A Typhoon In A Teacup? Evaluating Reporting On High-Profile Threats

Joe Slowik

Disclaimer

The Following Commentary Represents The Author’s Own, Personal Reflections On The Associated Topics & Is Not Associated With Any Employer Or Other Organization

Agenda

- Background: Volt Typhoon
- Defender’s Dilemma
- Information Sharing & Disclosure
- Making Decisions
- Lessons & Implications

Volt Typhoon

What Is Volt Typhoon?

Volt Typhoon

What Is Volt Typhoon?

Volt Typhoon

PRC-Linked Threat Actor Active Since At Least 2021*

Targeting Critical Infrastructure Entities In The US, Related Entities

Assessed To Focus On Preparation & Prepositioning For Disruptive Attacks

Theoretically Linked To Potential Taiwan Strait Scenario To Deter Or Disrupt US Support To The Country Of Taiwan

Defining Volt Typhoon

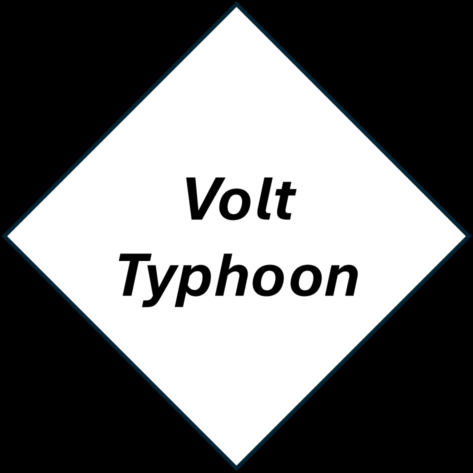
Volt Typhoon

Adversary:

- PRC-Linked
- Not Associated To Any Specific PRC Group

Capabilities:

- Persistent Use Of Living Off The Land Capabilities
- Supplemented With Publicly-Available Tools & Software



Volt Typhoon

Infrastructure:

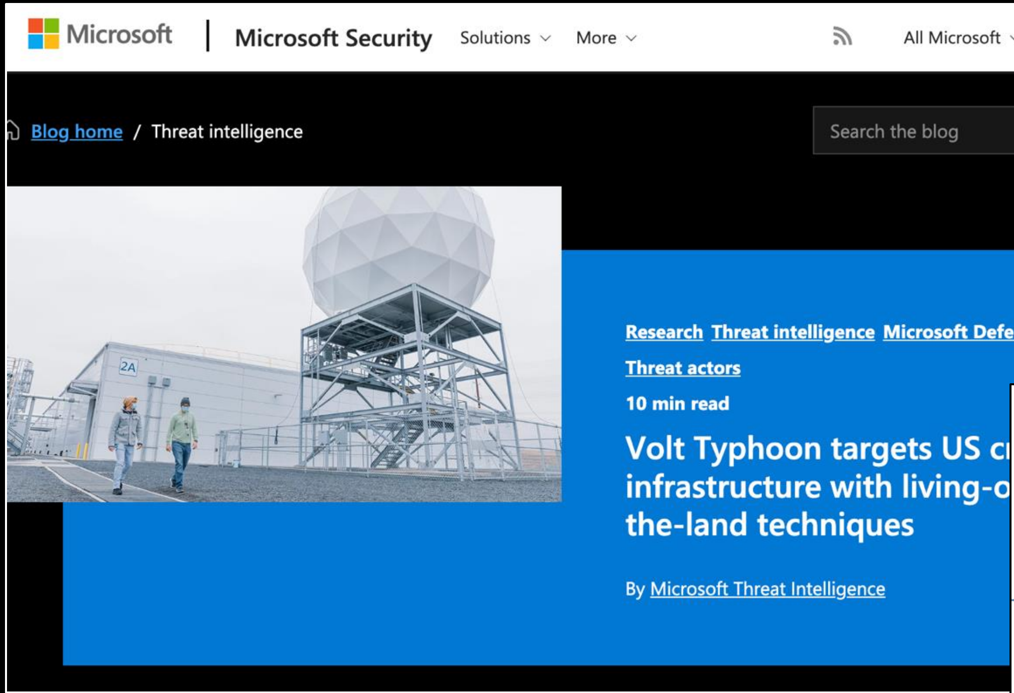
- Heavily Reliant On Botnets Of Compromised Devices
- Linked To Owned VPS Instances Managing Compromised Nodes

Victim:

- Primarily Focused On US, US-Related Critical Infrastructure
- Potential Targeting Of Entities Such As Australia, New Zealand; Activity In Africa?

Initial Reporting

Volt Typhoon

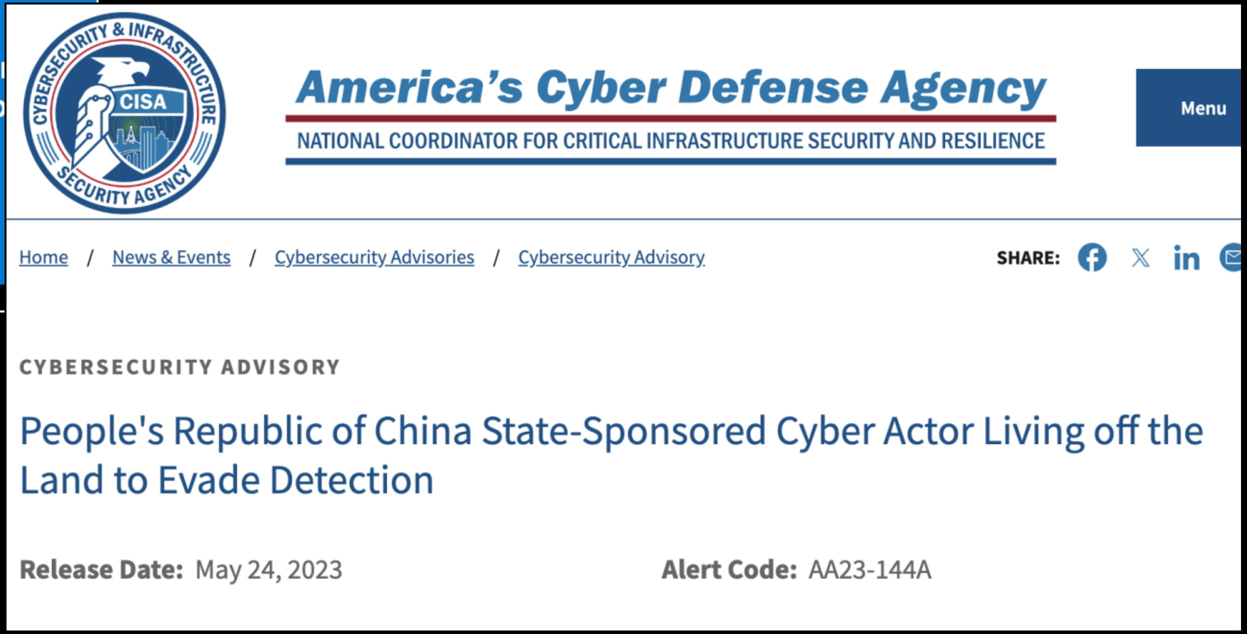


Volt Typhoon targets US c
infrastructure with living-o
the-land techniques

By Microsoft Threat Intelligence

https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
Menu
Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory
SHARE:

CYBERSECURITY ADVISORY

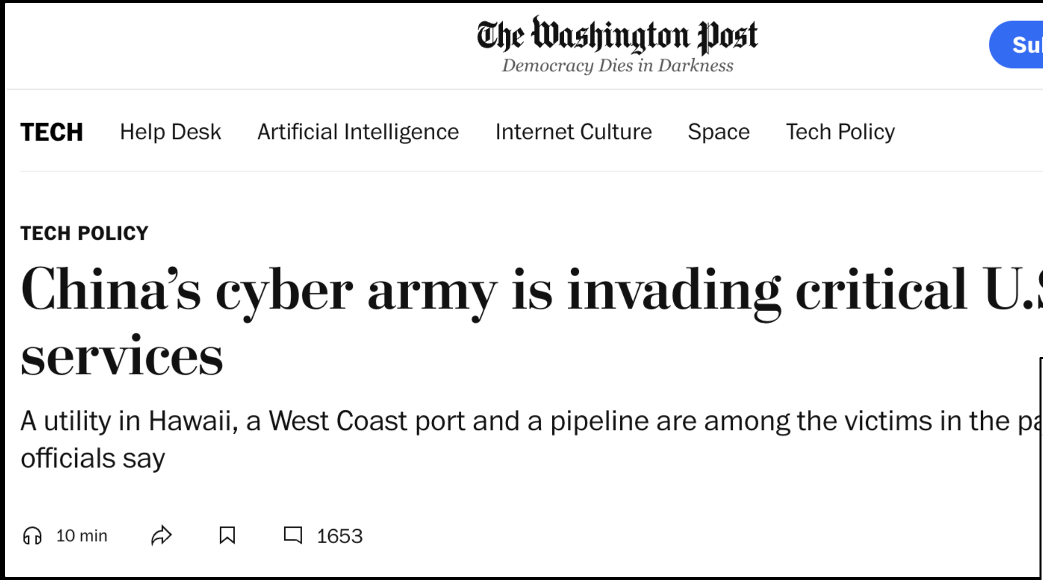
People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Release Date: May 24, 2023

Alert Code: AA23-144A

Media Follow-Up

Volt Typhoon



The Washington Post
Democracy Dies in Darkness

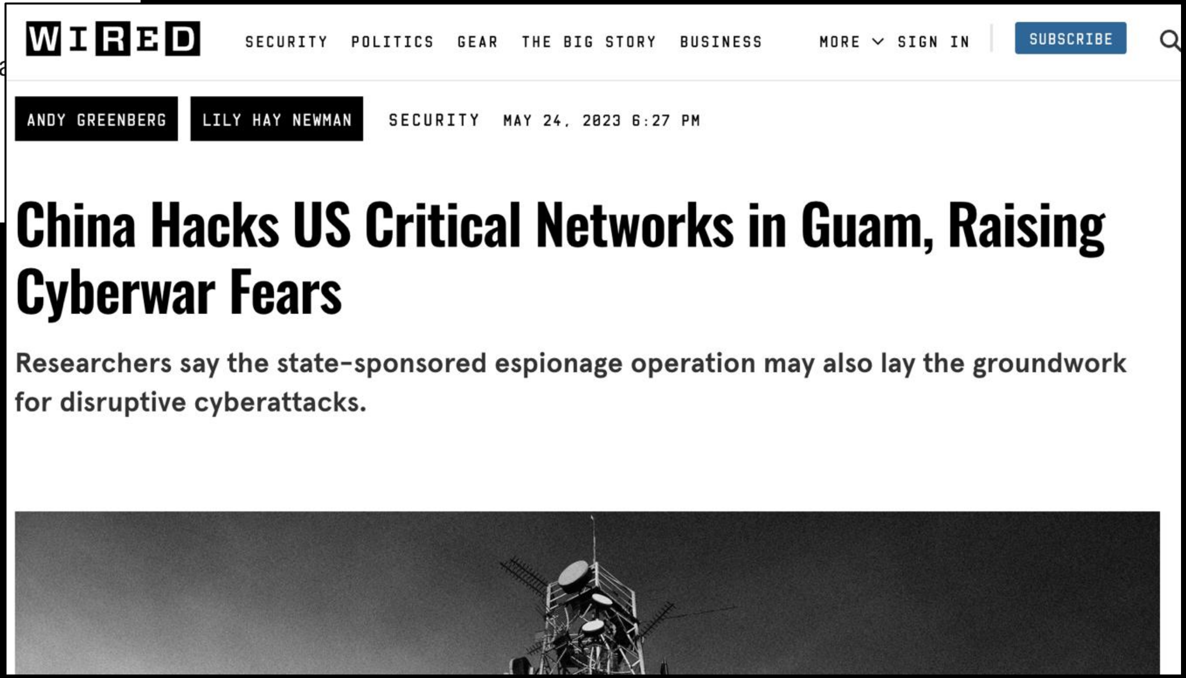
TECH POLICY

China’s cyber army is invading critical U.S. services

A utility in Hawaii, a West Coast port and a pipeline are among the victims in the pa
officials say

https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/

https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/



ANDY GREENBERG LILY HAY NEWMAN SECURITY MAY 24, 2023 6:27 PM

China Hacks US Critical Networks in Guam, Raising Cyberwar Fears

Researchers say the state-sponsored espionage operation may also lay the groundwork for disruptive cyberattacks.

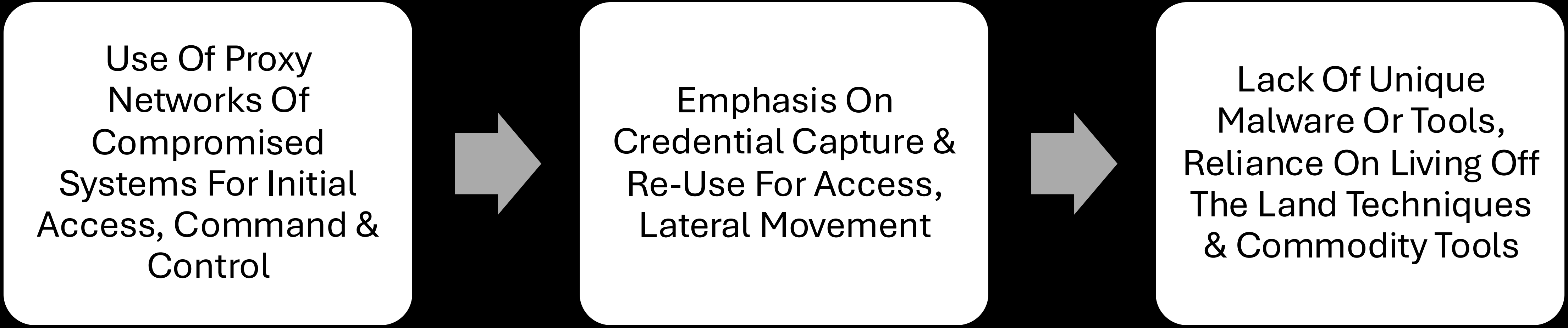
Victims & Targeting

Volt Typhoon

- Critical Infrastructure Entities On Guam
- Hawaiian Critical Infrastructure Entities
- Ports & Logistics Facilities
- Critical Infrastructure Entities Associated With Military Facilities
- ISPs & MSPs
- Smaller Utilities Such As Cooperatives & Municipal Entities

Intrusion Methodology

Volt Typhoon



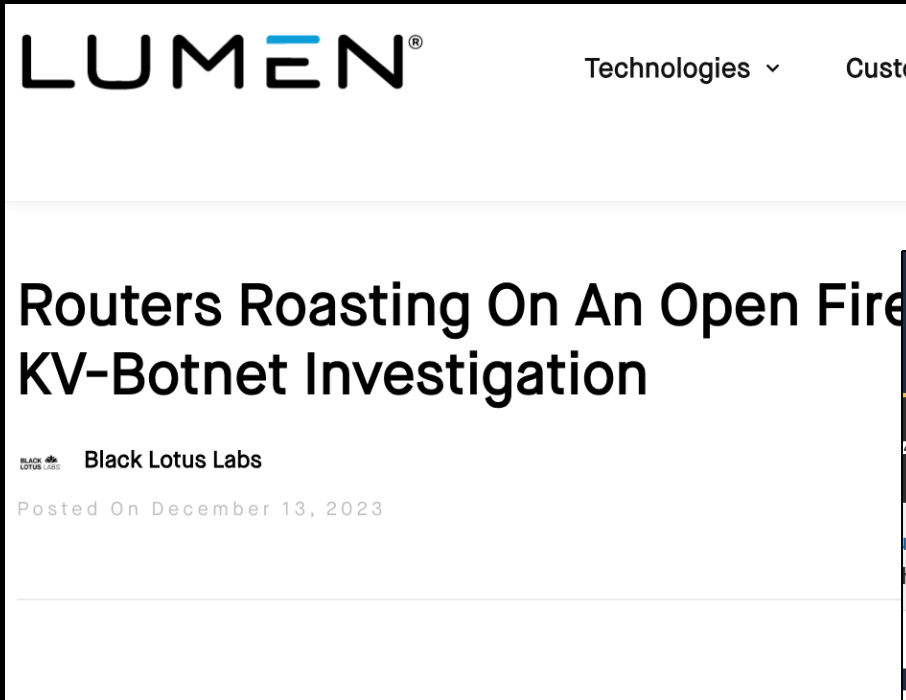
Use Of Proxy Networks Of Compromised Systems For Initial Access, Command & Control

Emphasis On Credential Capture & Re-Use For Access, Lateral Movement

Lack Of Unique Malware Or Tools, Reliance On Living Off The Land Techniques & Commodity Tools

Command & Control Infrastructure

Volt Typhoon



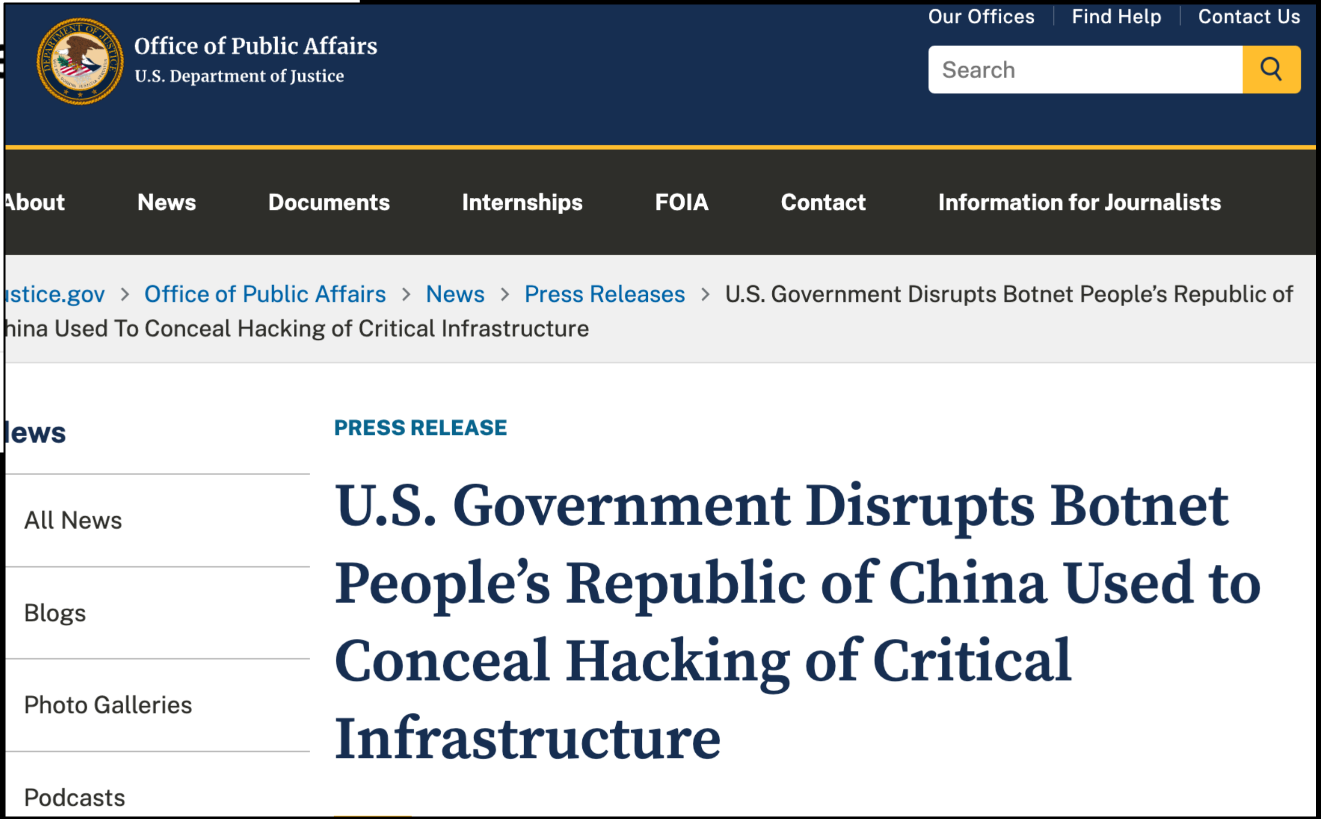
Routers Roasting On An Open Fire
KV-Botnet Investigation

Black Lotus Labs

Posted On December 13, 2023

https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical



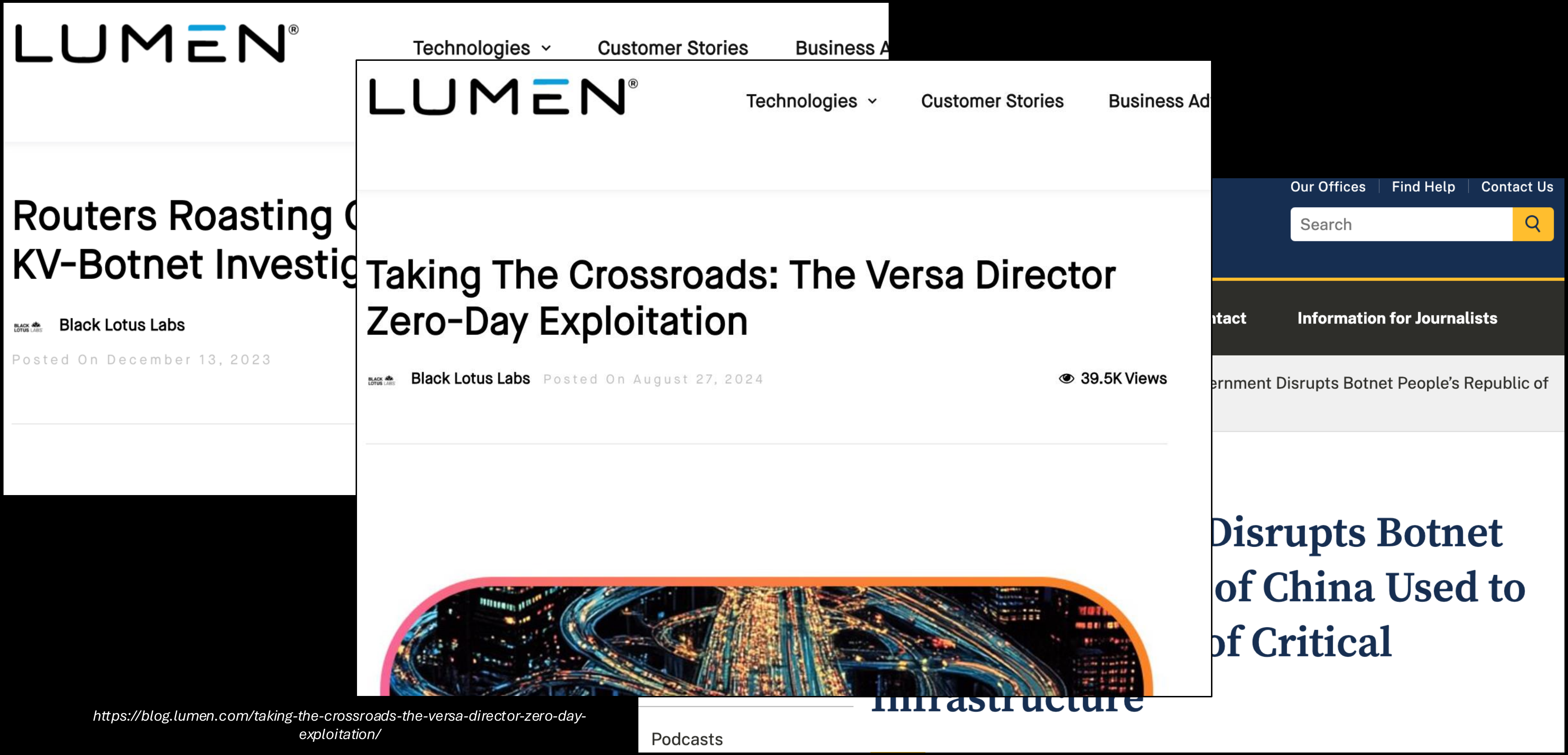
ıstice.gov > Office of Public Affairs > News > Press Releases > U.S. Government Disrupts Botnet People's Republic of hina Used To Conceal Hacking of Critical Infrastructure

PRESS RELEASE

U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure

Command & Control Infrastructure

Volt Typhoon



LUMEN®

Technologies ⌄ Customer Stories Business A

Routers Roasting C
KV-Botnet Investig

Black Lotus Labs

Posted On December 13, 2023

LUMEN®

Technologies ⌄ Customer Stories Business Ad

Taking The Crossroads: The Versa Director Zero-Day Exploitation

Black Lotus Labs Posted On August 27, 2024 39.5K Views

Our Offices | Find Help | Contact Us

Search

ntact Information for Journalists

ernment Disrupts Botnet People's Republic of

Disrupts Botnet
of China Used to
of Critical
Infrastructure

Podcasts

https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

Impacts

Volt Typhoon

???

Impacts

Volt Typhoon

To Date There Is No Publicly Known or Acknowledged Impact Resulting From Volt Typhoon Activity…

Impacts

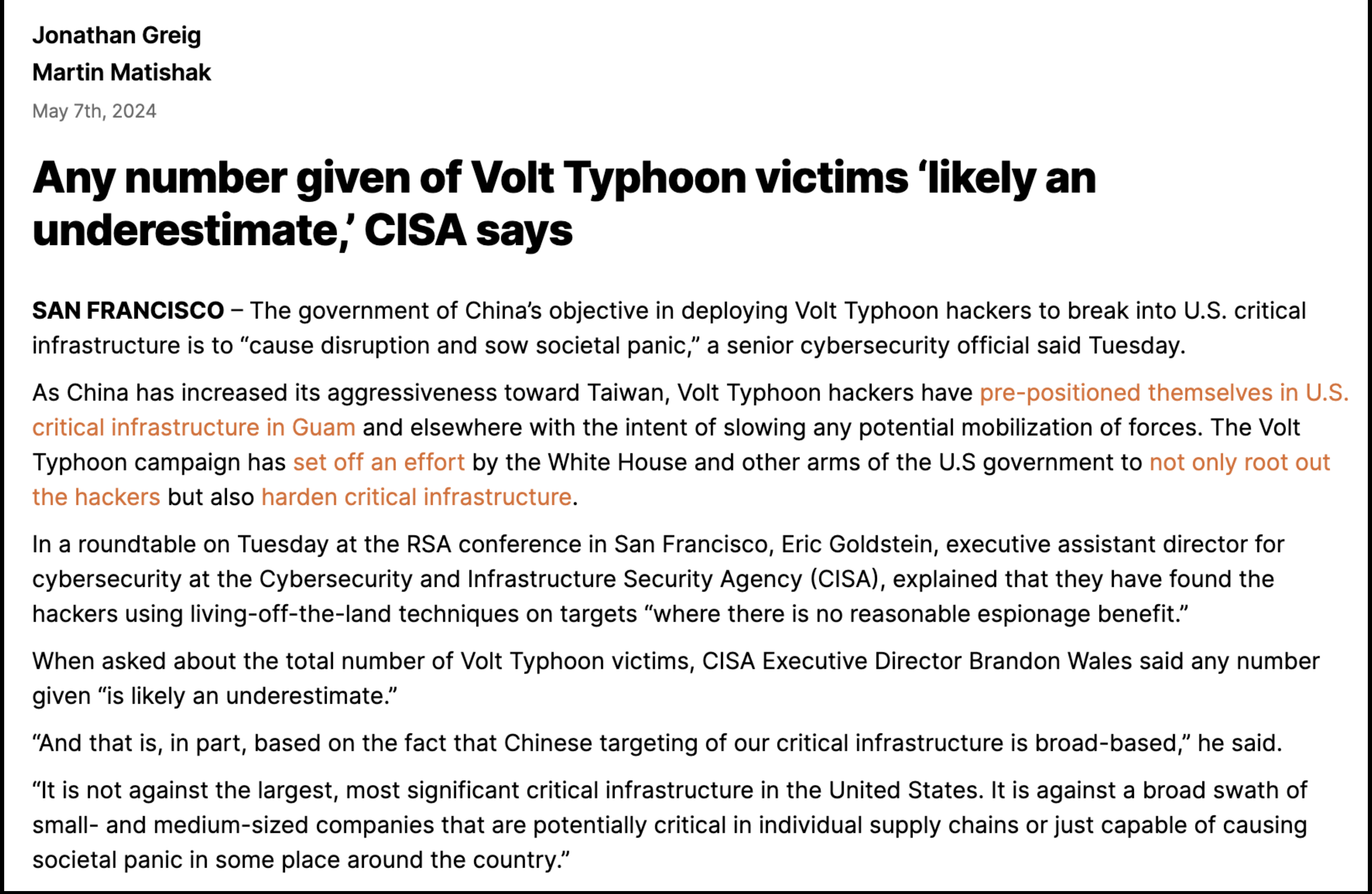
Volt Typhoon

To Date There Is No Publicly Known or Acknowledged Impact Resulting From Volt Typhoon Activity…

…Except Maybe A Lot Of Busy, Frustrated Analysts

Continued Hype

Volt Typhoon



Jonathan Greig
Martin Matishak
May 7th, 2024

Any number given of Volt Typhoon victims ‘likely an underestimate,’ CISA says

SAN FRANCISCO – The government of China’s objective in deploying Volt Typhoon hackers to break into U.S. critical infrastructure is to “cause disruption and sow societal panic,” a senior cybersecurity official said Tuesday.

As China has increased its aggressiveness toward Taiwan, Volt Typhoon hackers have pre-positioned themselves in U.S. critical infrastructure in Guam and elsewhere with the intent of slowing any potential mobilization of forces. The Volt Typhoon campaign has set off an effort by the White House and other arms of the U.S government to not only root out the hackers but also harden critical infrastructure.

In a roundtable on Tuesday at the RSA conference in San Francisco, Eric Goldstein, executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency (CISA), explained that they have found the hackers using living-off-the-land techniques on targets “where there is no reasonable espionage benefit.”

When asked about the total number of Volt Typhoon victims, CISA Executive Director Brandon Wales said any number given “is likely an underestimate.”

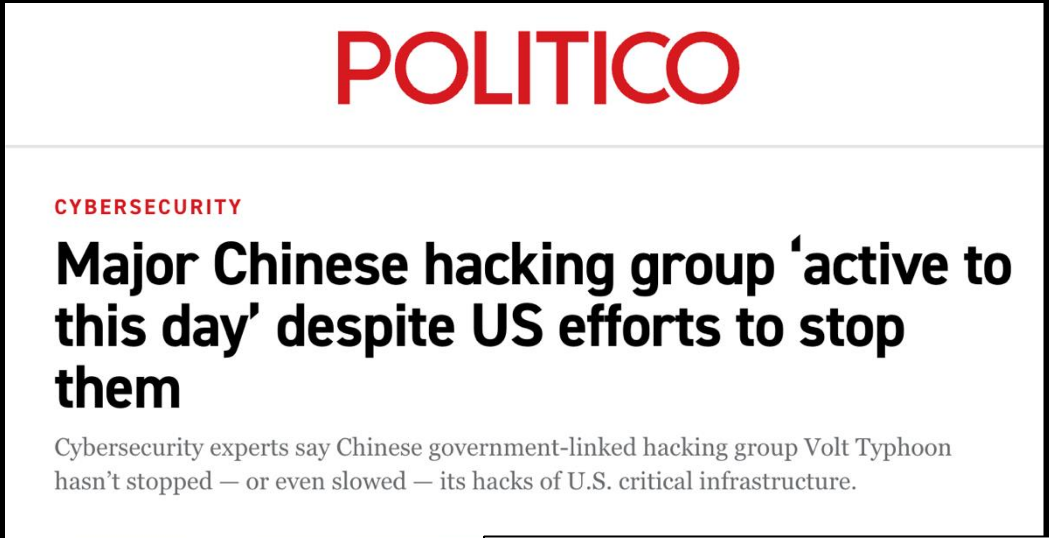
“And that is, in part, based on the fact that Chinese targeting of our critical infrastructure is broad-based,” he said.

“It is not against the largest, most significant critical infrastructure in the United States. It is against a broad swath of small- and medium-sized companies that are potentially critical in individual supply chains or just capable of causing societal panic in some place around the country.”

https://therecord.media/volt-typhoon-targets-underestimated-cisa-says

Continued Hype!

Volt Typhoon



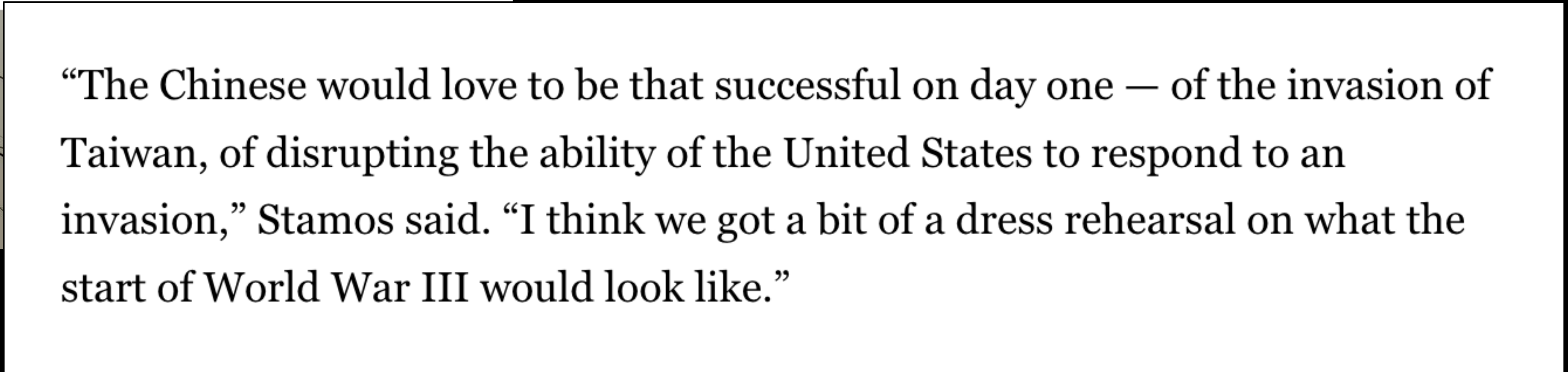
POLITICO

CYBERSECURITY

Major Chinese hacking group 'active to this day' despite US efforts to stop them

Cybersecurity experts say Chinese government-linked hacking group Volt Typhoon hasn't stopped — or even slowed — its hacks of U.S. critical infrastructure.

https://www.politico.com/news/2024/08/09/china-hacking-group-cybersecurity-00173454



"The Chinese would love to be that successful on day one — of the invasion of Taiwan, of disrupting the ability of the United States to respond to an invasion," Stamos said. "I think we got a bit of a dress rehearsal on what the start of World War III would look like."

Lack Of Information

Volt Typhoon

Despite Concerns, Publicly Available Information On Volt Typhoon Activity Remains Scarce, With Only A Handful Of Reports & Analysis

The Defender’s Dilemma

Attacks With No Impact (Yet)

The Defender’s Dilemma

Volt Typhoon Is A Concerning Entity – But Has Resulted In No, Known Impacts Or Effects

Attacks With No Impact (Yet)

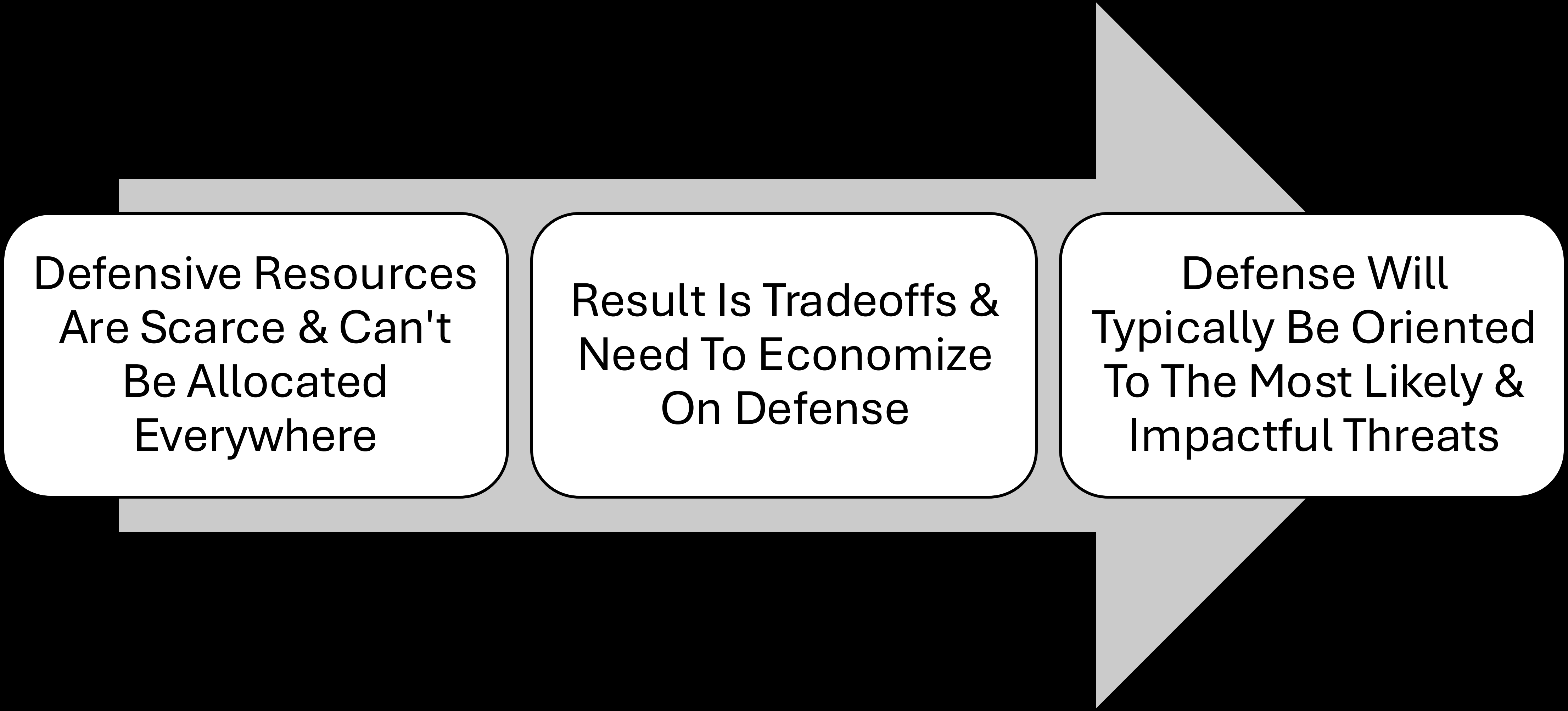
The Defender's Dilemma

Volt Typhoon Is A Concerning Entity – But Has Resulted In No, Known Impacts Or Effects

How Do Defenders & Decision Makers Evaluate A Threat With No Existing Impact?

Defense & Scarcity

The Defender’s Dilemma



Defensive Resources Are Scarce & Can't Be Allocated Everywhere

Result Is Tradeoffs & Need To Economize On Defense

Defense Will Typically Be Oriented To The Most Likely & Impactful Threats

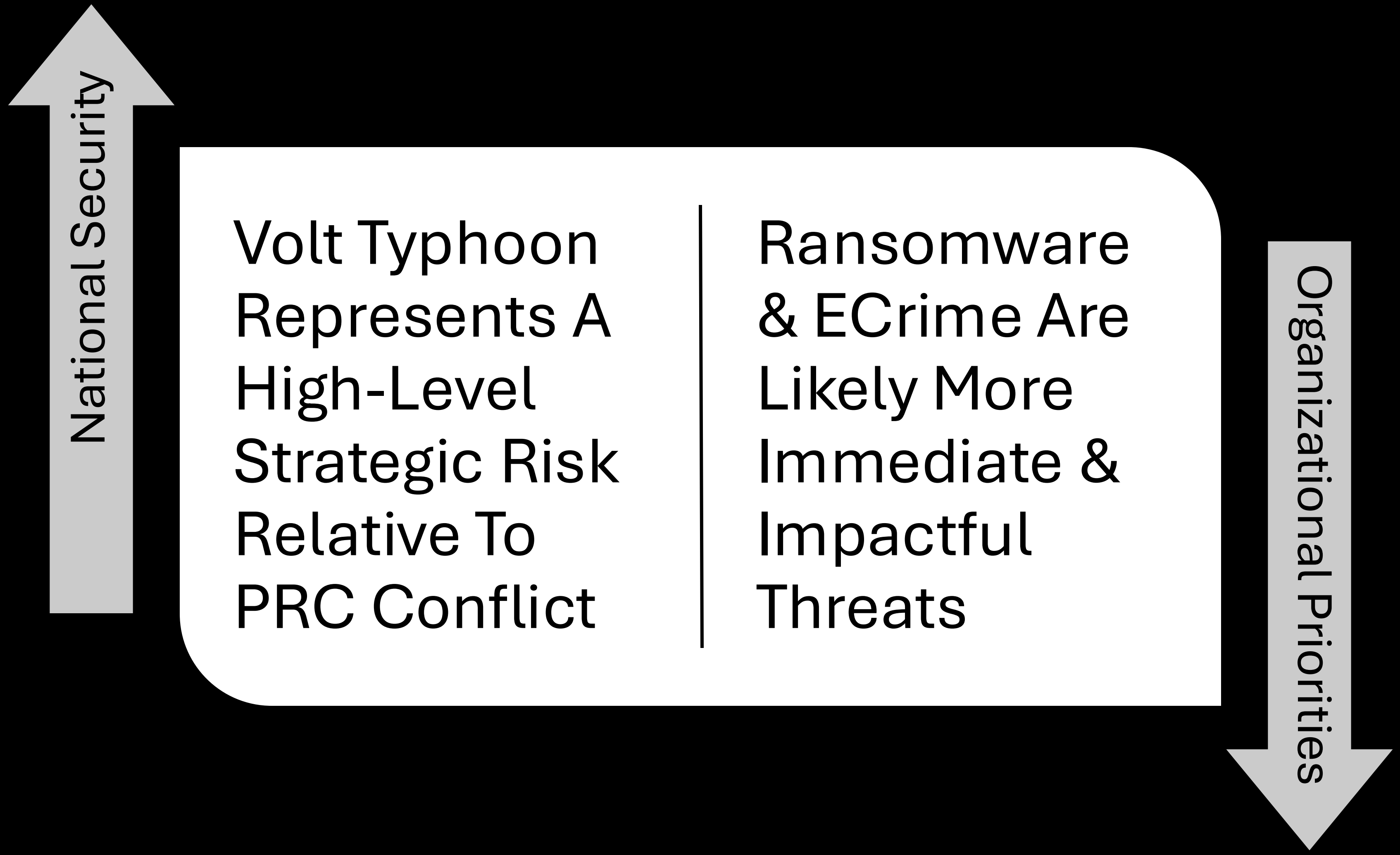
The Risk Of Volt Typhoon

The Defender’s Dilemma

Volt Typhoon Operations Currently Represent A Great STRATEGIC Risk To US Interests, But Thus Far Have Not Manifested As An IMMEDIATE Concern To Potential Victims!

Priorities

The Defender's Dilemma



National Security

Volt Typhoon Represents A High-Level Strategic Risk Relative To PRC Conflict

Ransomware & ECrime Are Likely More Immediate & Impactful Threats

Organizational Priorities

Priorities Simplified

The Defender’s Dilemma

Does The Security Team Invest Untold Hours & Resources Chasing Volt Typhoon, Or Hardening The Network Against Ransomware Activity?

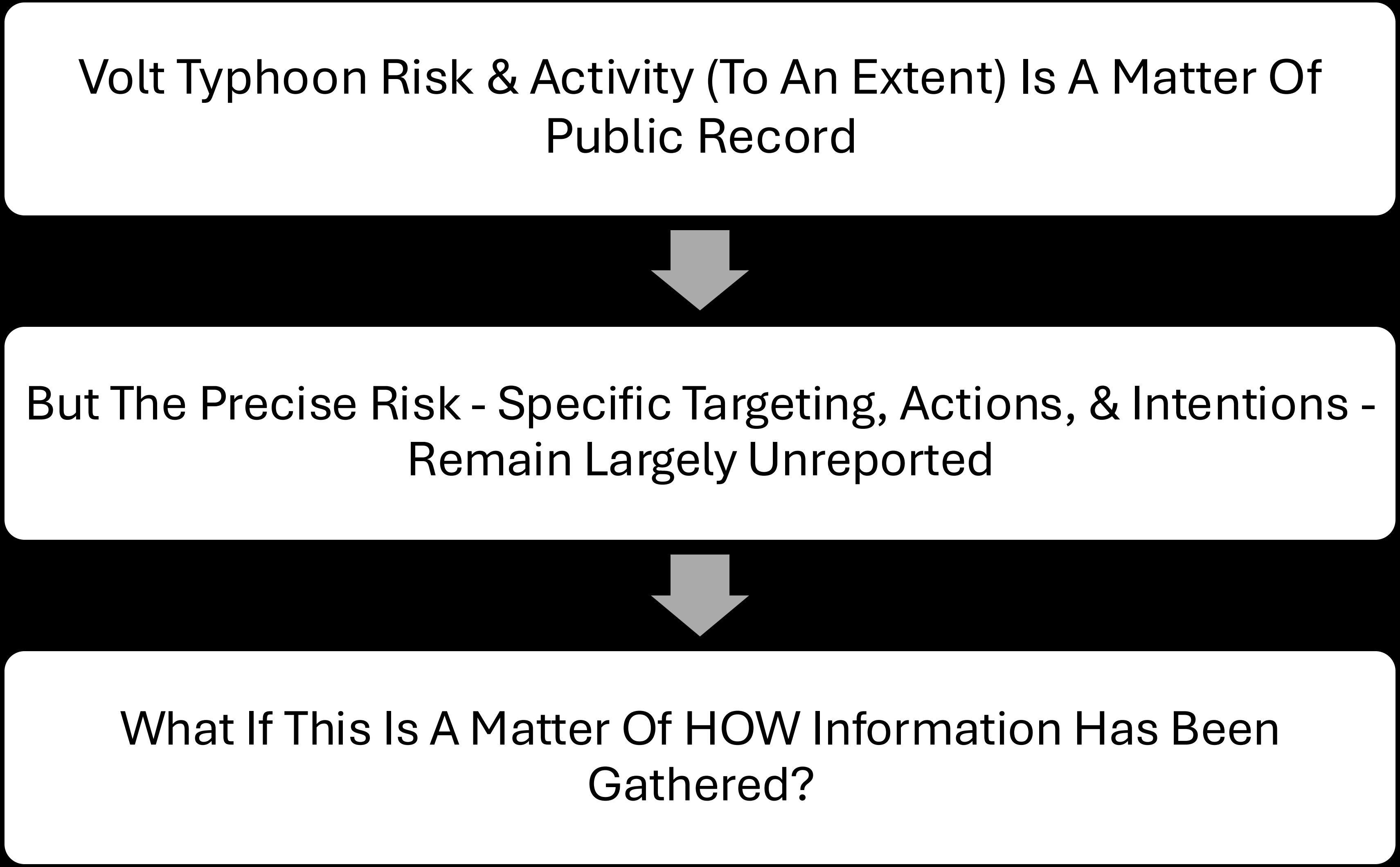
Information Sharing & Disclosure

What If Everything Is Secret?

Information Sharing & Disclosure

What If Everything Is Secret?

Information Sharing & Disclosure



Volt Typhoon Risk & Activity (To An Extent) Is A Matter Of Public Record

But The Precise Risk - Specific Targeting, Actions, & Intentions - Remain Largely Unreported

What If This Is A Matter Of HOW Information Has Been Gathered?

The Disclosure Dilemma

Information Sharing & Disclosure

Cyber Threat Intelligence Conference

April 15-17, 2024 | Berlin, Germany

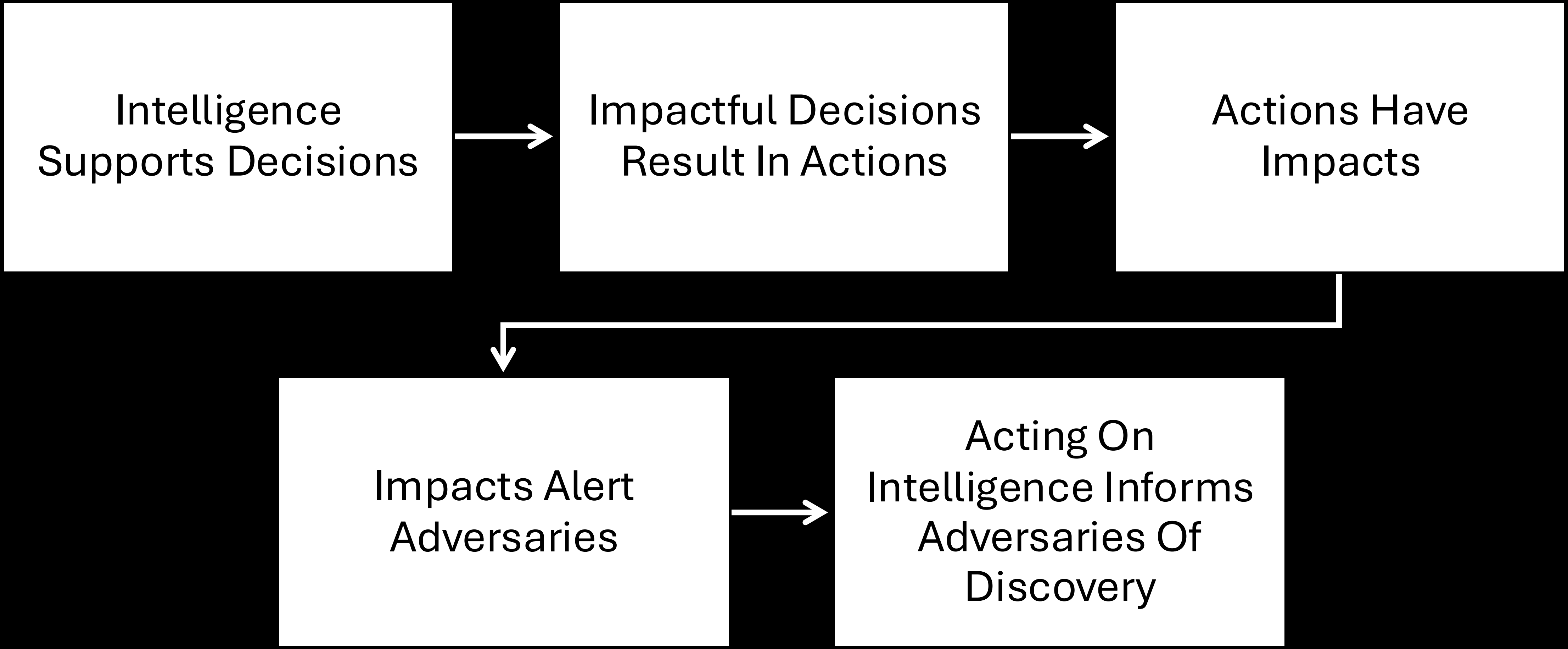
#FIRSTCTI24

The Disclosure Dilemma and Ensuring Defense

Joe Slowik (Paralus, US)

The Disclosure Dilemma

Information Sharing & Disclosure



Intelligence Supports Decisions

Impactful Decisions Result In Actions

Actions Have Impacts

Impacts Alert Adversaries

Acting On Intelligence Informs Adversaries Of Discovery

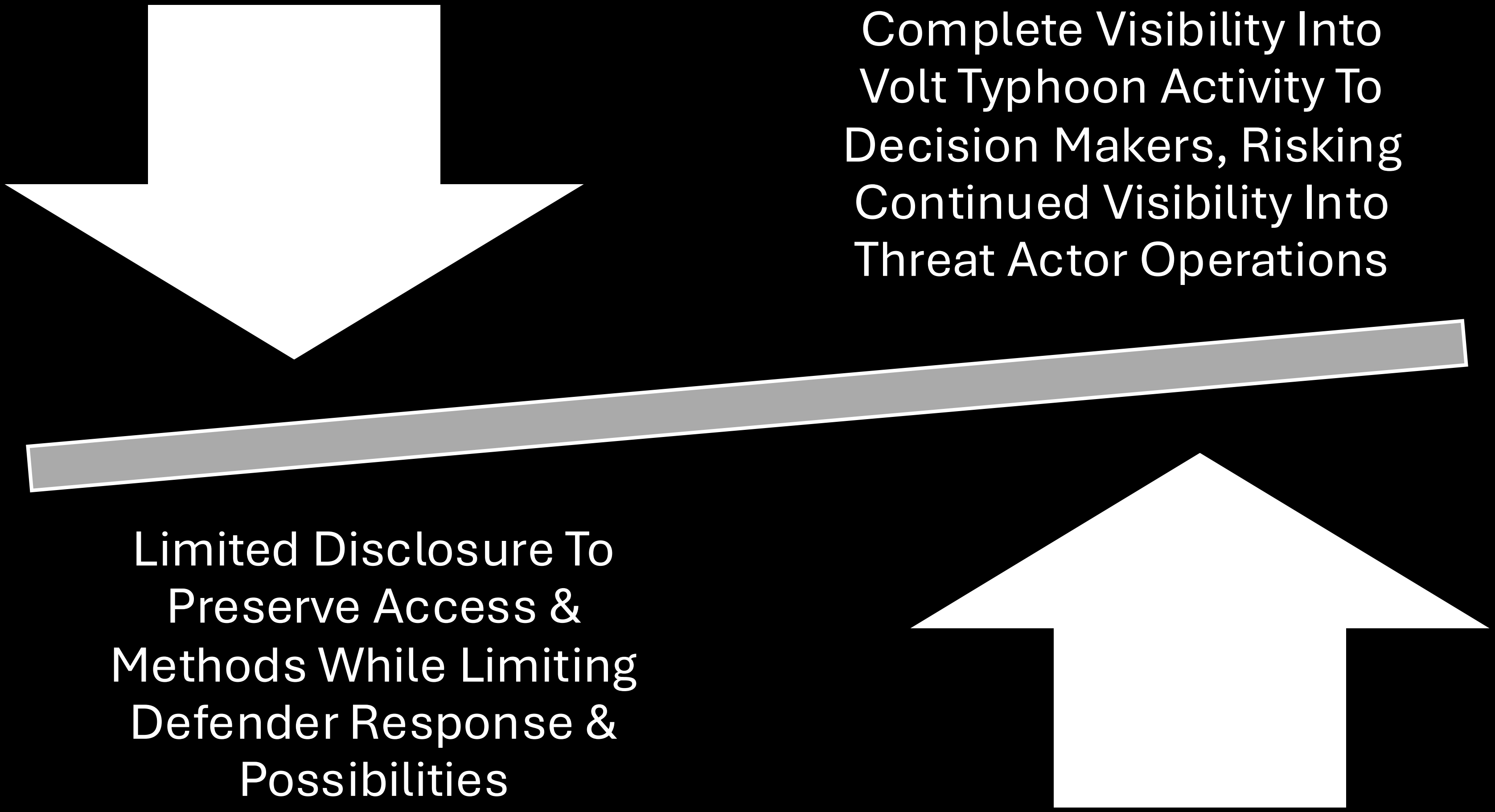
The Limits Of Sharing

Information Sharing & Disclosure

SIGNIFICANT Information May Exist About Volt Typhoon – But Sharing This Information May Risk Continued Information Collection & Surveillance!

Balancing Acts

Information Sharing & Disclosure



Complete Visibility Into Volt Typhoon Activity To Decision Makers, Risking Continued Visibility Into Threat Actor Operations

Limited Disclosure To Preserve Access & Methods While Limiting Defender Response & Possibilities

Sharing Objectives & Outcomes

Information Sharing & Disclosure

Presumably Authorities Desire To Improve Critical Infrastructure Defense

Sharing Objectives & Outcomes

Information Sharing & Disclosure

Presumably Authorities Desire To Improve Critical Infrastructure Defense

But The Very Act Of Doing So May Imperil Continued Visibility Into Adversary Activity

Sharing Objectives & Outcomes

Information Sharing & Disclosure

Presumably Authorities Desire To Improve Critical Infrastructure Defense

But The Very Act Of Doing So May Imperil Continued Visibility Into Adversary Activity

Stakeholders Need To Balance Defense & Intelligence Needs!

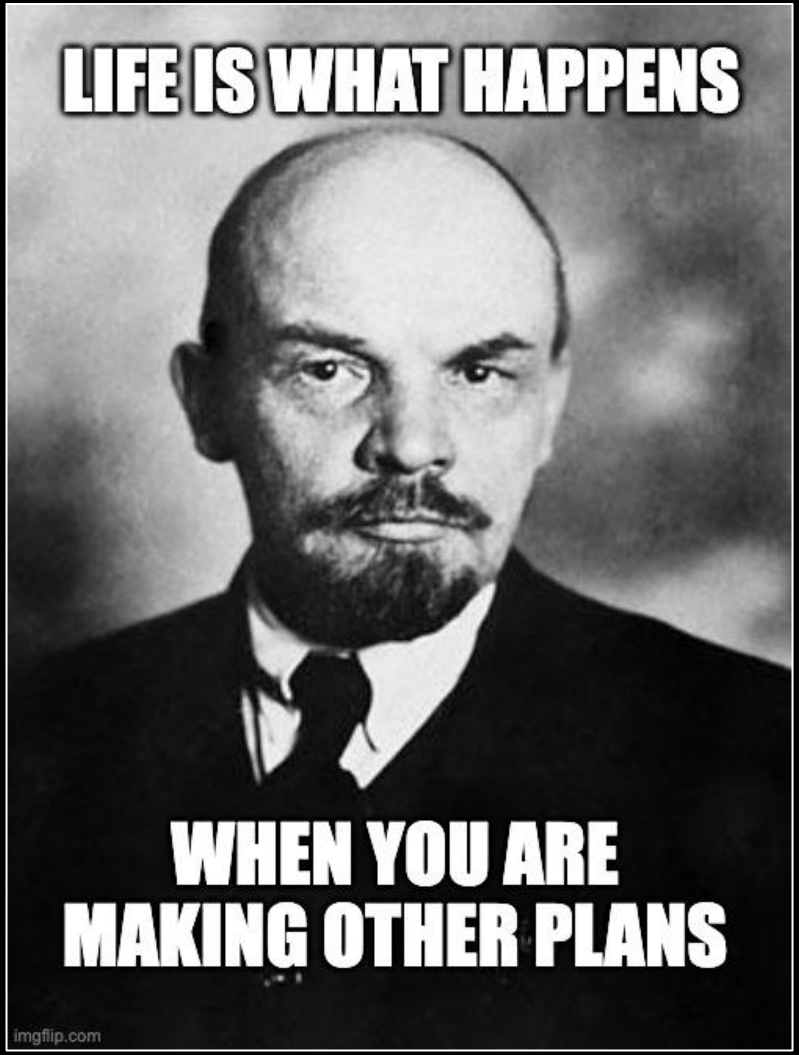
Making Decisions

Decisions Are Not Easy

Making Decisions

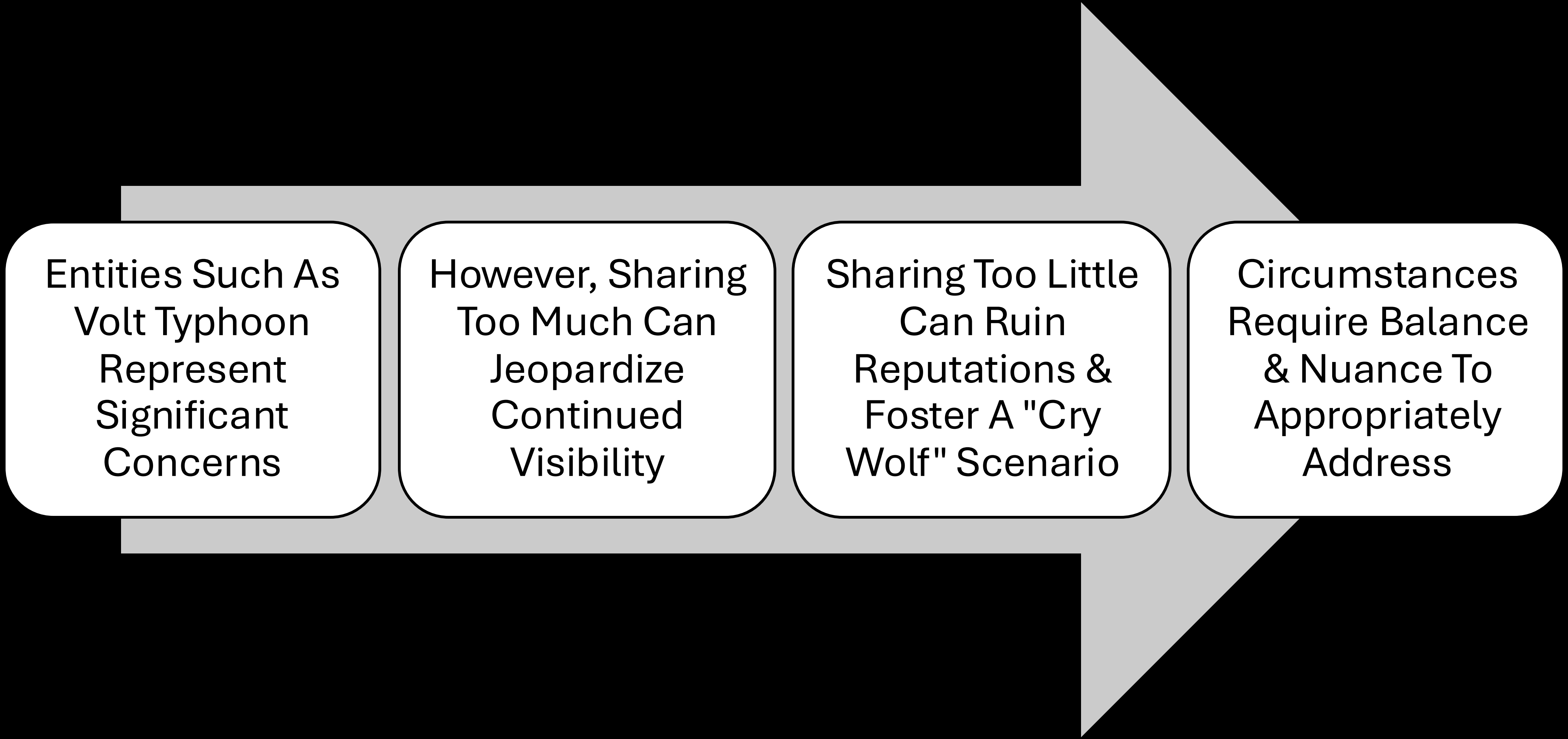
Decisions Are Not Easy

Making Decisions



Context, Balance, & Impact

Making Decisions



Entities Such As Volt Typhoon Represent Significant Concerns

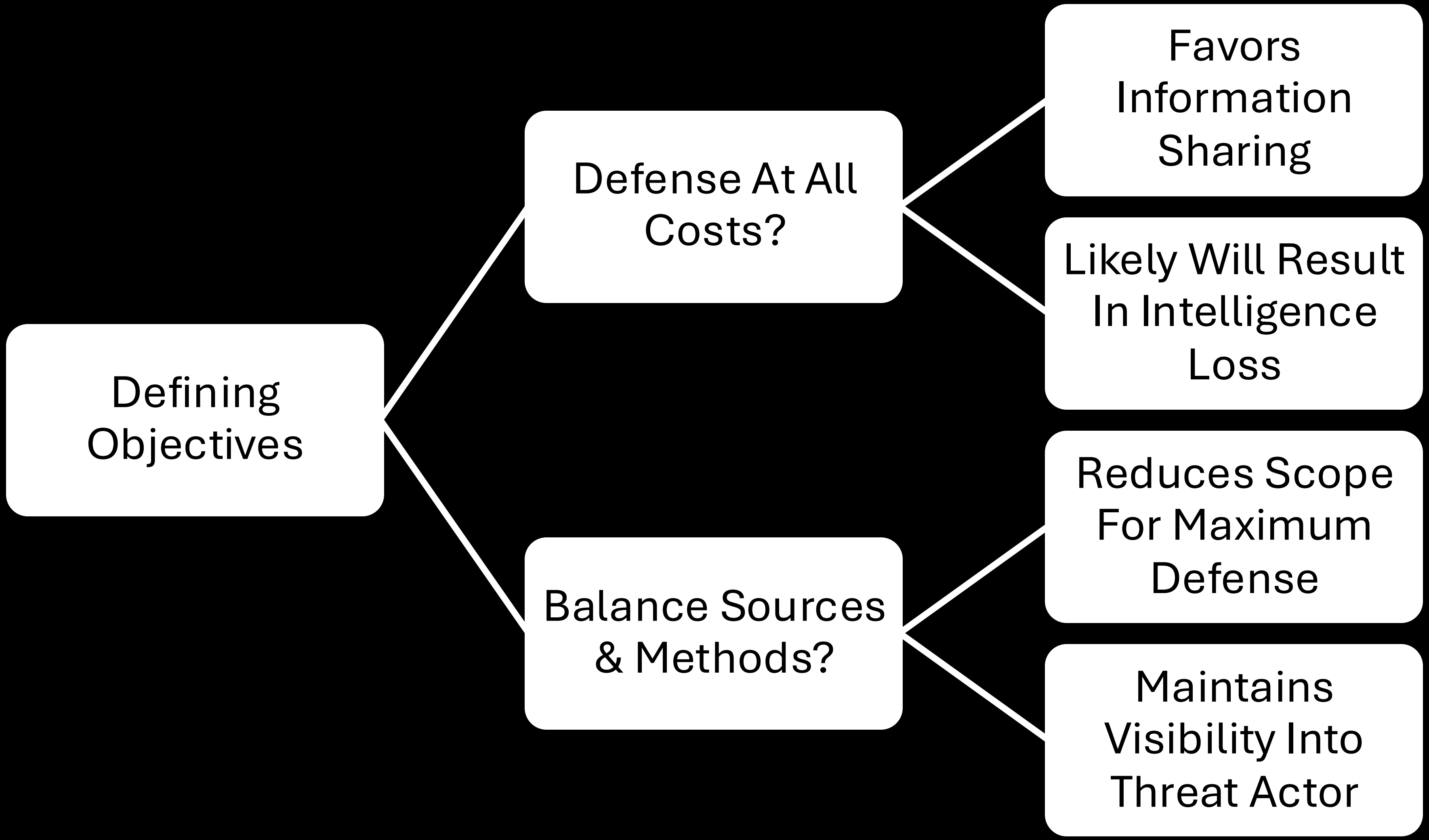
However, Sharing Too Much Can Jeopardize Continued Visibility

Sharing Too Little Can Ruin Reputations & Foster A "Cry Wolf" Scenario

Circumstances Require Balance & Nuance To Appropriately Address

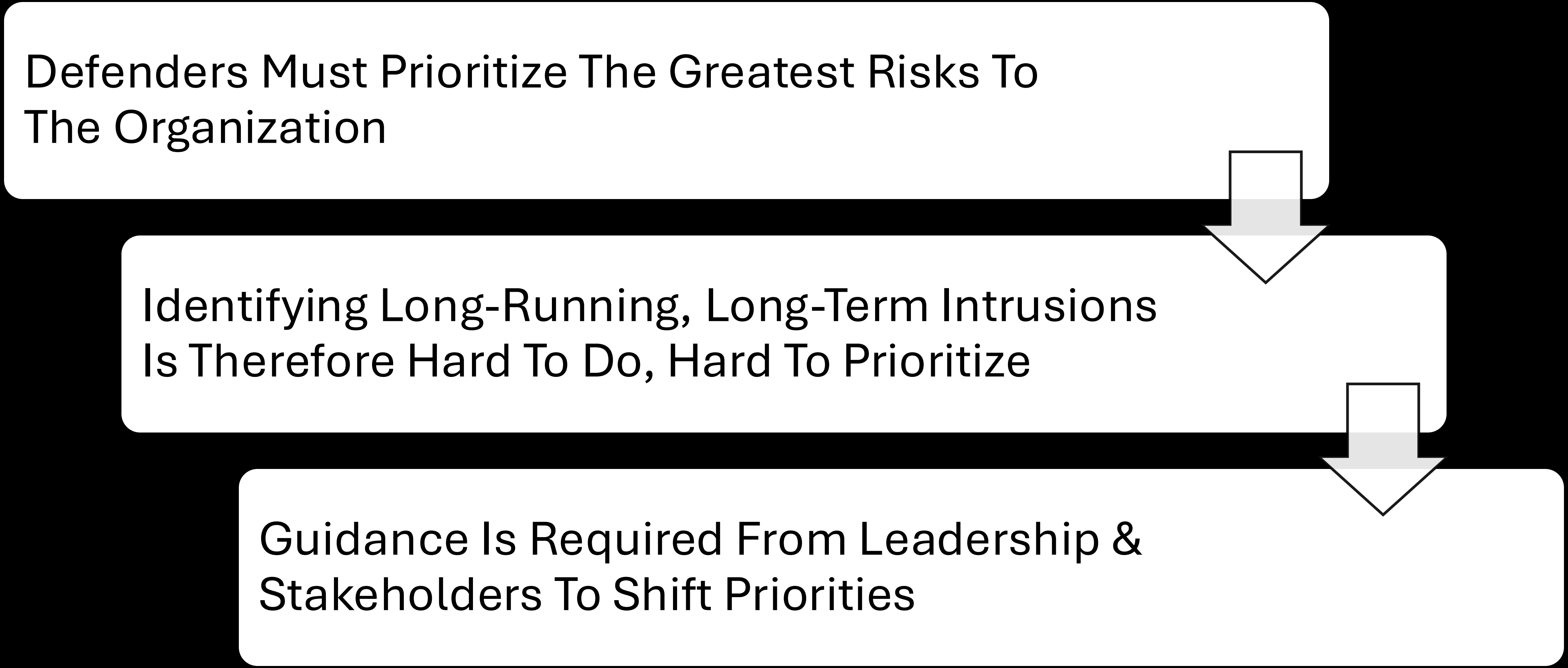
Strategic Context

Making Decisions


Defining Objectives
Defense At All Costs?
Balance Sources & Methods?
Favors Information Sharing
Likely Will Result In Intelligence Loss
Reduces Scope For Maximum Defense
Maintains Visibility Into Threat Actor

Defender Context

Making Decisions



Defenders Must Prioritize The Greatest Risks To The Organization

Identifying Long-Running, Long-Term Intrusions Is Therefore Hard To Do, Hard To Prioritize

Guidance Is Required From Leadership & Stakeholders To Shift Priorities

Communication Concerns

Making Decisions

Highlighting A Threat Can Call Attention To Concerns

But Doing So Absent Visible Impacts Risks "Crying Wolf"

Stakeholders Need To Be VERY CAREFUL In Balancing Between Awareness & Hype!

Threading The Needle

Making Decisions

Managing Latent, Emerging, Or Long-Running Threats With No Immediate Or Near-Term Impact Is VERY HARD!

Threading The Needle

Making Decisions

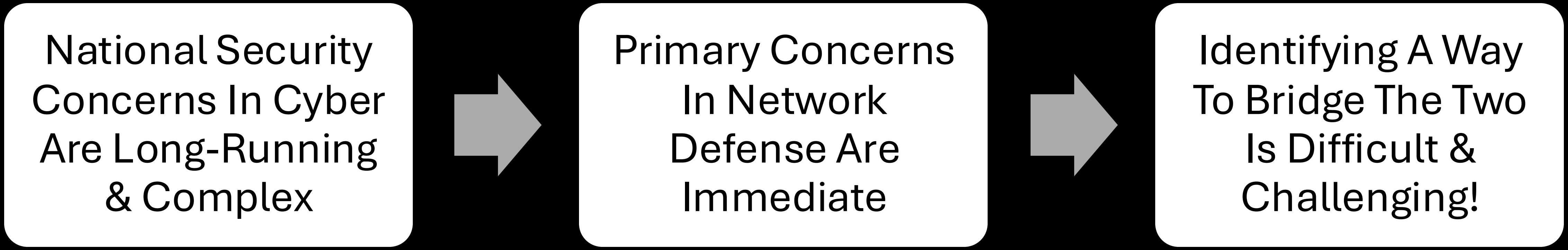
Managing Latent, Emerging, Or Long-Running Threats With No Immediate Or Near-Term Impact Is VERY HARD!

Best Course Of Action May Be To Keep Matters Quiet Outside Of Industry & Trusted Channels!

Lessons & Implications

Thorny Issues

Lessons & Implications



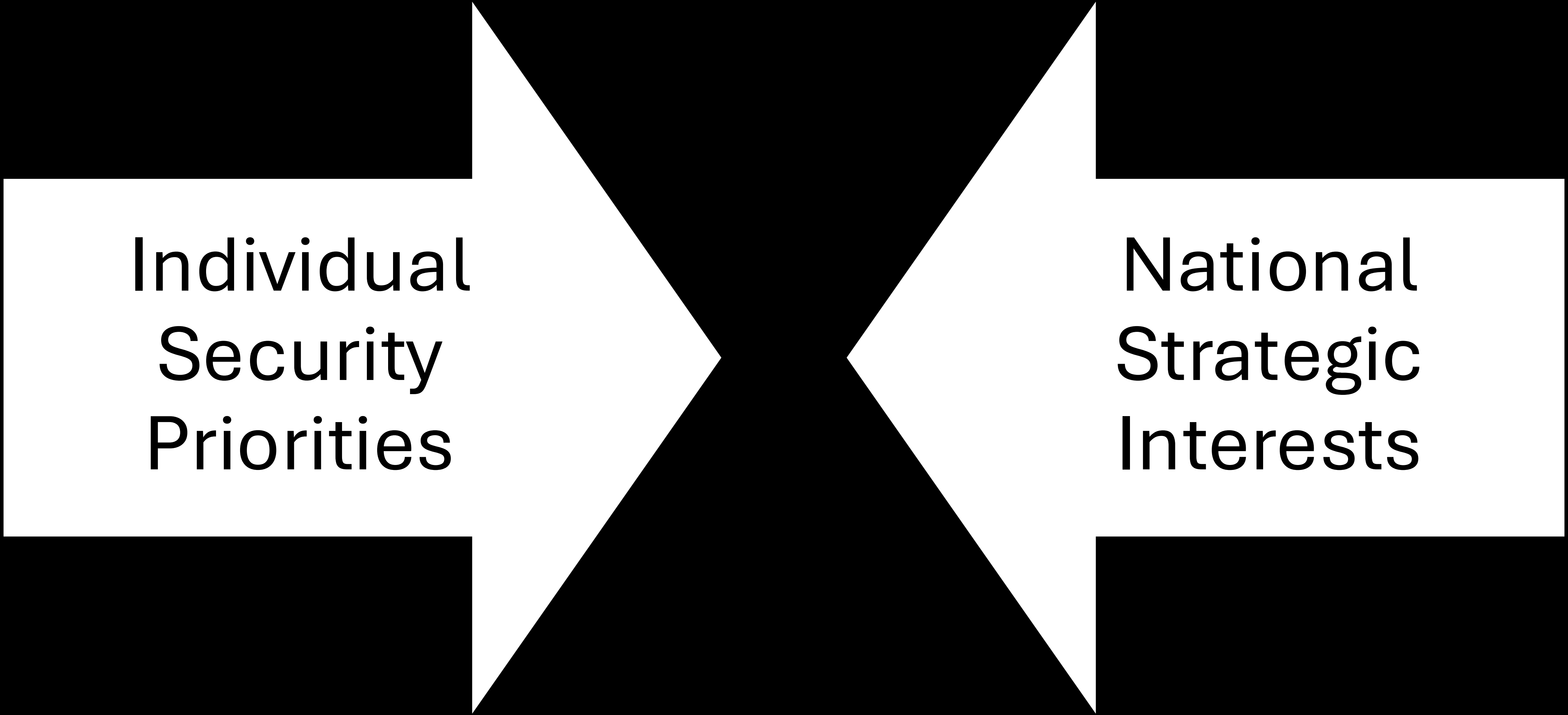
National Security Concerns In Cyber Are Long-Running & Complex

Primary Concerns In Network Defense Are Immediate

Identifying A Way To Bridge The Two Is Difficult & Challenging!

Conflicting Concerns

Lessons & Implications

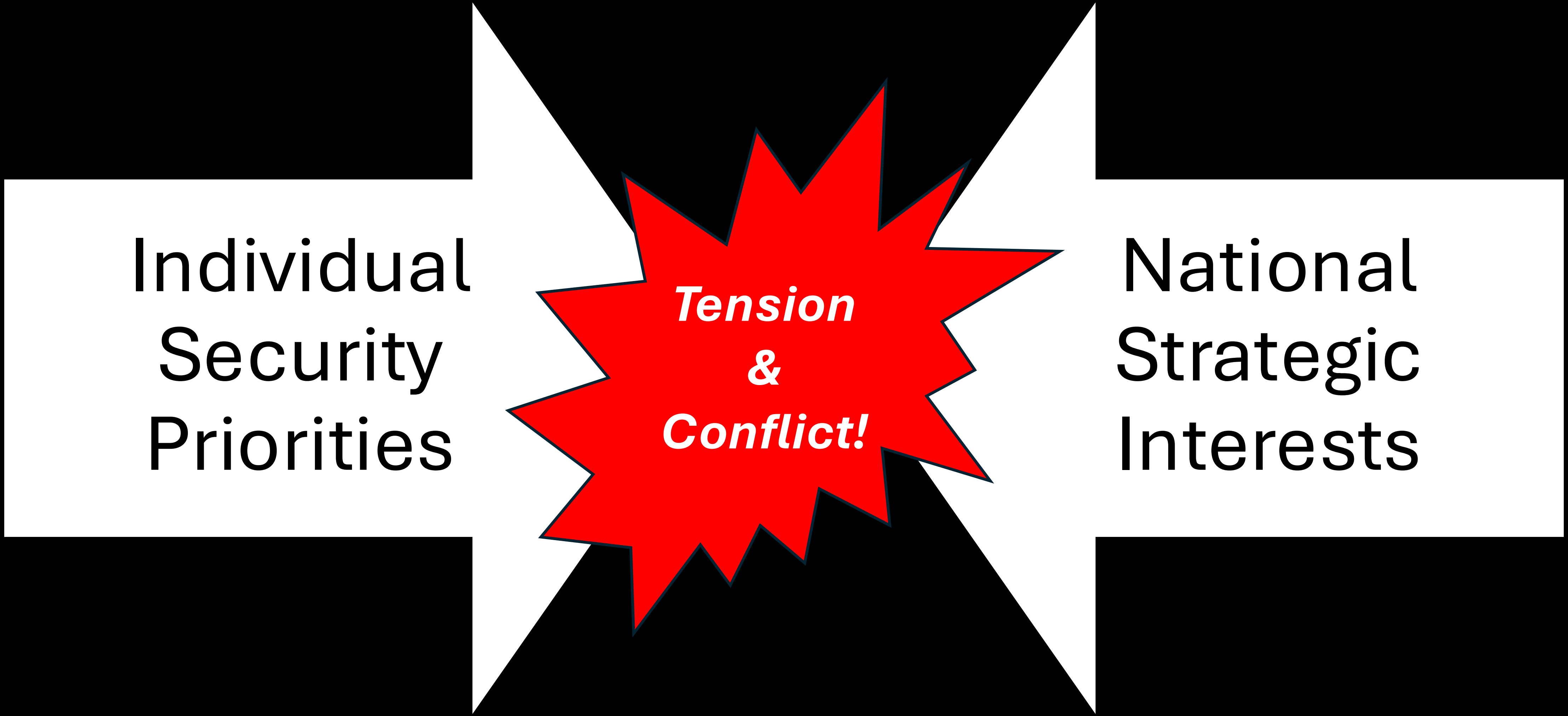


Individual Security Priorities

National Strategic Interests

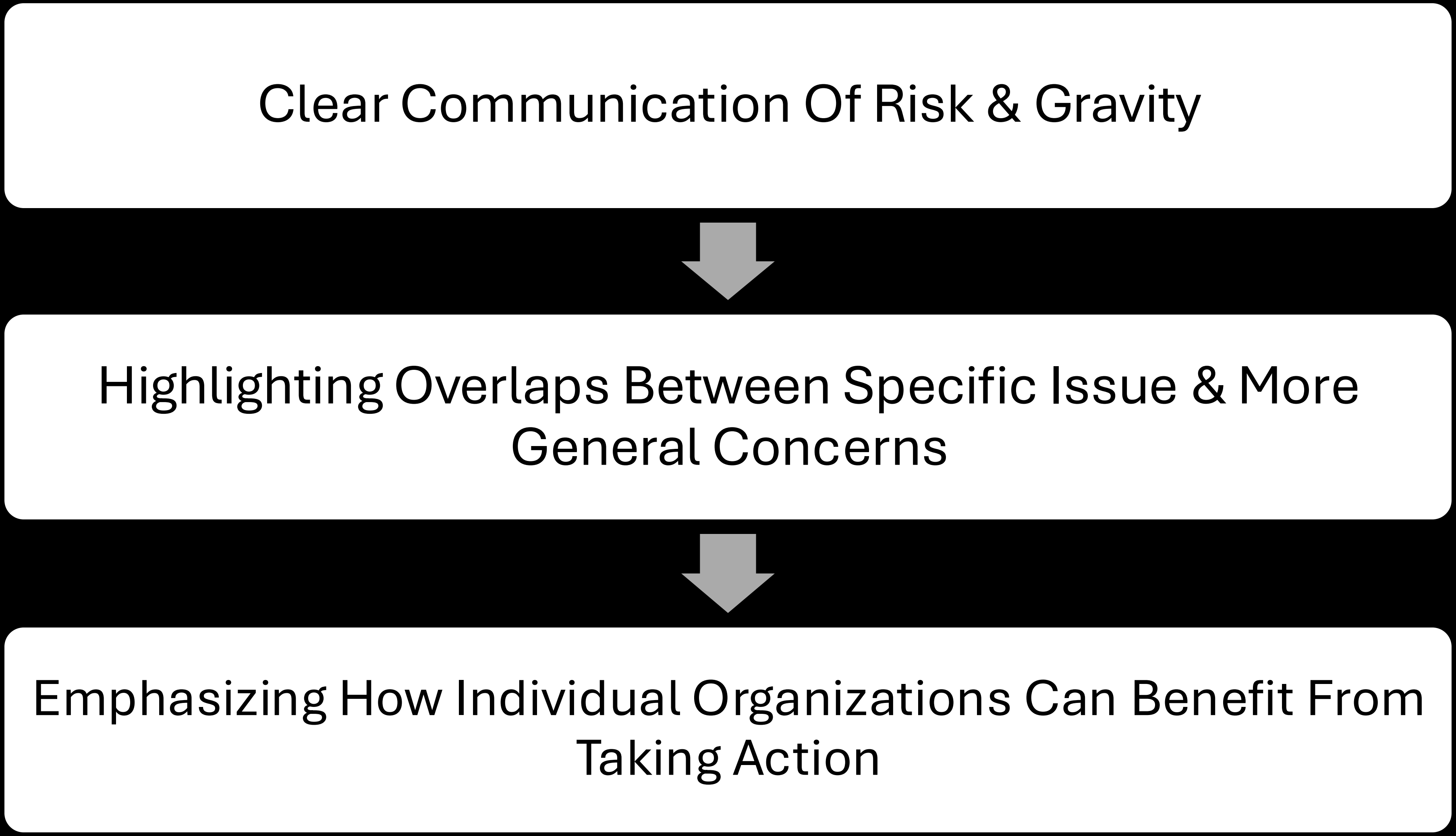
Conflicting Concerns

Lessons & Implications



Addressing Concerns

Lessons & Implications



Clear Communication Of Risk & Gravity

Highlighting Overlaps Between Specific Issue & More General Concerns

Emphasizing How Individual Organizations Can Benefit From Taking Action

Overlapping Actions?

Lessons & Implications

Some Problem Sets – Like LOLBIN Defense – May Benefit Organizations In Both Immediate & Strategic Contexts – This Benefit Needs To Be Communicated & Highlighted!

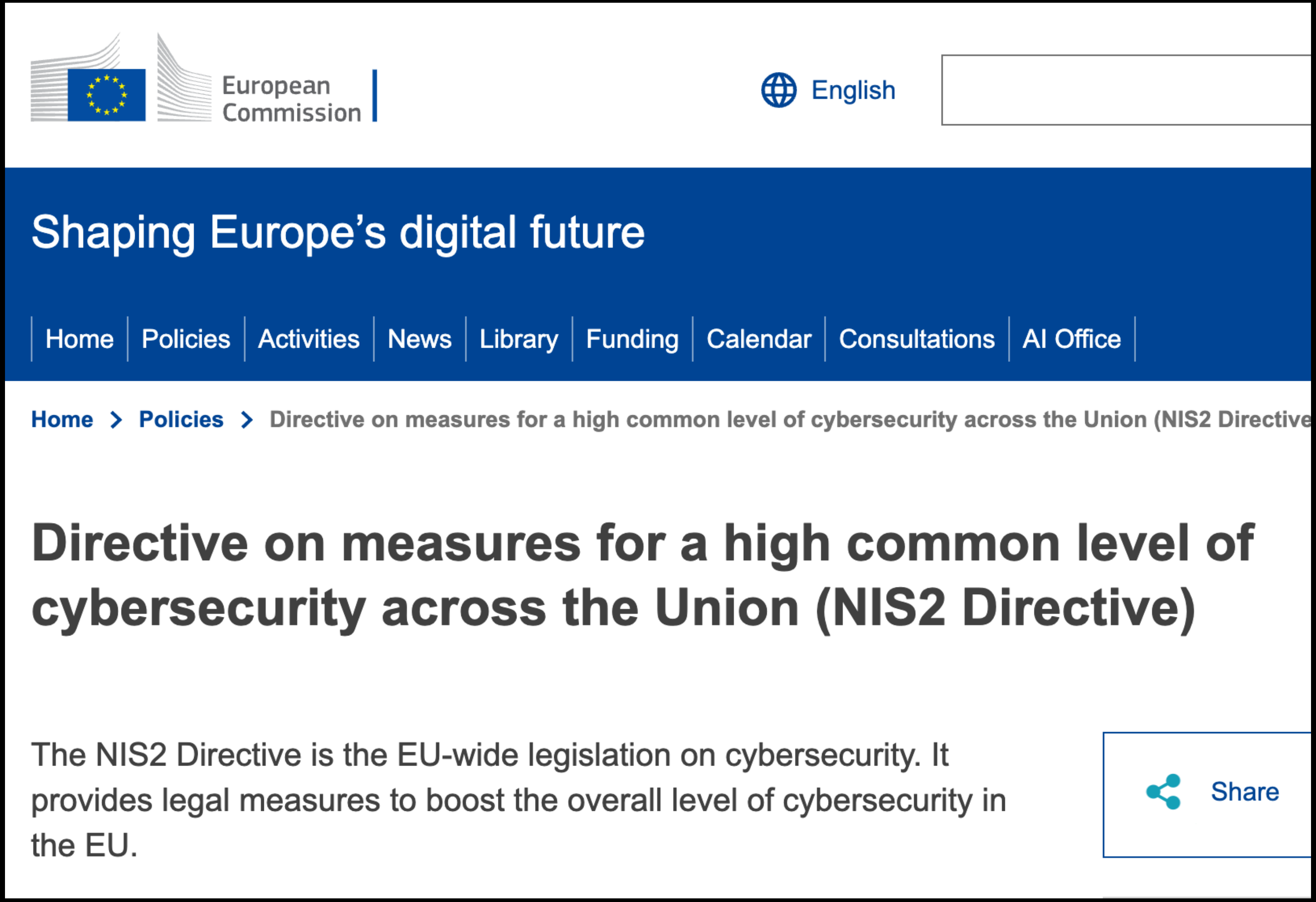
Unlocking Resources?

Lessons & Implications

https://media.istockphoto.com/id/160429199/photo/golden-pot-full-of-gold-coins-against-a-white-background.jpg?s=612x612&w=0&k=20&c=sq7GU--gNhRSnoQp9mAil8KBRmG4PqW1FjS5RqVxTbM=

Or Carrying Sticks?

Lessons & Implications



European Commission
English
Shaping Europe's digital future
Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office
Share

Home > Policies > Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Seeking Alignment

Lessons & Implications

Complex, Long-Running Threats (Whether Cyber, Climate, Or Similar) Require Aligning Long-Term & Specific/Short-Term Interests To Adequately Address & Combat Them

Questions?

References

- “Volt Typhoon targets US critical infrastructure with living-off-the-land techniques” – Microsoft Threat Intelligence (https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/)
- “People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection” – US CISA (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a)
- “China’s cyber army is invading critical U.S. services” – Ellen Nakashima & Joseph Menn, The Washington Post (https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/)
- “China Hacks US Critical Networks in Guam, Raising Cyberwar Fears” – Andy Greenberg & Lily Hay Newman, Wired (https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/)
- “Routers Roasting On An Open Firewall: The KV-Botnet Investigation” – Black Lotus Labs (https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/)
- “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure” – U.S. Department of Justice (https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical)
- “Taking The Crossroads: The Versa Director Zero-Day Exploitation” – Black Lotus Labs (https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/)
- ”Any number of given Volt Typhoon victims ‘likely an underestimate,’ CISA says” – Jonathan Greig & Martin Matishak, The Record (https://therecord.media/volt-typhoon-targets-underestimated-cisa-says)
- “Major Chinese hacking group ‘active to this day’ despite US efforts to stop them” – Maggie Miller, Politico (https://www.politico.com/news/2024/08/09/china-hacking-group-cybersecurity-00173454)
- “The Disclosure Dilemma and Ensuring Defense” - Joe Slowik, FIRST CTI (https://www.youtube.com/watch?v=Cuhs4EJqxMw)