

An aerial photograph of a high-tech facility, possibly a military or intelligence installation. The facility is enclosed by a high white wall with a crenelated top. Inside the wall is a large, flat, yellow field. Several white buildings are scattered around the perimeter and within the field. A red vehicle is parked on a road to the left. The overall scene suggests a secure, high-tech environment.

War Planning for Tech Companies

Greg Conti
Tom Cross

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.

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

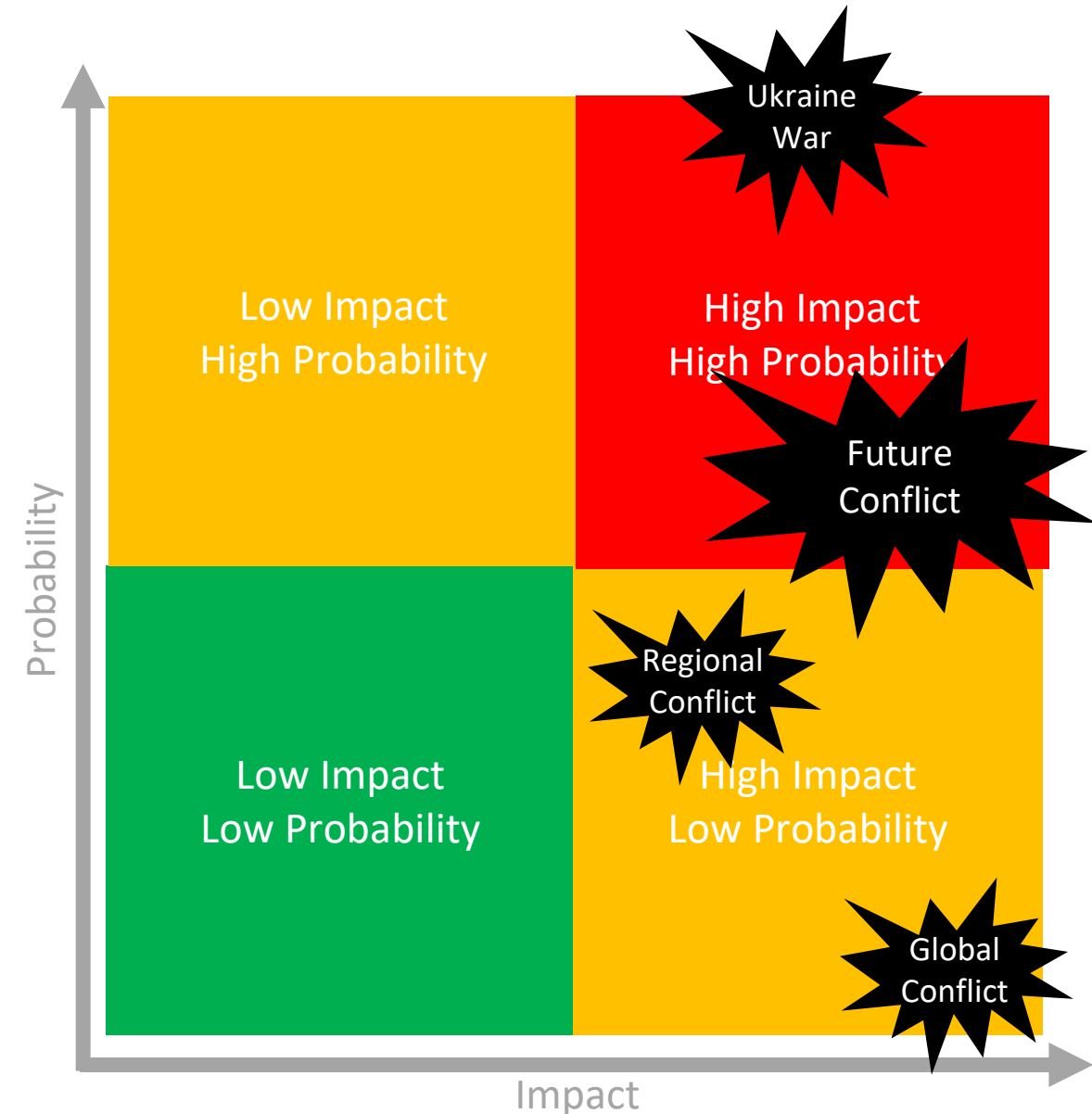
Companies Thought They Could Ignore Geopolitics. Not Anymore.

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?**

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."

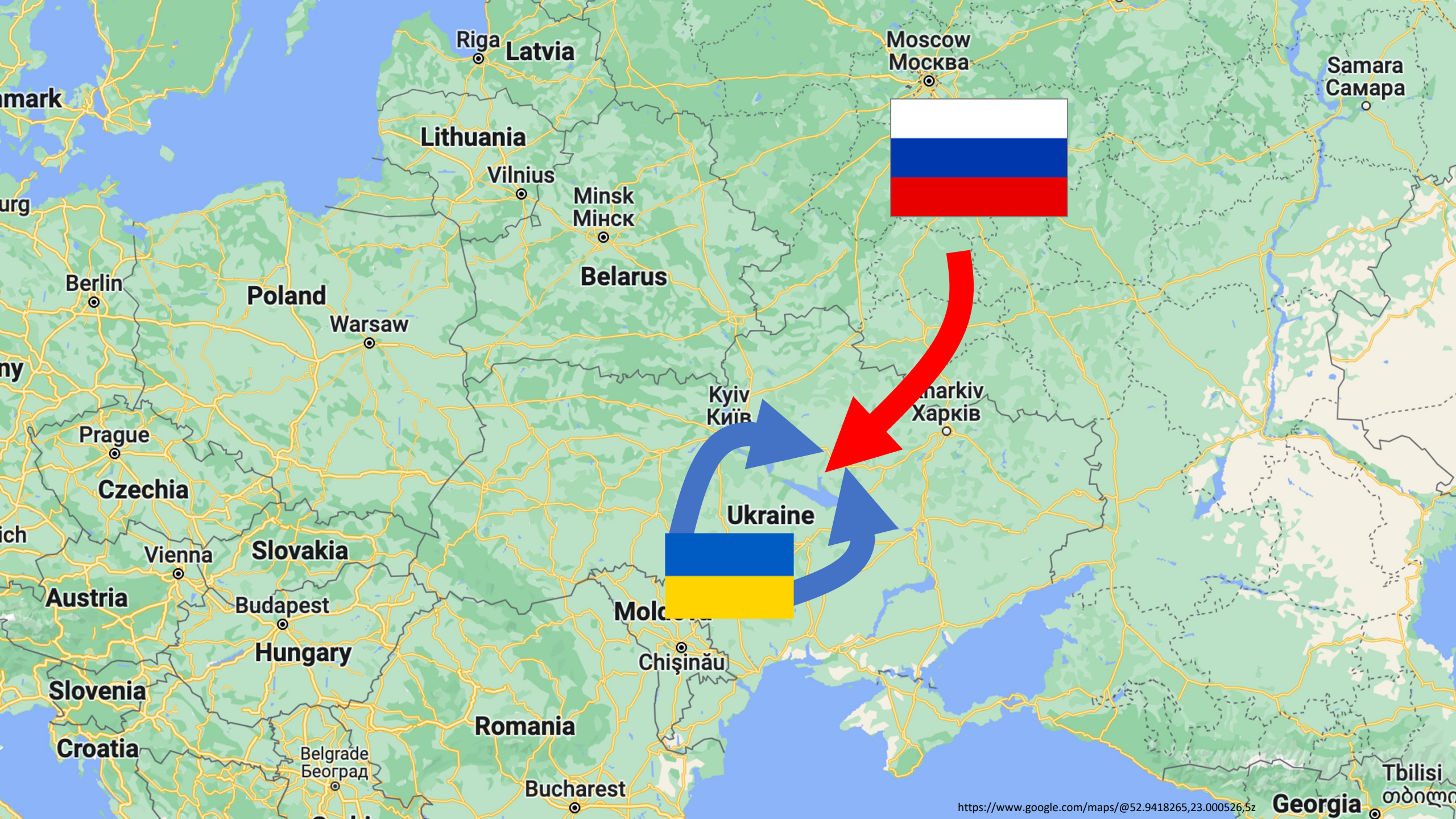
By SYDNEY J. FREEDBERG JR. on April 11, 2023 at 2:08 PM

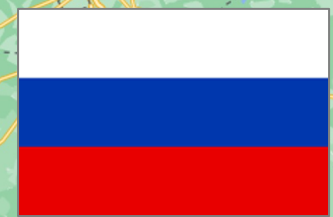
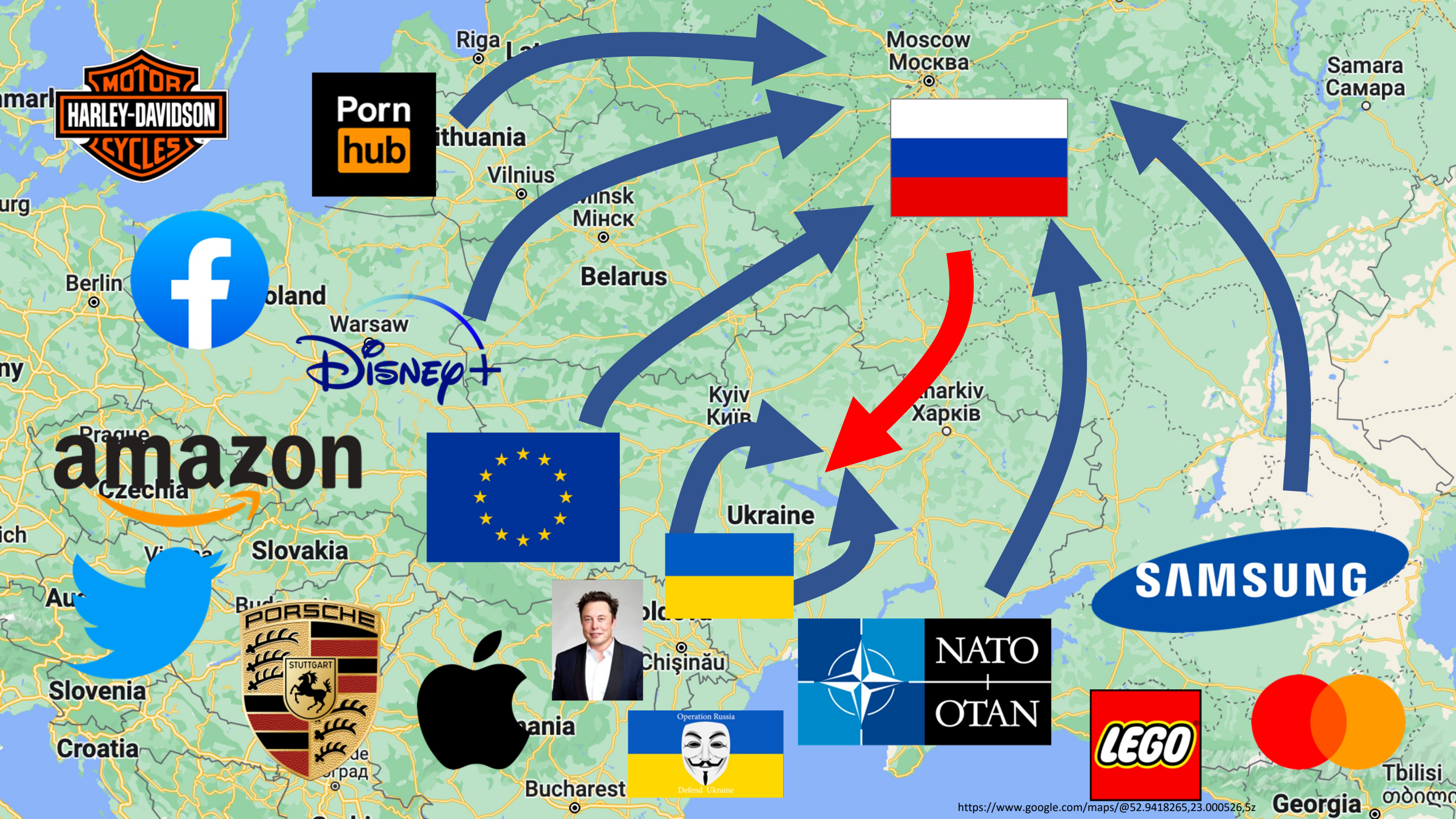


Robert Joyce, director of cybersecurity at the National Security Agency (NSA), speaks during a Senate Armed Services Subcommittee hearing in Washington, D.C., U.S., on Wednesday, April 14, 2021. (Al Drago/Bloomberg via Getty Images)

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

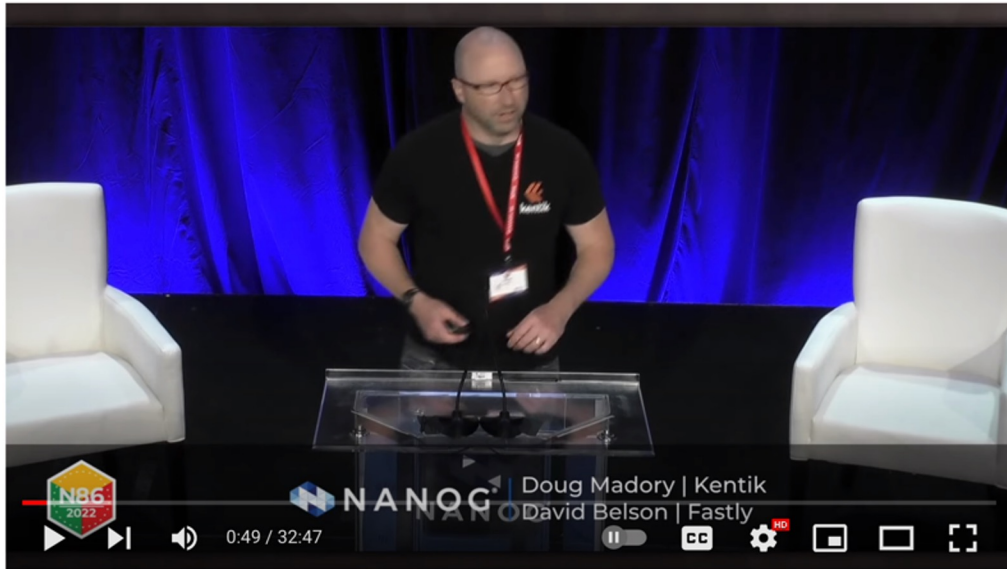
“You want to be planning now.”







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

Risk Management

Business Continuity Planning

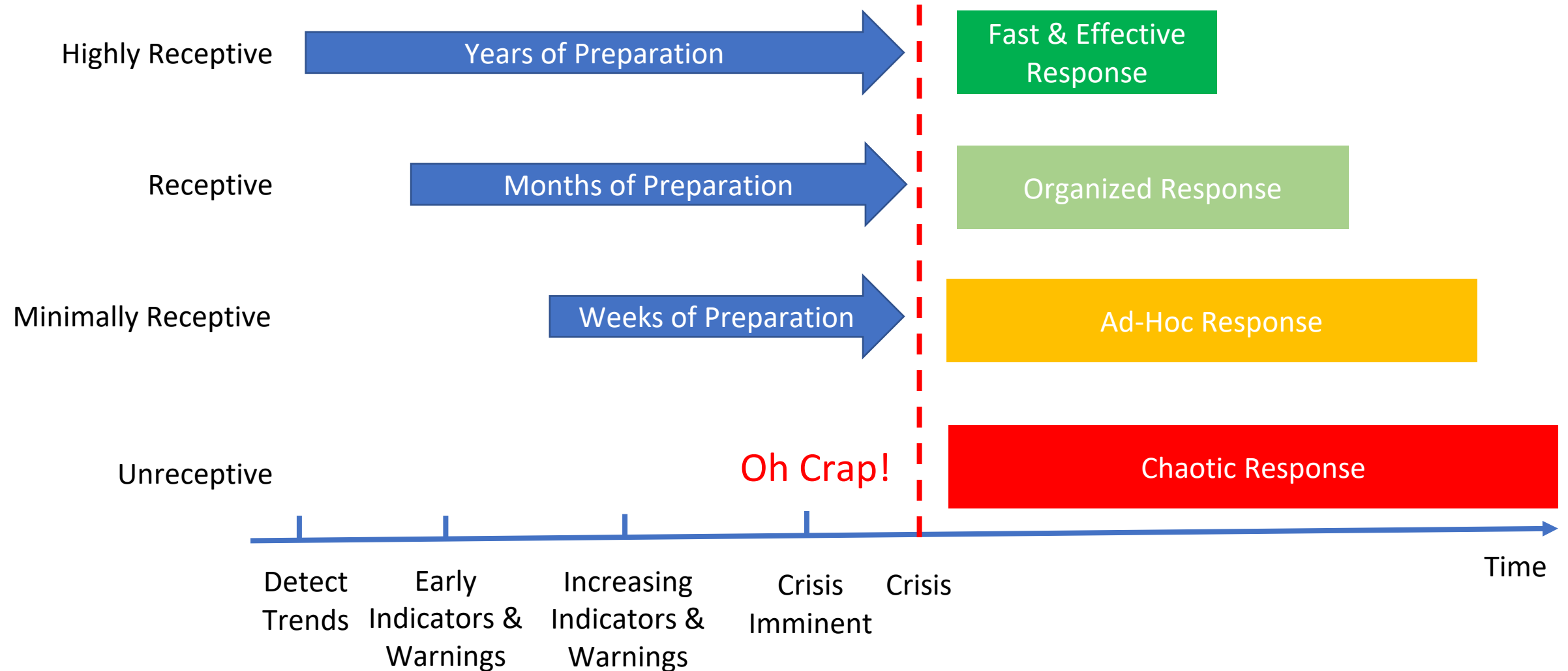
Crisis Management

Cyber Resilience

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**

$$\text{Risk} = \text{Probability} \times \text{Impact}$$

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.

Travel Advisory February 19, 2020	Ukraine - Level 2: Exercise Increased Caution	C U H O
Global Health Advisory: Do Not Travel. Avoid all international travel due to the global impact of COVID-19 .		... [READ MORE]

Travel Advisory August 24, 2020	Ukraine - Level 3: Reconsider Travel	C U H O
Reconsider travel to Ukraine due to COVID-19. Exercise increased caution due to crime and civil unrest. Some areas have increased risk. Read the entire Travel Advisory.		... [READ MORE]

Travel Advisory February 24, 2022	Ukraine - Level 4: Do Not Travel	C U H O
Do not travel to Ukraine due to armed conflict and COVID-19. U.S. citizens in Ukraine should depart immediately if it is safe to do so using any commercial or other privately available ground transportation options.		... [READ MORE]



NEWS | Nov. 28, 2022

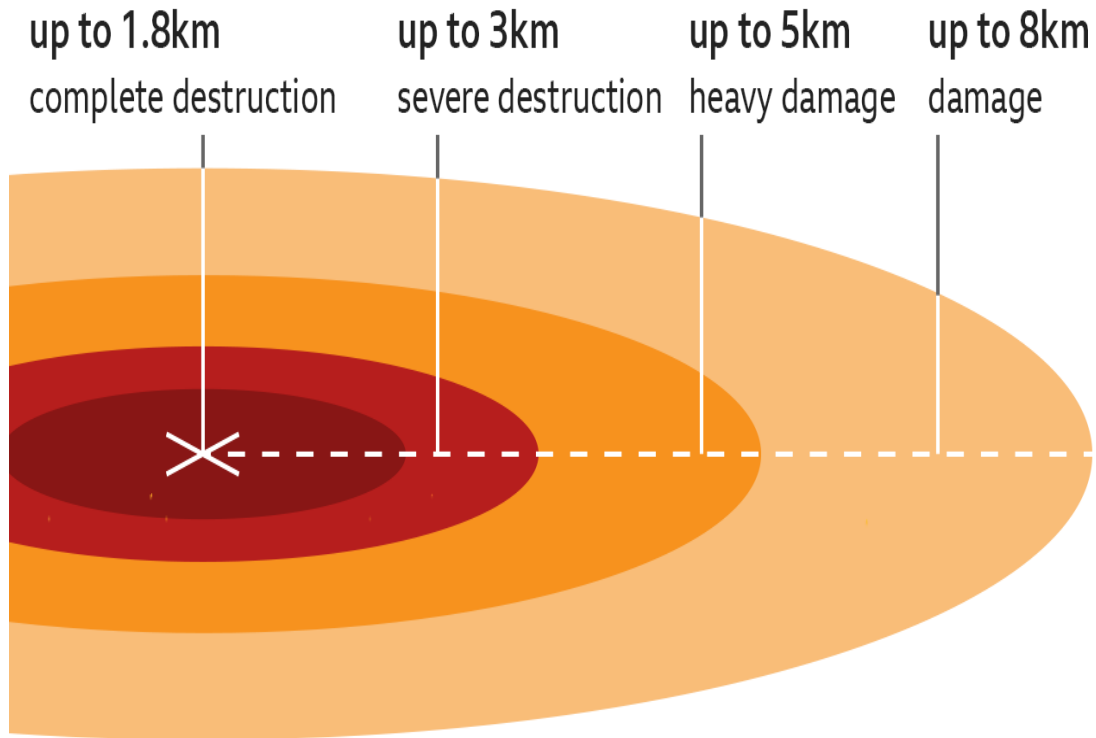
Before the Invasion: Hunt Forward Operations in Ukraine

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?

Damage zones from 100kT nuclear weapon



[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

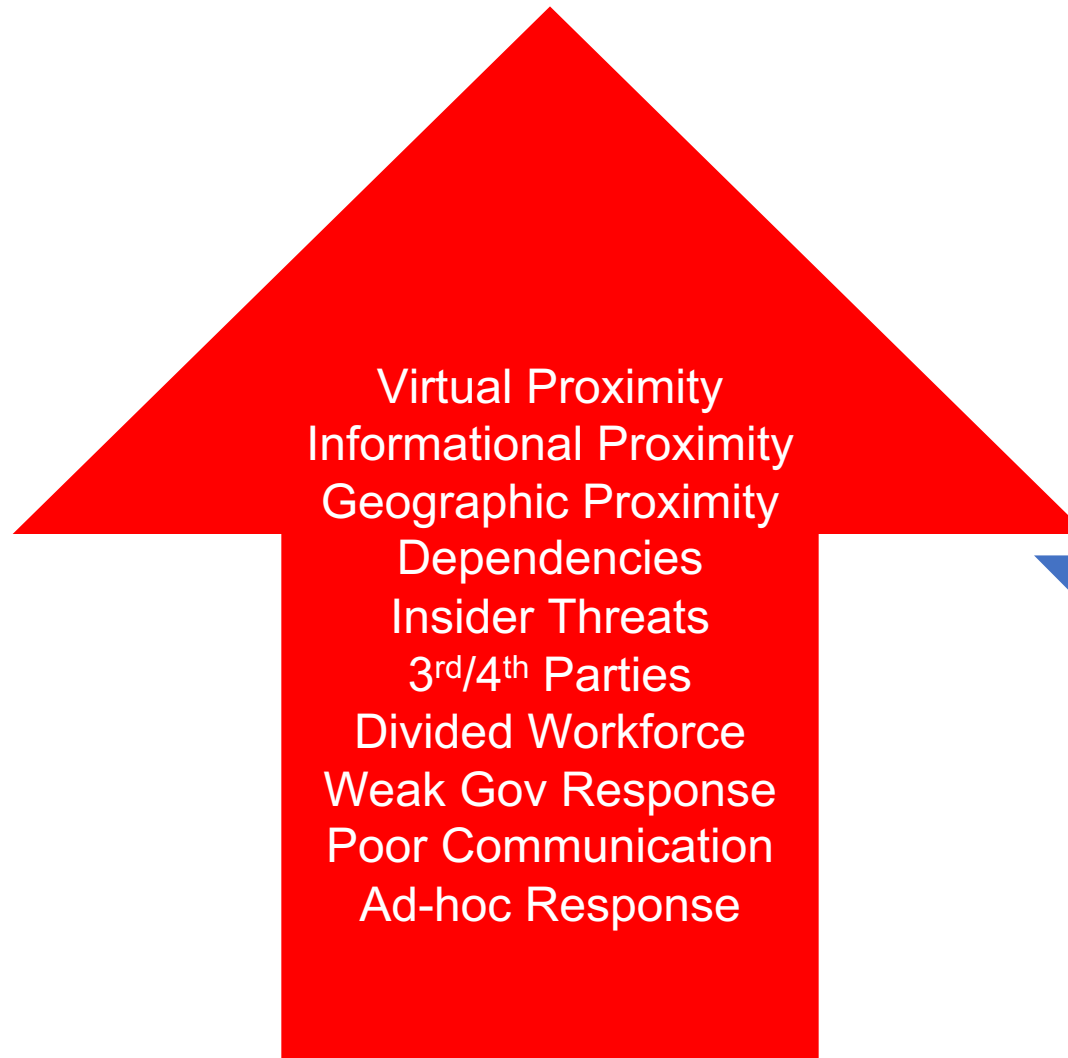
Business Down
(Permanently)

Business Down
(Temporarily)

Operations Up
and Down

Operations
Degraded

Business as Usual



Upward Pressure

Downward Pressure



What is a War Plan?



“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.

Strategic (Country-level)

Operational (Enterprise-level)

Tactical (SOC/Team-level)

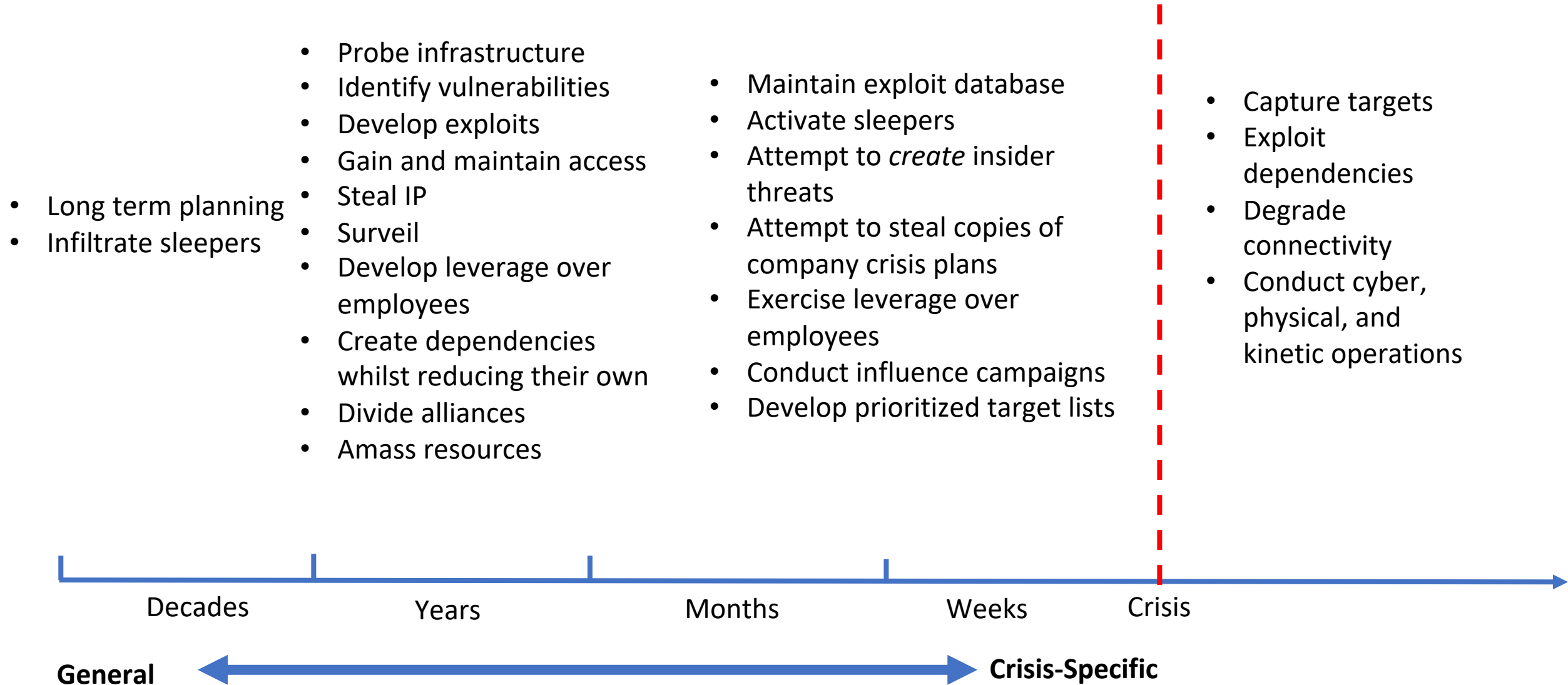
Examples of How to Prepare

- 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

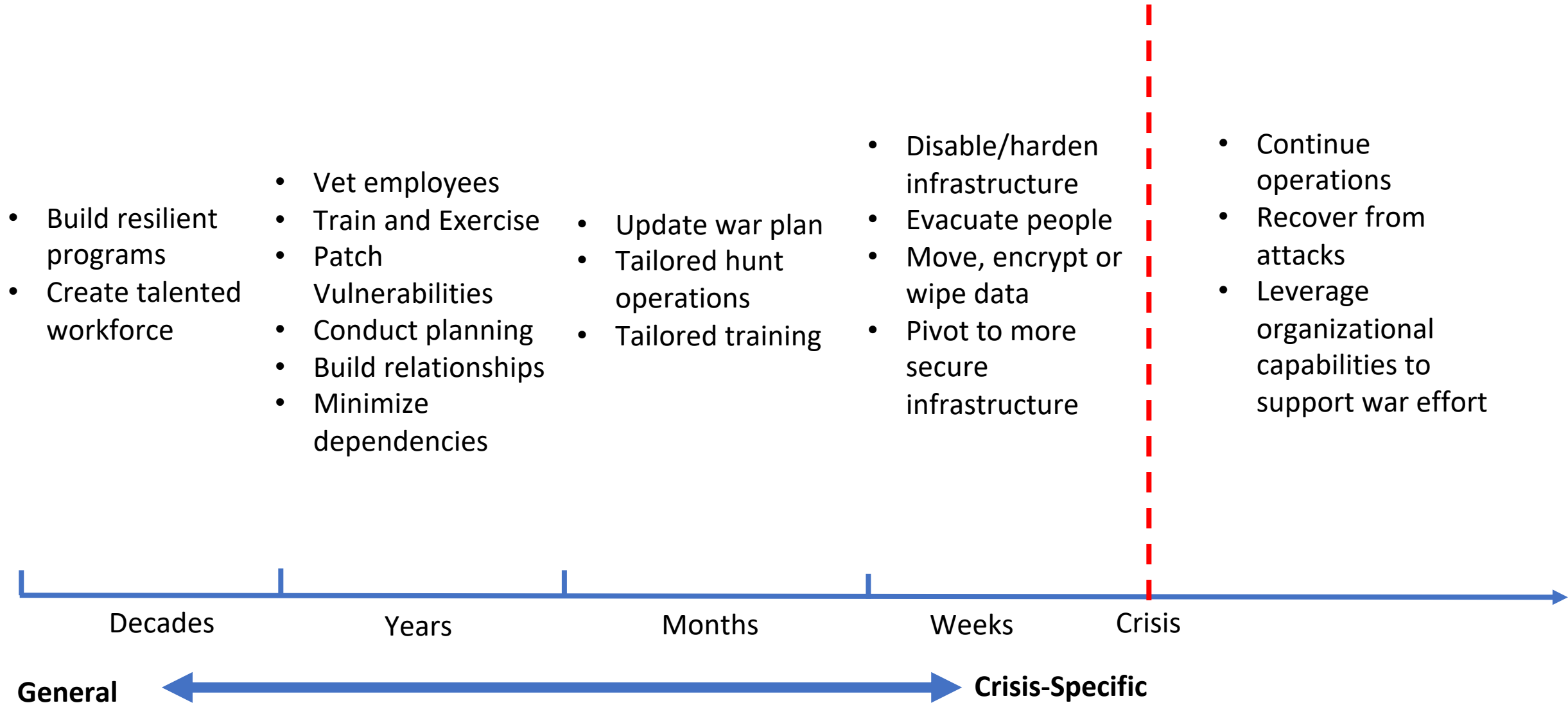
- Assess capabilities
- Determine vulnerabilities
- Enumerate & war game scenarios
- **Develop generic war plan and test**
- Develop situational awareness
- Develop counter-insider threat programs
- **(Develop scenario-specific plans)**

- 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



Organizational Planning and Preparation



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

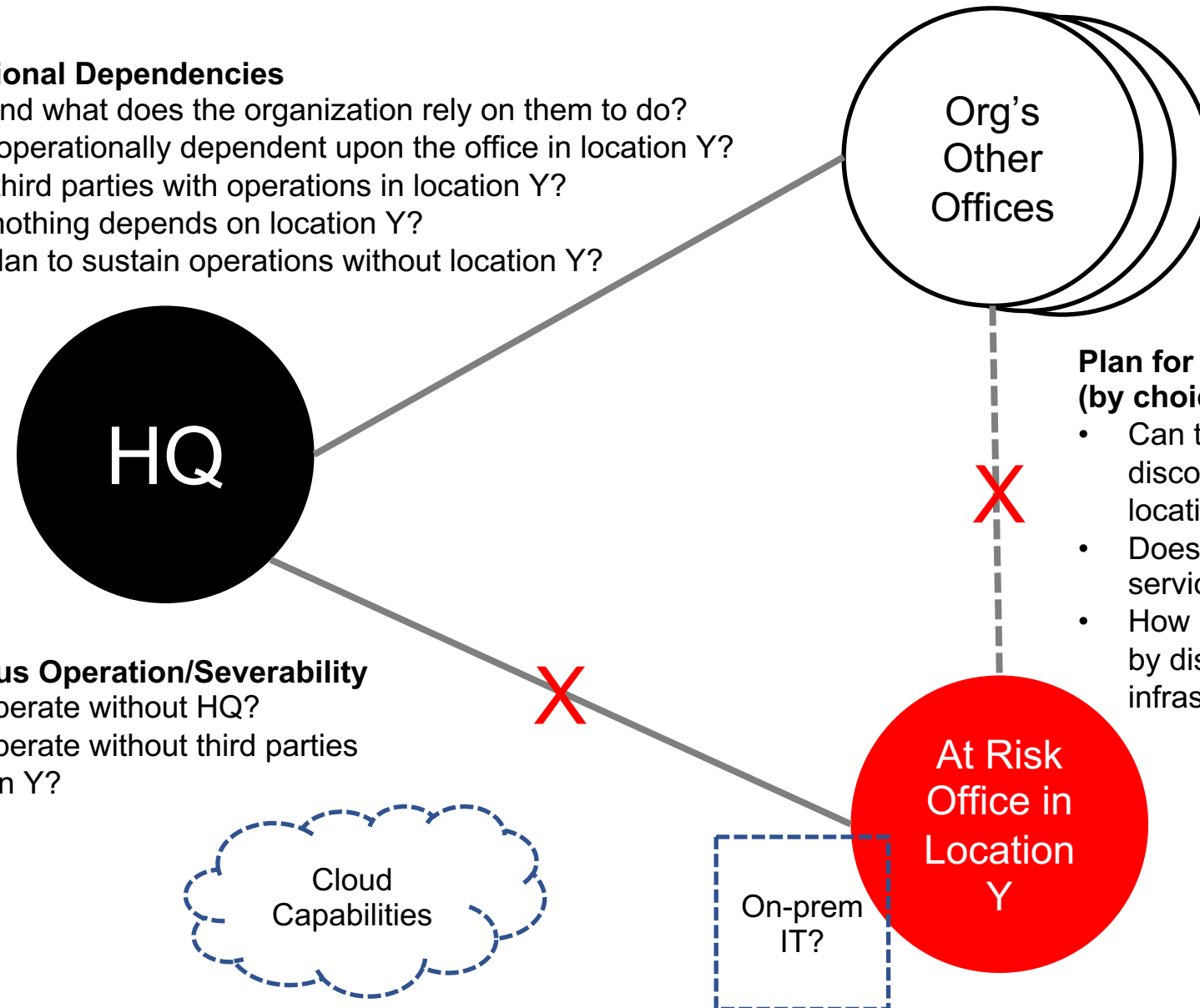
- Who works in location Y and what does the organization rely on them to do?
- Is HQ or another location operationally dependent upon the office in location Y?
- Does HQ depend on any third parties with operations in location Y?
- Can that be reworked so nothing depends on location Y?
- What is the contingency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

Plan for Autonomous Operation/Severability

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



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	Reversible destruction procedures
	Isolate	Remote choke points where interconnectivity can be removed
	Repurpose	See: Superpowers

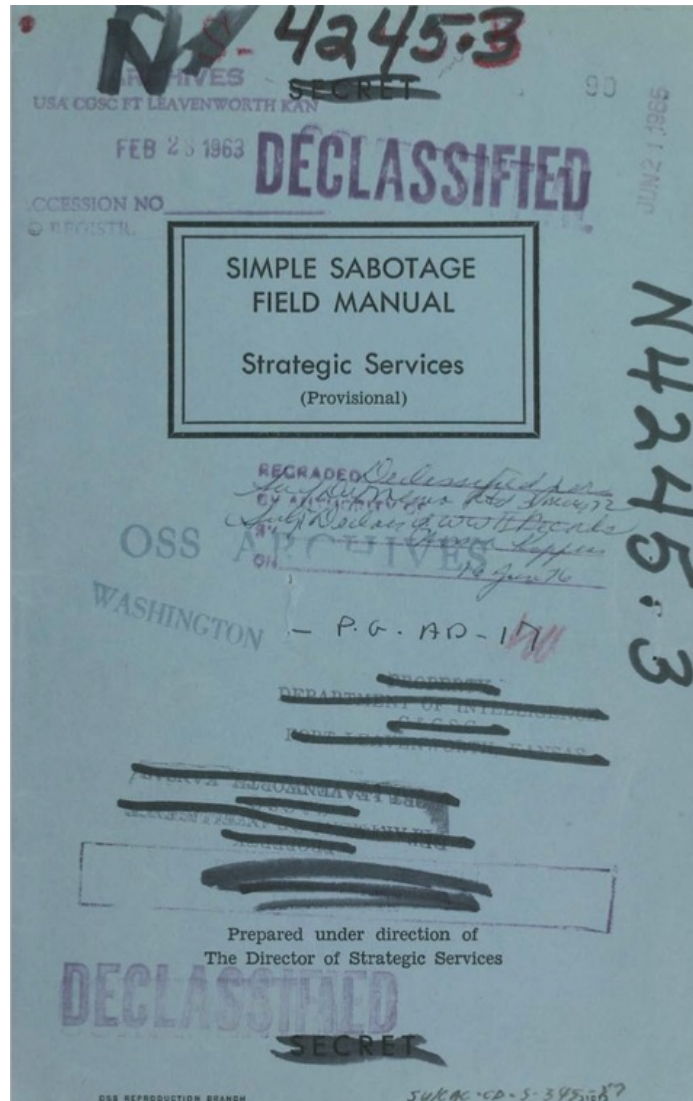
People



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**

From Wartime Defense to Wartime Offense



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



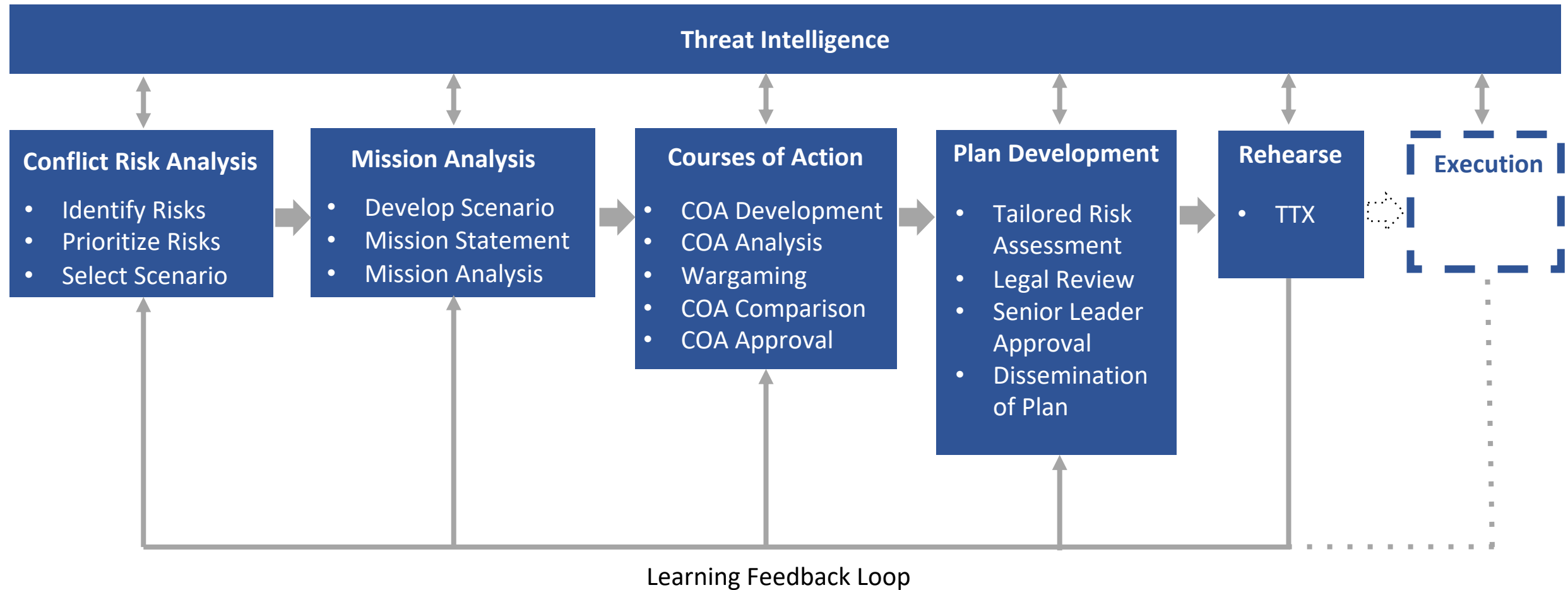
<https://www.verzetsmuseum.org/en/world-war-ii-in-the-netherlands>

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

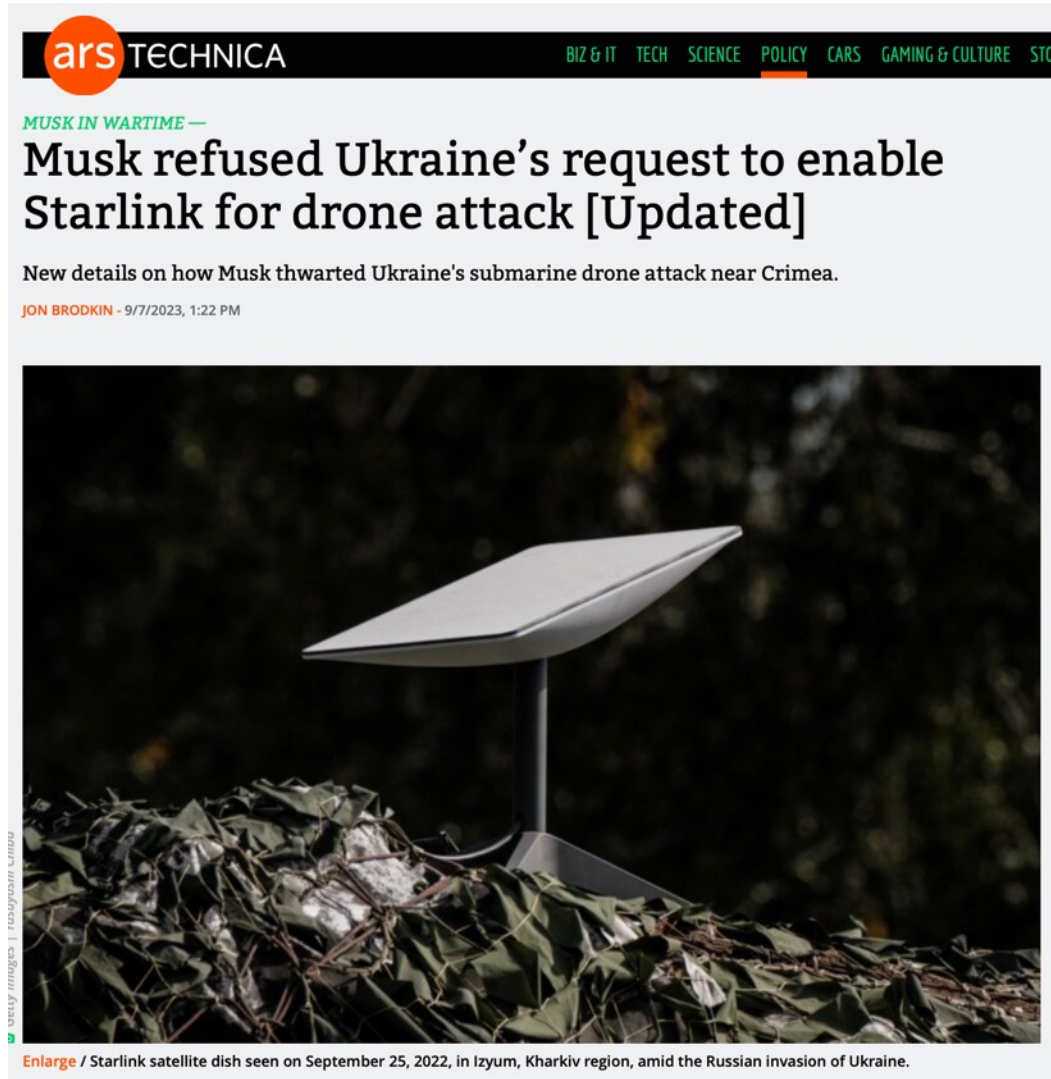


Key Takeaways from MDMP

- 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



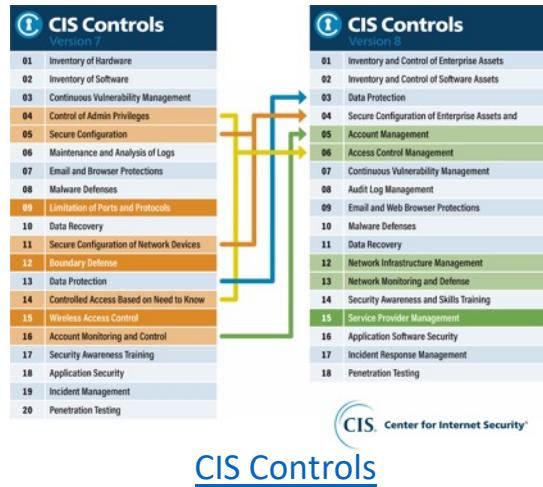
Organizational Cohesion, Disruption, and Destruction



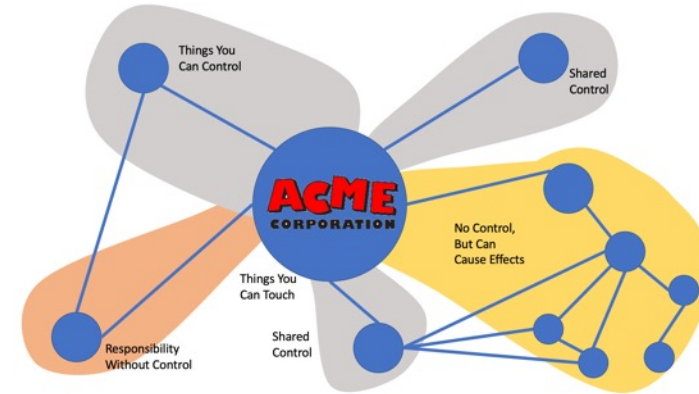
- Picking sides vs. neutrality
- Organizational political stance
- Employee, donor and customer allegiances
- Social media
- Patriotism or lack thereof
- Global multinationals
- Support to government
- **Wars will tear apart some organizations**

Related Work to Explore

Security Controls



Multidomain Attack Surface Analysis



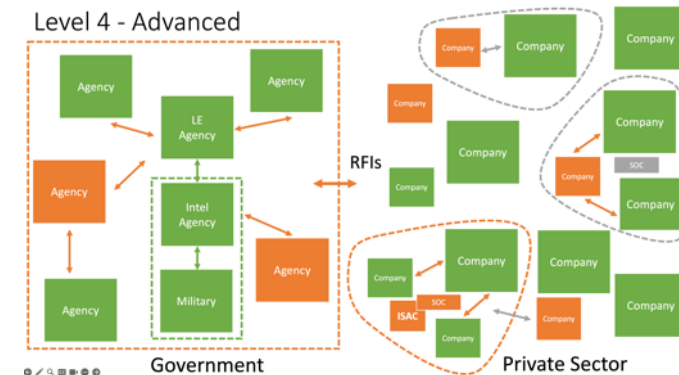
Comprehensive Cross-Domain Enterprise Threat Exposure Analysis, BSides Delhi ([Video](#))

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



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

Analyzes

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

Visit kopidion.com/workshop.html
to download*

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

Questions???



Greg Conti



Tom Cross



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