CYBERSECURITY

# FLIPPING THE SCRIPT

Imposing our will on the adversary requires changing mindsets and challenging orthodoxies

# Scott Fogarty

RIDGEBACK

# Tim Solie

PHASE II

# Traditional cybersecurity technologies, including AI, have gaps.

New tools that complement traditional solutions can fill gaps and expedite mission objectives.

**Fact-based Situational Awareness**

**Drive Decision Dominance**

**Bias for Action**


# Agenda

- Real world example parallels cyber challenge
- IT security: evolutions in signal classification
- Deterministic (fact-based) solutions in cyber
- How adding fact-based solutions can help


GAZA
OCTOBER 7, 2023

# Israel defense posture

- Gaza – 25 miles x 6 miles
- Fenced / walled
- Intensively covered by surveillance & detection systems
  - Ground sensors
  - RADAR
  - Cameras
  - Comms. monitoring
- Less HUMINT

Home ▸ The October 7 Hamas attack: An Israeli overreliance on technology?

# The October 7 Hamas attack: An Israeli overreliance on technology?

MIDDLE EAST INSTITUTE. OCT 23, 2023

ANALYSIS

## Israel's Military Tech Fetish Is a Failed Strategy

A fixation on technology created an illusion of safety—and an excuse to avoid hard choices.

FOREIGN POLICY. OCT 26, 2023

Technology

## Hamas assault on Israel shows surprise still possible in AI era: Peter Apps

**Reuters**

October 9, 2023 7:03 PM EDT · Updated 3 months ago


REUTERS. OCT 9, 2023

## Israel's Failure to Stop the Hamas Attack Shows the Danger of Too Much Surveillance

**Hundreds dead, thousands wounded—Hamas' surprise attack on Israel shows the limits of even the most advanced and invasive surveillance dragnets as full-scale war erupts.**

WIRED. OCT 8, 2023

Home ▸ The October 7 Hamas attack: An Israeli overreliance on technology?

# The October 7 Hamas attack: An Israeli overreliance on technology?

MIDDLE EAST INSTITUTE. OCT 23, 2023

ANALYSIS

## Israel's Military Tech Fetish Is a Failed Strategy

A fixation on technology created an illusion of safety—and an excuse to avoid hard choices.

FOREIGN POLICY. OCT 26, 2023

Technology

## Hamas assault on Israel shows surprise still possible in AI era: Peter Apps

Reuters

October 9, 2023 7:03 PM EDT · Updated 3 months ago

REUTERS. OCT 9, 2023

## Israel's Failure to Stop the Hamas Attack Shows the Danger of Too Much Surveillance

Hundreds dead, thousands wounded—Hamas' surprise attack on Israel shows the limits of even the most advanced and invasive surveillance dragnets as full-scale war erupts.

WIRED. OCT 8, 2023

**Misplaced confidence. Broken decision loops.**

# How was monitoring subverted?

1. **Degrade**
   Sensors & monitoring stations disabled by snipers / drones.

2. **Distract**
   Thousands of rockets fired overwhelm air defenses.

3. **Attack**
   Unexpected attack vectors at 30 breach points.
   - Paragliders
   - Mopeds
   - Tunneling

DAILY MAIL. OCT 7, 2023

# Insights

- The enemy has a vote – they plan as students of their adversary's capabilities.
- Information must be accurate, timely, accessible – and linked with action.

Surveillance and detection need real time overwatch.

Are there parallels between
Gaza and the current state of cyber?

# Agenda

- Real world example parallels cyber challenge
- IT security: evolutions in signal classification
- Deterministic (fact-based) solutions in cyber
- How adding fact-based solutions can help

# Evolution of Cybersecurity Techniques



Firewall, Antivirus

IDS, IPS

SIEM

EDR, XDR, UBA

1980s

1990s

2000s

2010+

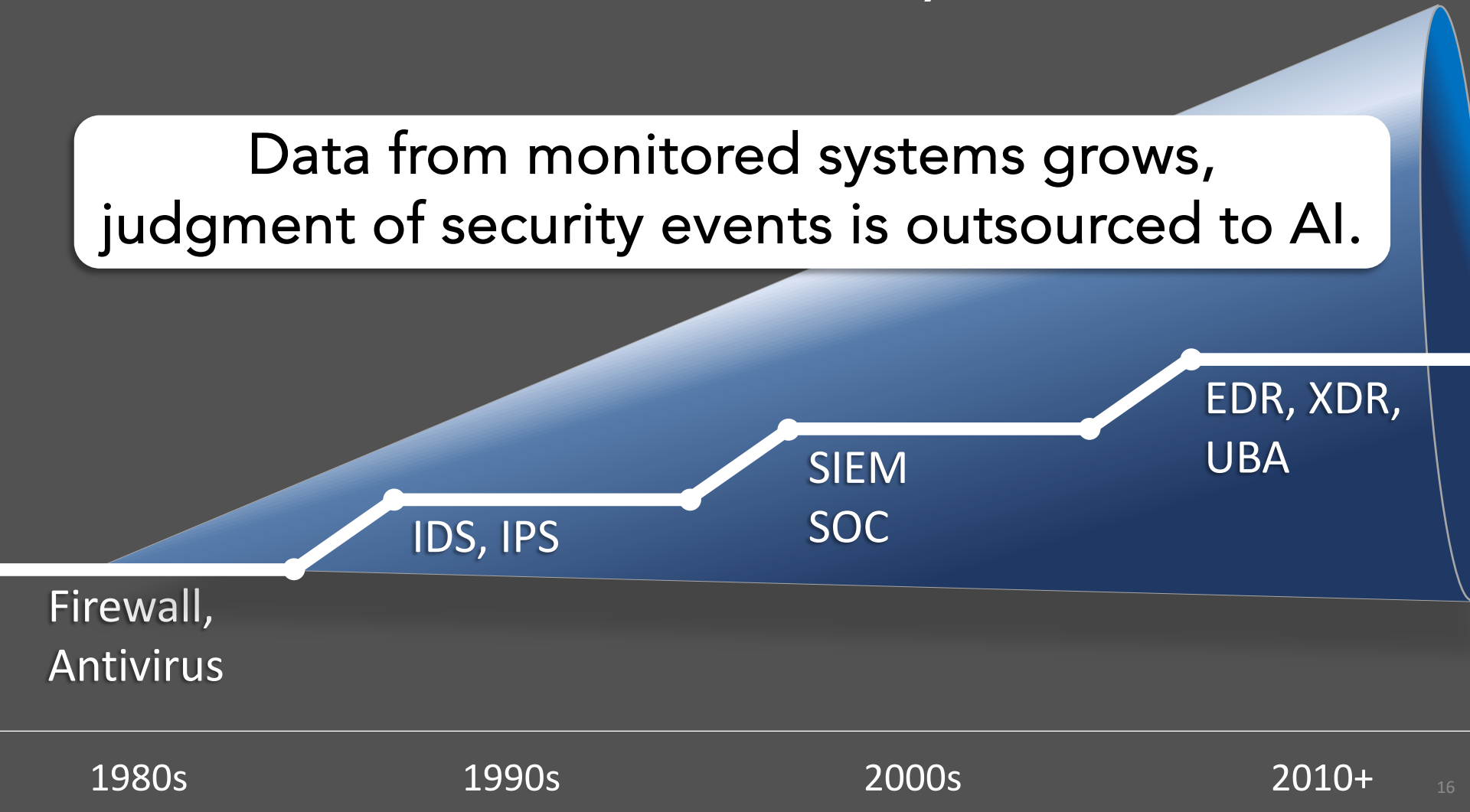
# Signal Classification

## Monitor, Analyze, Alert, Respond

# A.I.

Statistical models infer malicious behavior

# Data Volume Increases, AI Assists



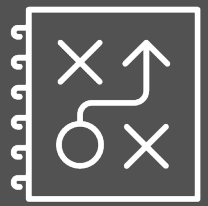
# A.I.

building brand equity since 1950

# Probabilities change when an adversary is involved…

Adversaries inject signals to break models or to ‘modify normal’

Adversaries escape detection by using unexpected techniques



Adversaries use the same AI for offense we use for defense

…still an arms race

# How much do we spend on solutions globally?

| $111 Billion | $213 Billion |
| --- | --- |
| 2018 | 2023 |

**+$100 Billion**

*Double the focus of effort*

Source: PANW August 2023

Cost of a Data Breach Report 2023

# How was the security breach identified?


Only one-third of breaches were identified by security teams and systems.

## How much do we spend on solutions globally?

| $111 Billion | $213 Billion |
|---|---|
| 2018 | 2023 |

**+$100 Billion**

*Double the focus of effort*

Source: PANW August 2023

## What is average adversary dwell time?

| 257 Days | 277 Days |
|---|---|
| 2017 | 2023 |

**+3 weeks**

Source: IBM Cost of a Data Breach, 2023

Gartner

# Stop Performing Cybersecurity Theater: It Is No Longer Scaling

Cybersecurity theater refers to actions that purport to reduce risk, without actually doing so, and it's endemic. The size and complexity of the digital asset base is now so significant that cybersecurity leaders can't keep up with the demand to pretend to protect everything, let alone do so.

March 2023

# Agenda

- Real world example parallels cyber challenge
- IT security: evolutions in signal classification
- Deterministic (fact-based) solutions in cyber
- How adding fact-based solutions can help


Control is zero-sum
Yampil
Novodruzhesk
Bilohorivka
LYSYCHANSK
Borivsk
Siversk
Mykolaivka
SLOVIANSK
Raihorodok
Toshkivka
Hirske
Novoselivske
Soledar
Zolote
Donetskyi
Sentianivka
Holubivka
Popasna
Pervomaisk
Irmino
Chervonohvardiiske
Stakhanov
Almazna
Briianka
Yuvinka
ALCHEVSK
Myronivskyi
Svitlodarsk
Yuzhna Lomuvatka
Artemivsk
Zorynsk
Yasnohyrivka
Bunavka
Kurdiumivka
Bakhmut
Chasiv Yar
Oleksiievo-Druzhkivka
Raiske
Kostiantynivka
Toretsk
Zalizne
Nelipivka
Nilu-York
Holmivskyi
Debaltseve
Horodyshche
Vuhlehirsk
HORLIVKA
Karlo-Marksove
Bulavynske
Yenakiieve
Panteleimonivka
Pokrovsk
Hrodivka
Ocheretyne
Myrnohrad
Novoekonomichne
Rodynske
Bilytske
Dobropillia
Bilozerske
Udachne
Shevchenko
Novohrodivka
Petrovske
Malomykolaivka
Ivanivka
Sofiivskyi
Novoaidar
Donetske
Barvinkove
Novodonetske
Krasnorichka
KRAMATORSK
Byhasivka

# Deterministic approaches complement big data solutions

| Probability-based | Fact-based |
| --- | --- |
| Statistical models infer whether behavior is malicious. | Actual, observed behavior forms the basis for action. |

# Deterministic approaches complement big data solutions

| Probability-based | Fact-based |
| --- | --- |
| Statistical models infer whether behavior is malicious. | Can the behavior of each endpoint, all on its own, without any analysis, serve as the basis for counter-engagement? |

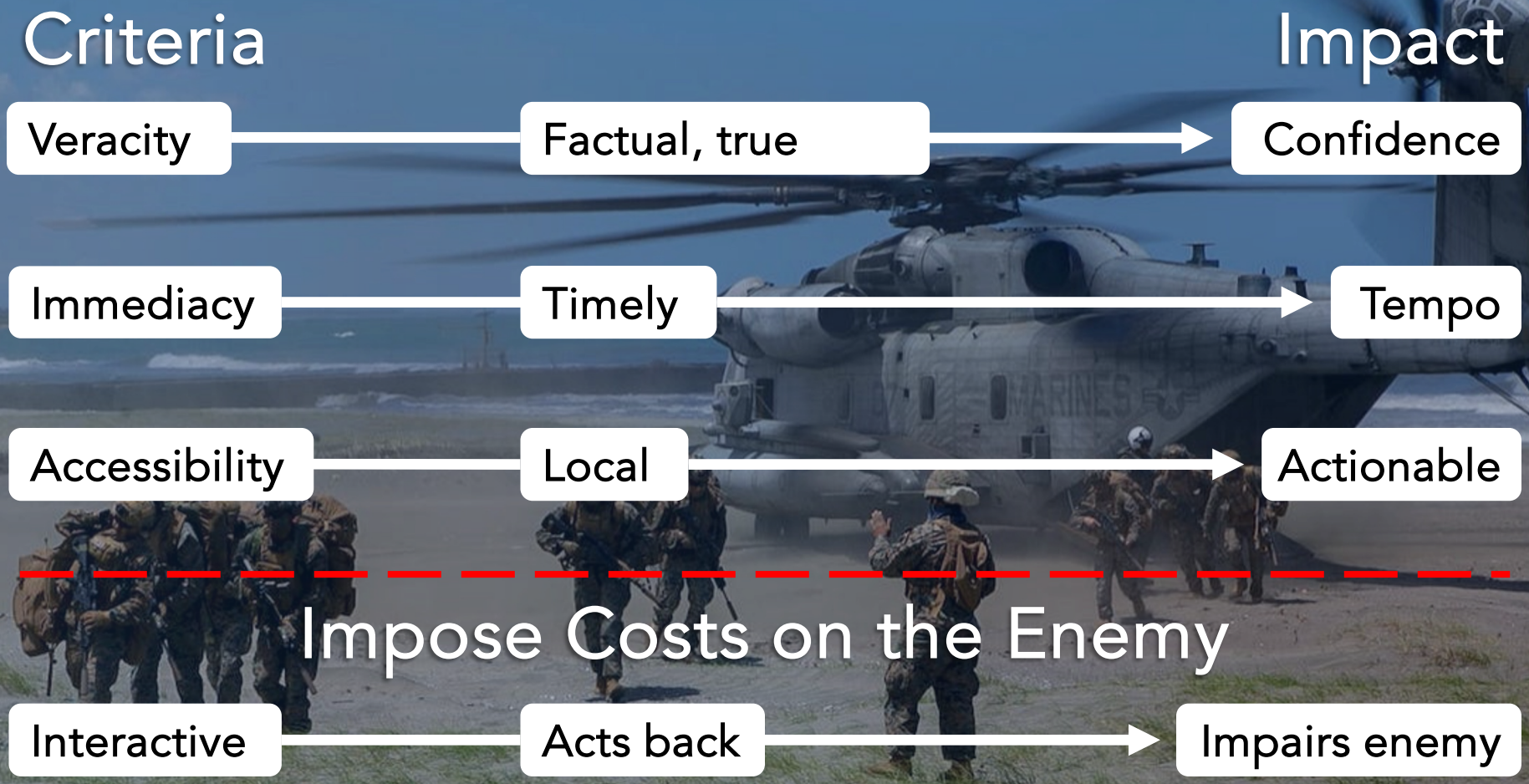
# Deterministic approaches complement big data solutions

| Probability-based | Fact-based |
| --- | --- |
| ▪ After-the-fact | ▪ At connection |
| ▪ Guessing | ▪ No guessing |
| ▪ Central data lakes | ▪ Local data |
| ▪ **Passive** | ▪ **Interactive (fights back)** |
| ▪ **Human response** | ▪ **Automated** |

# Agenda

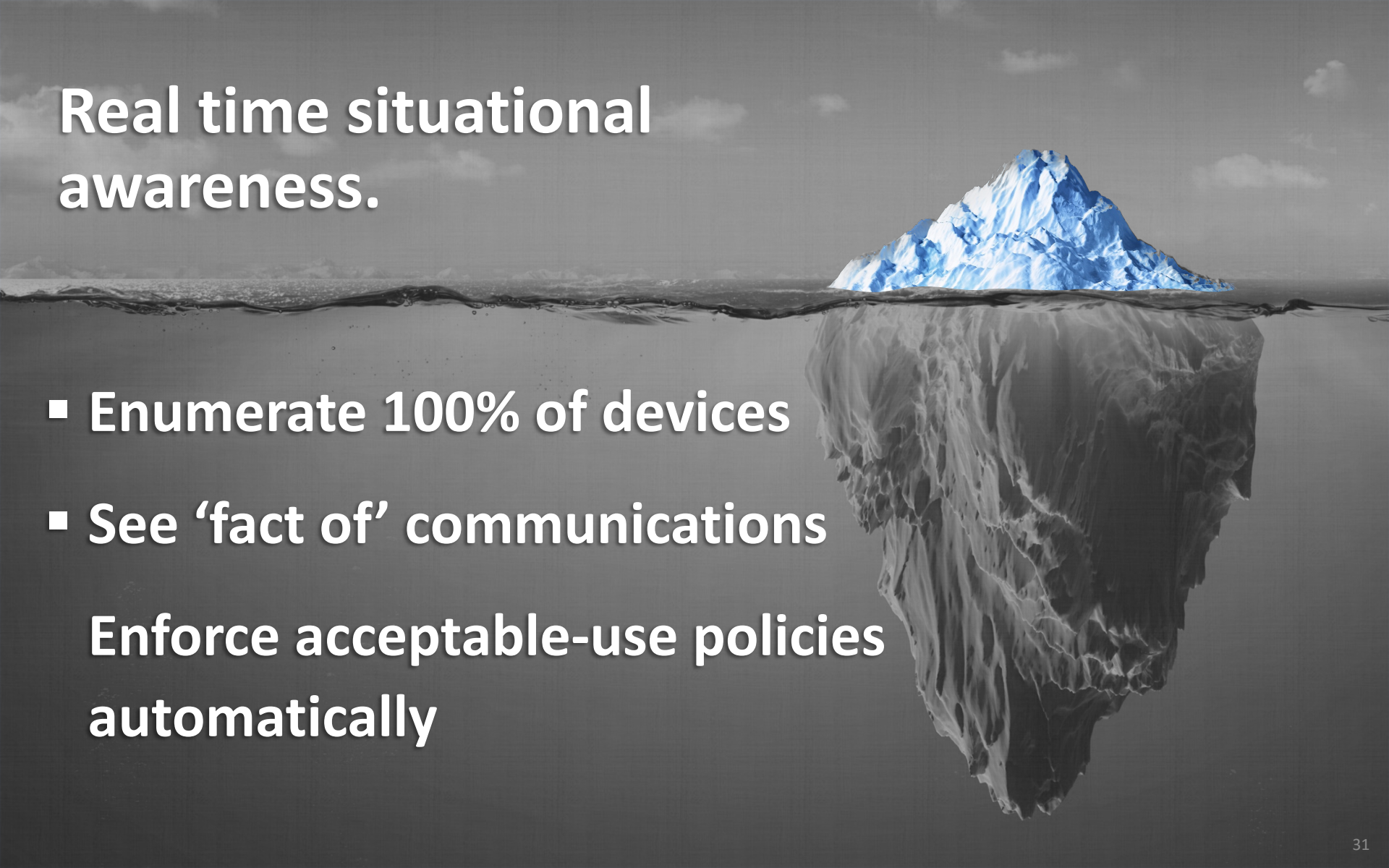
- Real world example parallels cyber challenge
- IT security: evolutions in signal classification
- Deterministic (fact-based) solutions in cyber
- How adding fact-based solutions can help

# Decision Dominance in Cyber



# What can fact-based methods do in a network setting?

# Real time situational awareness.



- Enumerate 100% of devices
- See ‘fact of’ communications

Enforce acceptable-use policies automatically

# Unassigned IPs: The dark space

Active IP addresses

Dark IP addresses

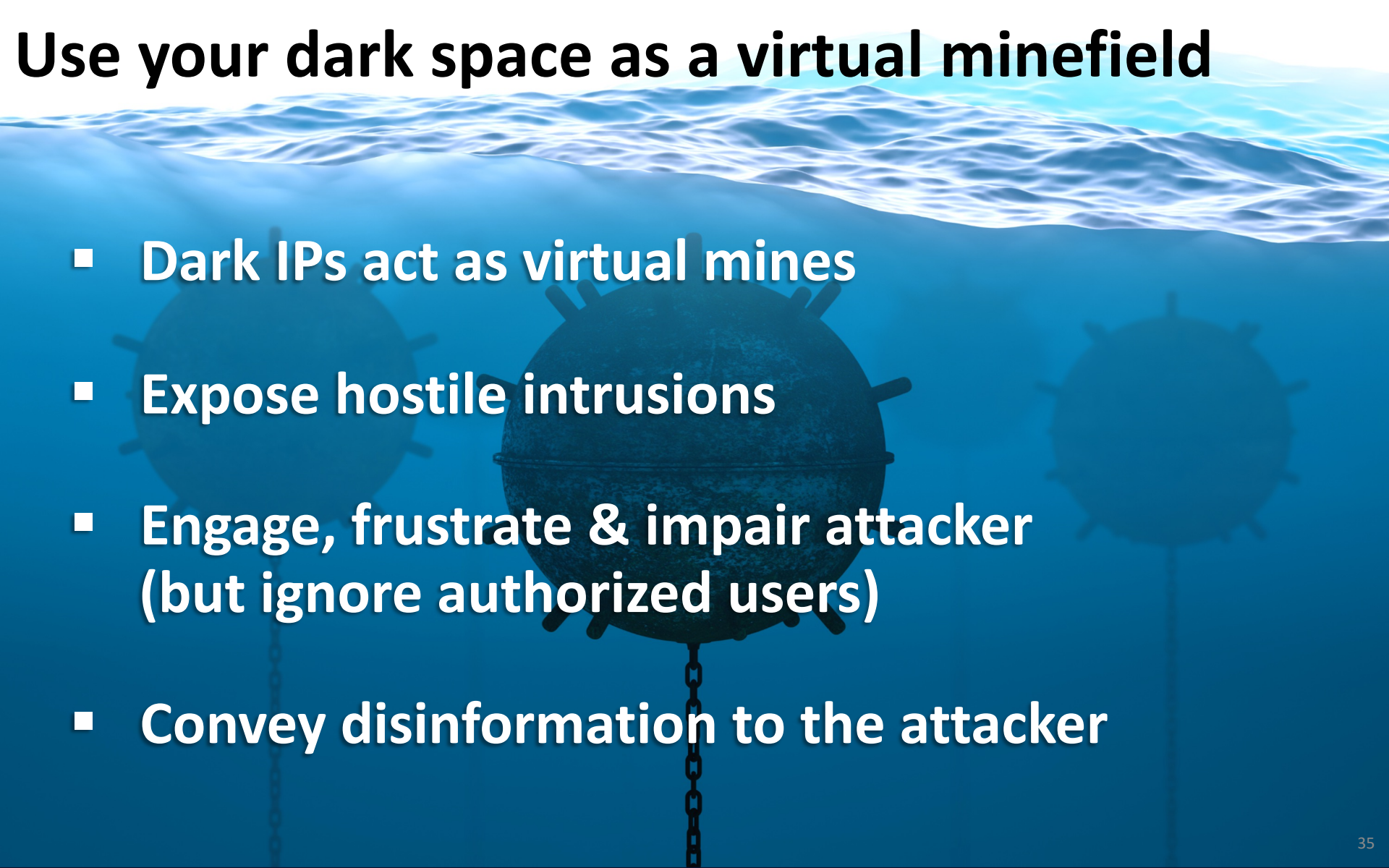
# What do attempts to access the dark space mean?

**Attacks in Progress**

**Productivity & Security Issues**

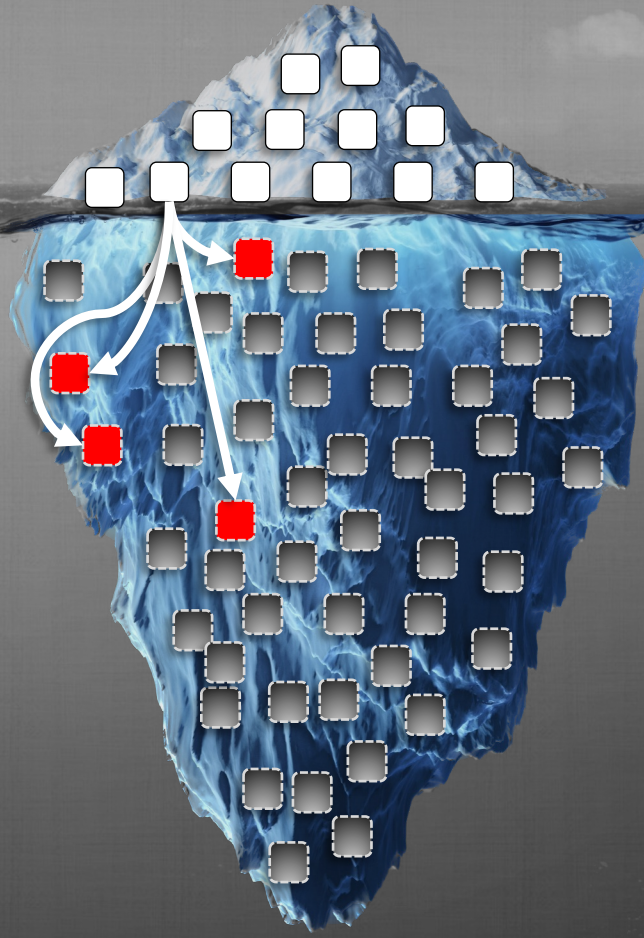
- Intruder Discovery & Enumeration
- Automated Malware Propagation
- Misconfigurations
- Data Leaks

# Use your dark space as a virtual minefield



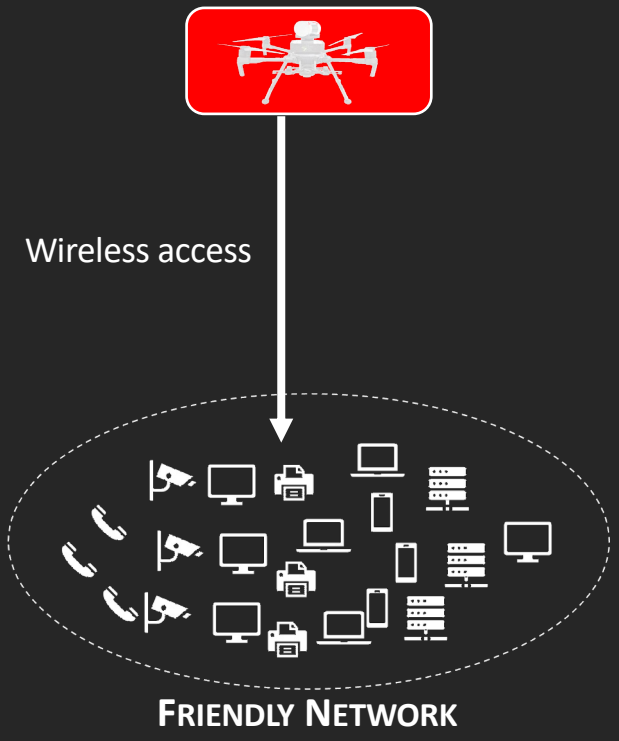
- Dark IPs act as virtual mines
- Expose hostile intrusions
- Engage, frustrate & impair attacker (but ignore authorized users)
- Convey disinformation to the attacker

Intruders can’t navigate your network when mines deliver real time overwatch



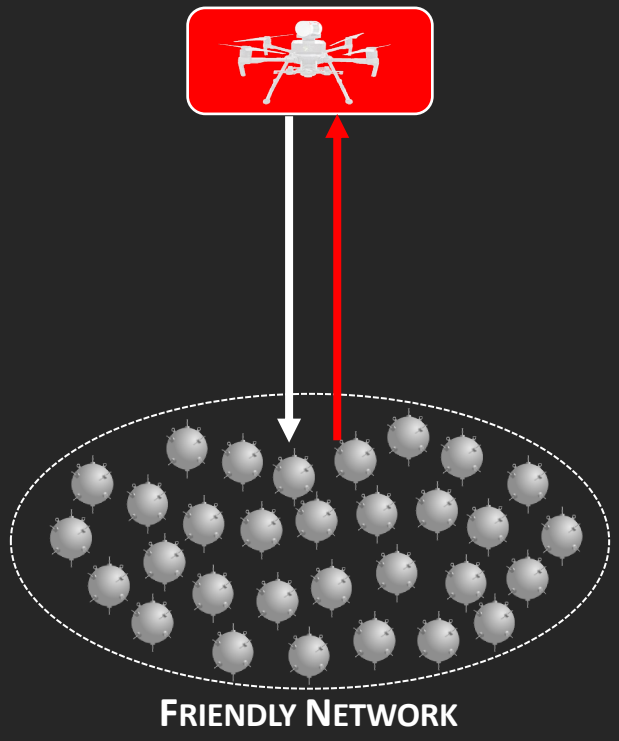
# Real world example: Drone exploit

**ACTUAL:**
**NO INTERACTIVE SOLUTION**

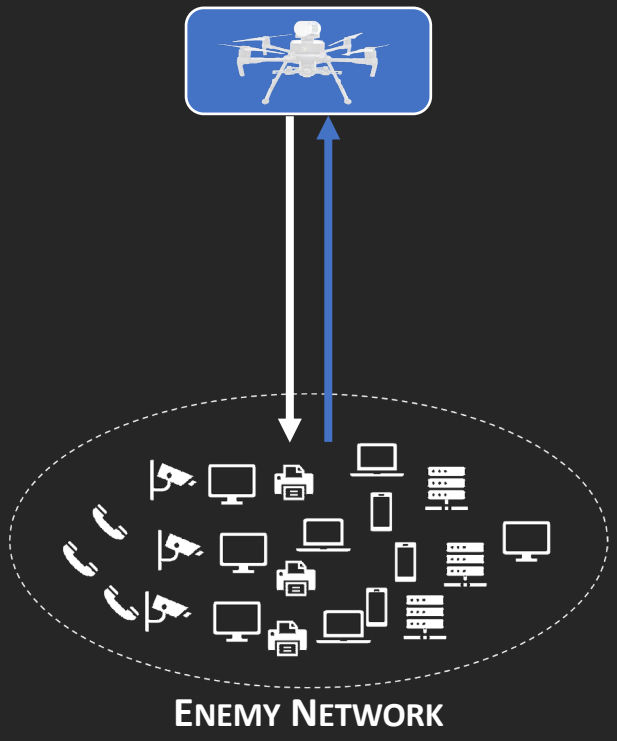



**RED WINS**

**PROPOSED:**
**WITH INTERACTIVE SOLUTION**




**PROPOSED:**
**NON-CONSENSUAL DEPLOYMENT**




**BLUE WINS**

# Fact-based approaches

- Complement Probabilistic / AI
- Drive Decision Dominance
- Counter-engage the Enemy
- Straightforward to Operationalize

# Interactive, Deterministic Solutions

Achieve **data veracity**

Enable **decision dominance**

Add **system overwatch**

# Scott Fogarty

RIDGEBACK

Scott Fogarty is the CEO of Ridgeback Network Defense Inc. The world is in perpetual cyber-war. Together with Ridgeback's founder and inventor, Thomas Phillips, Scott leads Ridgeback, building and deploying tools that battle despicable criminals who would rob our families, hijack our hospitals, and impose on our economic freedoms. Ridgeback's approach draws on using a range of techniques that automatically engage, disrupt, and impair attackers during connection.

Ridgeback inventor Phillips worked with the US Intelligence Community for 25 years following his military service as a USMC Russian linguist.

Prior to Ridgeback, Scott has led and founded media, information and technology companies as CEO. Prior to his career in general management, Scott was responsible for $1.5 billion in information industry Private Equity and Venture Capital investments.

# Tim Solie

PHASE II

Colonel (Ret) Timothy Solie is the Chief Information Security Officer for Phase II. Tim works with partners along the technology corridor to develop emerging technologies and assist new businesses to deliver emerging capabilities to the government.

COL Solie retired from the United States Army at the rank of Colonel. While on active duty, he last served as the Requirements and Resourcing Division Chief for the Cyberspace Directorate, Office of the Deputy Chief of Staff, G3/5/7, Headquarters, Department of the Army. Prior to assignment at the Pentagon, Solie was a key member of the Cyberspace community while he was the Deputy Chief of the Joint Cyber Center (JCC), Headquarters USCENTCOM.

COL Solie received the Defense Superior Service Award for his role impacting ISIS operations in Operation INHERENT RESOLVE, and the Bronze Star for Service with the 101st Airborne Division in Operation Iraqi Freedom in 2003.