

Extended Team
- Legal (International & Sanctions Compliance)
- Physical Security
- Relevant Operational Managers
- HR
- IT
- PR & Investor Relations
- Senior Strategic Leadership

In your org, who else should participate?

Who should lead War Planning efforts?

	Teams	Key Insights
Core Teams	**Business Continuity Planning**	Identifying scenarios where conflict may impact the organization Mapping regional dependencies Developing operational & IT resiliency plans
	Business Risk Management	Determining the financial impact of downtime and the cost of contingency plans
	Cybersecurity	Threat intelligence Identifying vulnerabilities and attack vectors Threat modeling
Extended Teams	**Legal**	International legal obligations Sanctions compliance
	Facilities Mgmt & Physical Security	Facility security and contingency planning
	Relevant Operational Managers	Identifying operational dependencies & developing alternatives Executing changes
	HR	Identifying employees who may be impacted by conflict or changes in laws Internal communications about the organization's posture and planning
	PR & Investor Relations	Communications plans & updates
	Senior Strategic Leadership	Financial support, resourcing, and prioritization for contingency planning Decisions to exit markets Decisions to modify products or service offerings
	IT	Network infrastructure Resiliency / Backups

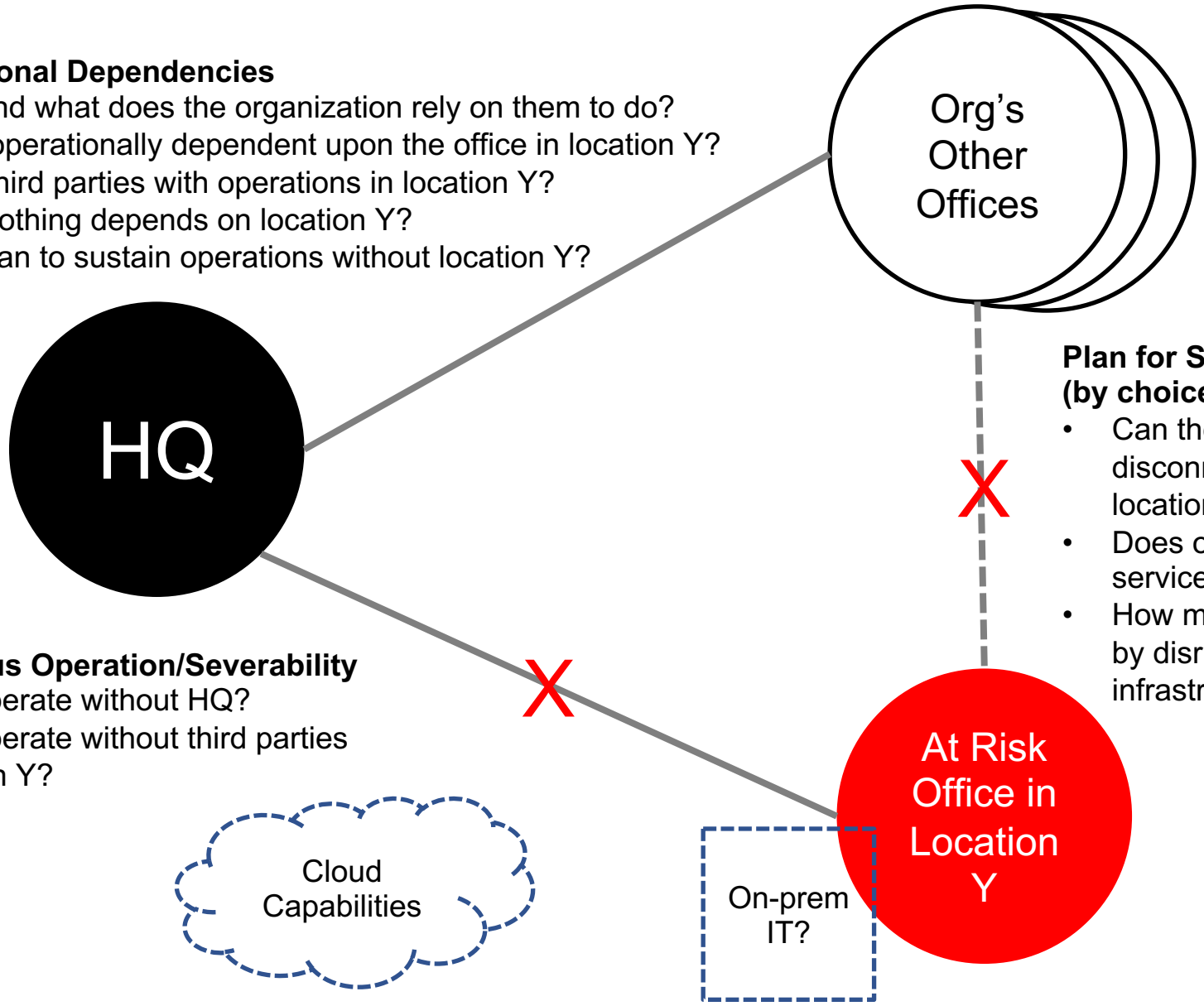
DIMEFIL - Multiple Sources of National Power

Power Sources	Applications	Effects
Diplomacy	Changes to trade agreements New sanctions Denied parties	Legal prohibitions on cooperation & trade Taxes & tariffs International travel restrictions & prohibitions **Employment restrictions & prohibitions** Immigration restrictions
Information	Propaganda Disinformation	Boycotts Consumer confusion **Creation of insider threats**
Military	Kinetic operations	Destruction of infrastructure Commandeering/Repurposing of infrastructure Curfews & internal travel restrictions **Personnel who are drafted** Personnel who are interned or killed
Economic	Voluntary boycotts Companies that exit a market	Loss of access to third parties & infrastructure
Financial	Changes in sponsorship for government programs	Loss of programs
Intelligence	Spying	Compromises of computer systems and networks
Law Enforcement	Crackdowns on dissident activity	**Arrests of personnel**

Operational Interdependencies & Resiliency

Plan for Severing of Operational Dependencies

- Who works in location Y and what does the organization rely on them to do?
- Is HQ or another location operationally dependent upon the office in location Y?
- Does HQ depend on any third parties with operations in location Y?
- Can that be reworked so nothing depends on location Y?
- What is the contingency plan to sustain operations without location Y?



Plan for Severing of IT Infrastructure (by choice or not)

- Can the office in location Y be disconnected from HQ and other locations at the network level?
- Does office have separate IT services/infrastructure?
- How might location Y be impacted by disruptions to local infrastructure?

Plan for Autonomous Operation/Severability

- Can location Y operate without HQ?
- Can location Y operate without third parties outside of location Y?

Infrastructure

Situation	Effect/Action	Preparatory Actions
Damaged	Repair, Replace	Off-site backups
		Spare parts
		“Break glass” admin logins
		Procedures suitable for third parties
	Substitute	Cloud infrastructure
		Satellite communication links
Commandeered	Destroy	Pre-planned and tested destruction procedures Defcon 19 - Emergency Data Destruction https://www.youtube.com/watch?v=1M73USsXHdc Defcon 23- Further Explorations in Data Destruction https://www.youtube.com/watch?v=-bpX8YvNg6Y
	Deny	Reversable destruction procedures
	Isolate	Remote choke points where interconnectivity can be removed
	Repurpose	See: Superpowers

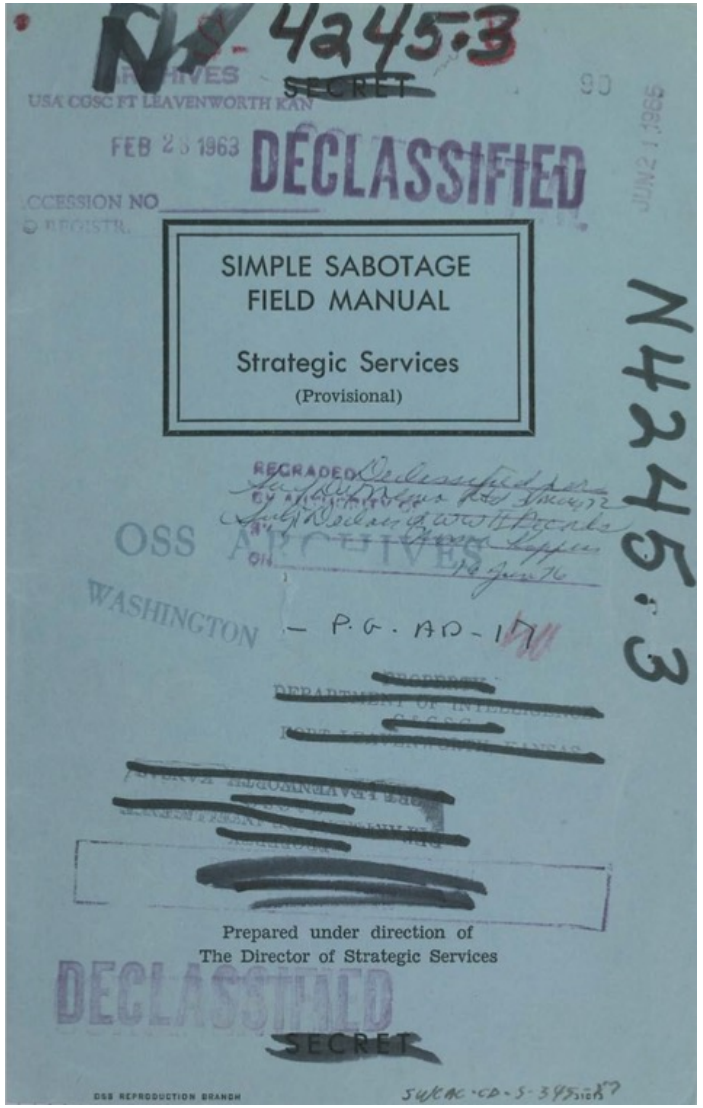
People

Your people aren't John Wick

- Family members in combat zone, business partners, local national employees, contractors
- Your office's physical security isn't designed to stop an invading army
- Best practice is for foreigners to get out early
  - Another is to go to embassy for help
- Non-combatants and theoretically protected under Geneva Convention and Law of Armed Conflict, until...
- Insider threat risk is heightened
- **Special crisis preparedness training may be useful**

https://www.denofgeek.com/movies/best-john-wick-fight-scenes-ranked/

From Wartime Defense to Wartime Offense



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

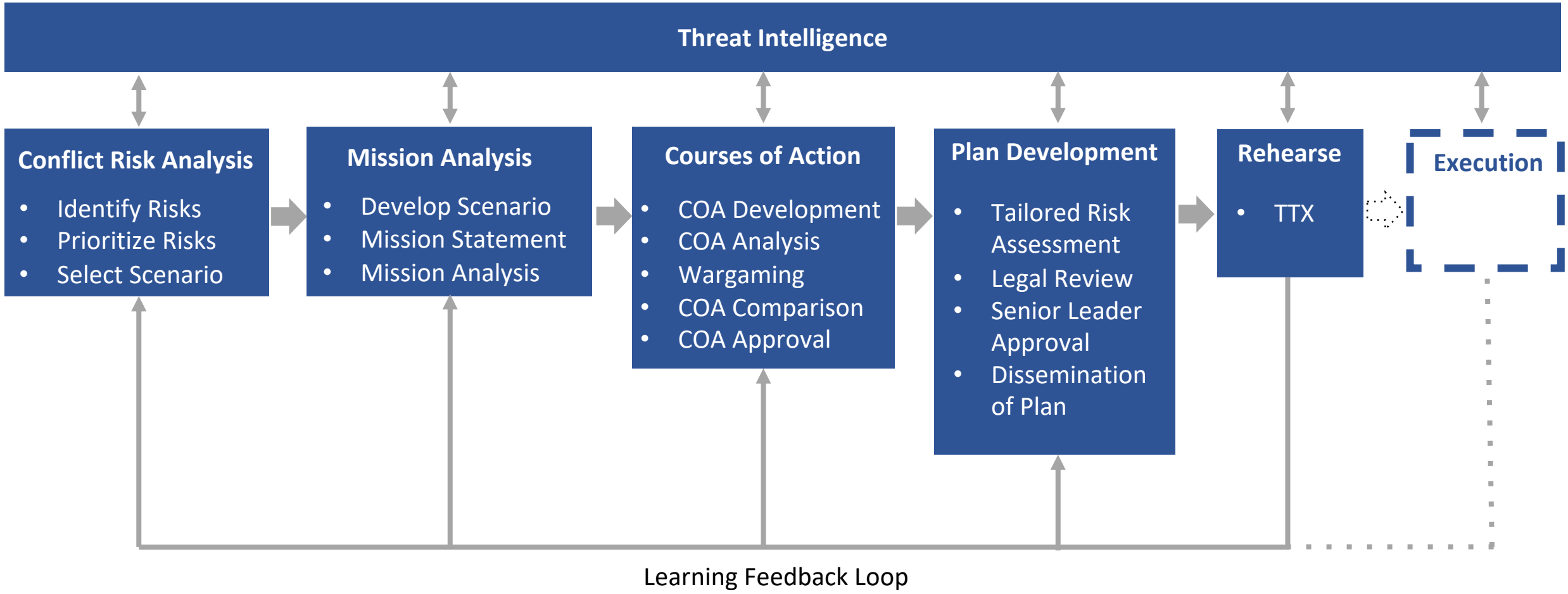
https://www.verzetsmuseum.org/en/world-war-ii-in-the-netherlands

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

What are your organization's Superpowers?

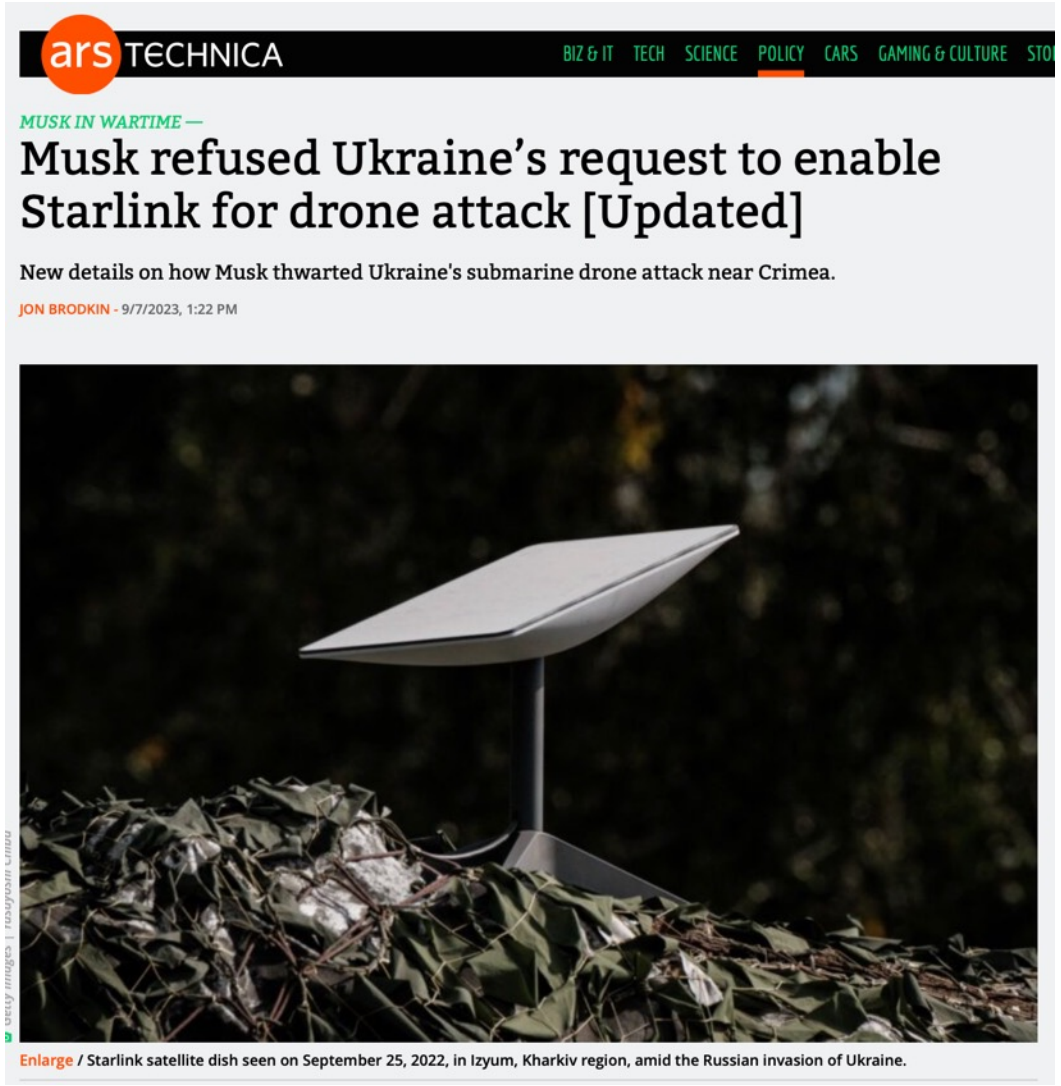
Military Planning and Decision Making Process



Key Takeaways from MDMP

- Clear chain of command – put someone in charge
- Clear goals and objectives
- Careful planning of what to do and who will do it
- Critical analysis of the plan to identify flaws
  - Wargaming
  - Risk analysis
- Testing/Rehearsal
- Senior leadership support and buy-in
- Legal Review (Red Cross LOAC)
- Feedback and learning from experience

Organizational Cohesion, Disruption, and Destruction



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

MUSK IN WARTIME —

Musk refused Ukraine's request to enable Starlink for drone attack [Updated]

New details on how Musk thwarted Ukraine's submarine drone attack near Crimea.

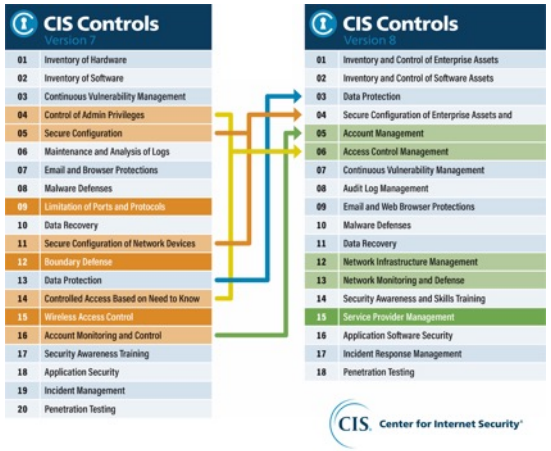
JON BRODKIN - 9/7/2023, 1:22 PM

Enlarge / Starlink satellite dish seen on September 25, 2022, in Izyum, Kharkiv region, amid the Russian invasion of Ukraine.

- Picking sides vs. neutrality
- Organizational political stance
- Employee, donor and customer allegiances
- Social media
- Patriotism or lack thereof
- Global multinationals
- Support to government
- **Wars will tear apart some organizations**

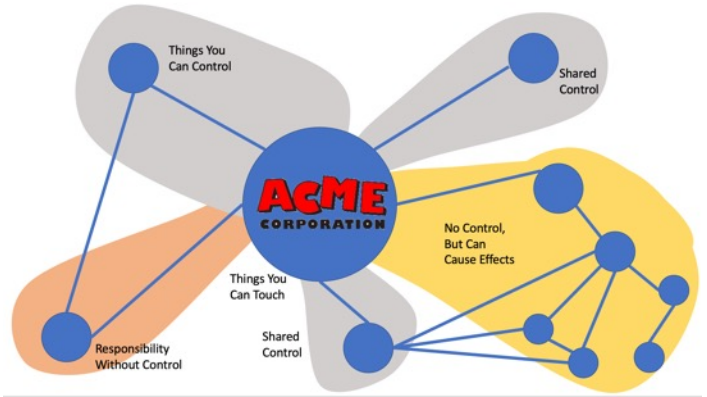
Related Work to Explore

Security Controls



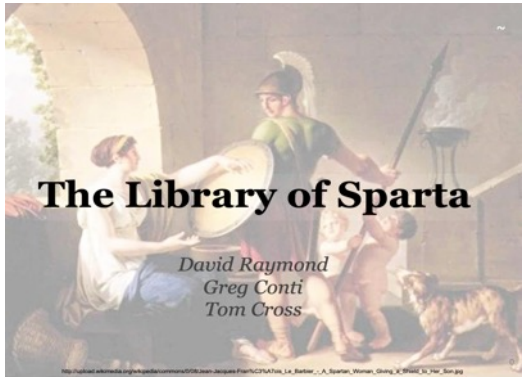
[CIS Controls]

Multidomain Attack Surface Analysis



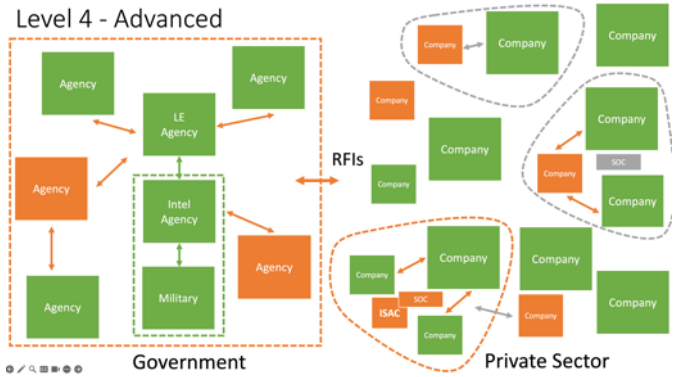
Comprehensive Cross-Domain Enterprise Threat Exposure Analysis, BSides Delhi (Video)

Military Strategy and Tactics for Cybersecurity



The Library of Sparta, Black Hat USA (Video)

Collective Defense



Operational Templates for State-Level Attack and Collective Defense of Countries Black Hat USA (Video)

War Planning Self-Assessment Checklist

Analyzes

- Infrastructure and Technical
- Intelligence and Awareness
- Plans and Policies
- Command and Control
- HR / People
- Training
- Legal
- Resourcing
- Operational Resilience

- Pick a major conflict scenario
- Estimate **Probability** of scenario
- Estimate **Exposure and Impact** of scenario
- Creative Commons license
- Thank you to Chris Chiras

Visit Kopidion.com to download*

* We are not harvesting data on this website, it's just a download

Questions???

Greg Conti

Tom Cross

KOPIDION™

info@kopidion.com

Takeaways

- The probability of a large-scale conflict in the next ten years isn't zero.
- The probability is high enough and the implications serious enough to merit deliberate planning at the organizational-level now.
- Planning is essential. Organizations need to be proactive rather than reactive when preparing for future conflicts.
- Organizations must have plans that consider the potential of a large-scale conflict in order to protect people, data, infrastructure and business operations