Industry 5.0 versus The Growing Threat Landscape

Balancing Innovation versus Security Threats

Cristina Dolan

Prof. Columbia University
Crimson Vista (Cybersecurity)
Board Director -NASDAQ: SEALSQ & GRIID

Every technological revolution is driven by the **optimism** to envision a better future...

...with the **courage** to build it!

The Knowledge-Economy Promise

- Data-driven Innovation
  - Data Growth
  - Proliferation of connected devices
  - Critical infrastructure heavily digitized
  - AI-Powered Edge Computing
  - AI-enabled IoT Devices
- Human-AI Collaboration
  - Human 'Jobs' using AI to perform 'tasks'
  - New insights and solutions
- Goldman Sachs:
  - 7% Growth Global GDP over next 10 years
  - $7 Trillion Value
  - 1.5% labor productivity increase
  - AI companies' 2x net income in a year

UNFORTUNATELY

Expanding Threat Landscape

- Increasing complexity
- Increasing connectivity
- Increasing data value
- Cascading effects of attacks

Weaponization of Cyber

- Geopolitical Threats
- Criminal Motivations

"Cyber is the most immediate, financially material sustainability risk organizations face today – and adversaries weaponize it."

Why Target Infrastructure?

- Disrupt Essential Services
- High Cost of Remediation
- Sensitive or Critical Data
- Cascading Effects

RANSOMWARE: High potential for payout –urgency

DDoS : Quick execution and disruption

PHISHING & SOCIAL ENGINEERING: Human vulnerability

IoT ATTACKS: Many vulnerable devices

MALWARE: Versatile and destructive

INSIDER THREATS: Leverage access

SUPPLY CHAIN ATTACKS: Multiple Targets

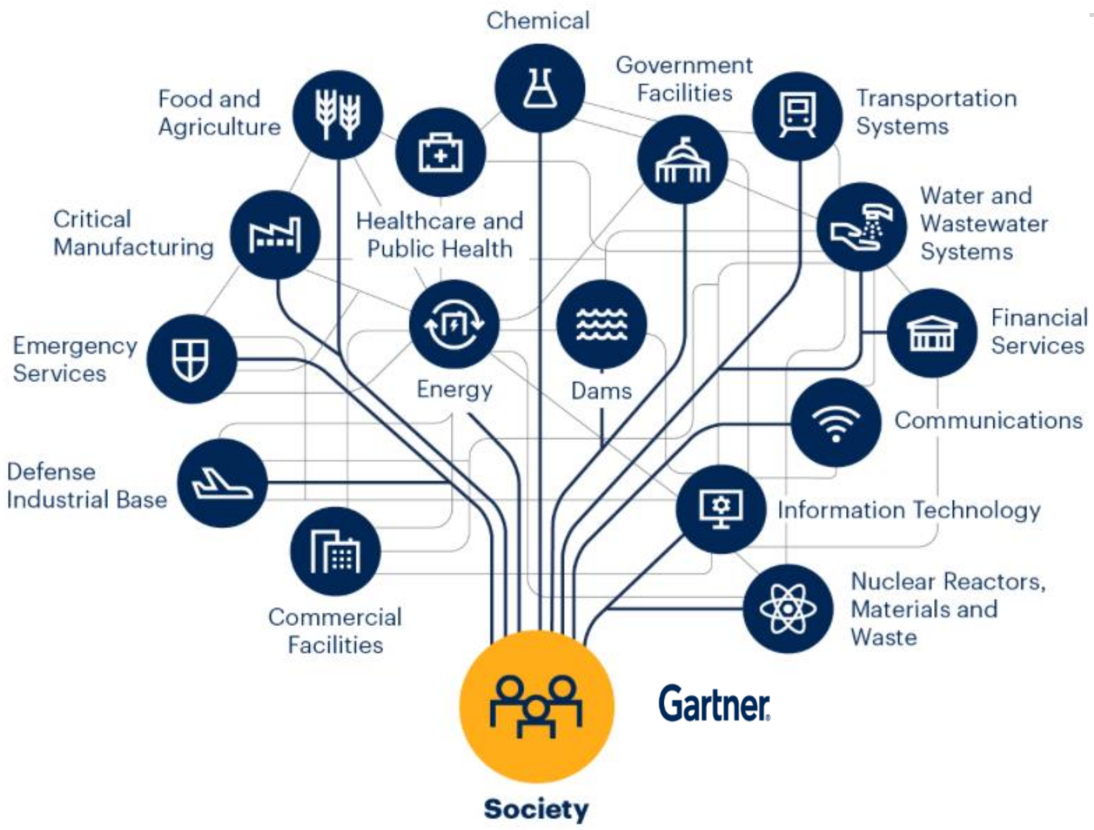
REMOTE ACCESS EXPLOITATION: Vulnerabilities

CYBER-PHYSICAL ATTACKS: Physical impacts

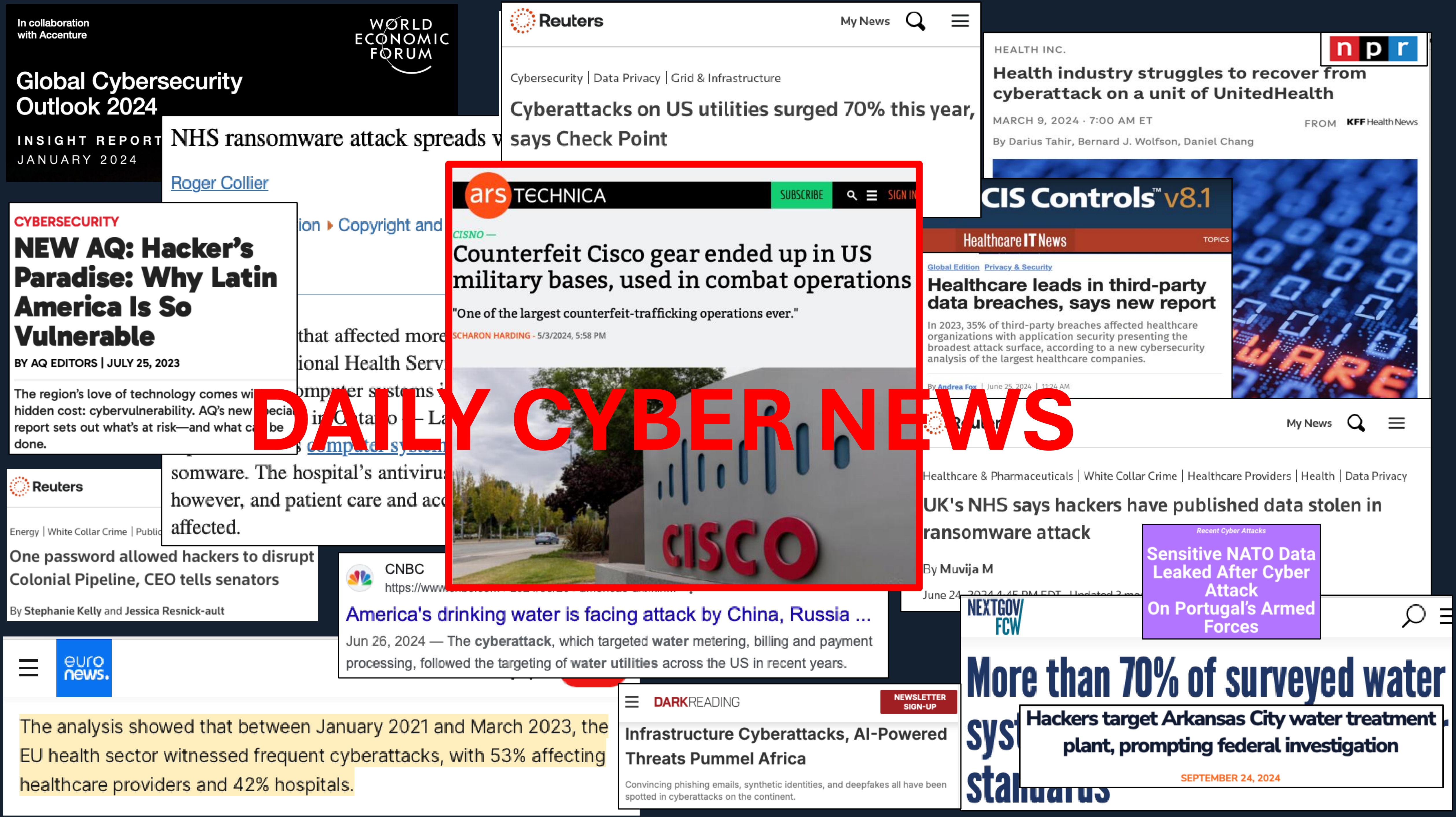
DATA MANIPULATION: Critical data integrity

INDUSTRIAL ESPIONAGE: IP and Infrastructure

EXPLOITATION PUBLIC APPLICATIONS: Fear



DAILY CYBER NEWS



In collaboration with Accenture

WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2024

INSIGHT REPORT
JANUARY 2024

NHS ransomware attack spreads w

Roger Collier

ion ▸ Copyright and

that affected more
ional Health Serv
mputer systems i
in Ontario – La
s computer system
somware. The hospital's antivirus
however, and patient care and acc
affected.

CYBERSECURITY

NEW AQ: Hacker's Paradise: Why Latin America Is So Vulnerable

BY AQ EDITORS | JULY 25, 2023

The region's love of technology comes wi hidden cost: cybervulnerability. AQ's new specia report sets out what's at risk—and what ca be done.

Reuters

Energy | White Collar Crime | Public

One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

By Stephanie Kelly and Jessica Resnick-ault

Reuters My News

Cybersecurity | Data Privacy | Grid & Infrastructure

Cyberattacks on US utilities surged 70% this year, says Check Point

ars TECHNICA SUBSCRIBE SIGN IN

CISNO —

Counterfeit Cisco gear ended up in US military bases, used in combat operations

"One of the largest counterfeit-trafficking operations ever."

SCHARON HARDING - 5/3/2024, 5:58 PM

HEALTH INC. npr

Health industry struggles to recover from cyberattack on a unit of UnitedHealth

MARCH 9, 2024 · 7:00 AM ET FROM KFF Health News

By Darius Tahir, Bernard J. Wolfson, Daniel Chang

CIS Controls™ v8.1

Healthcare IT News TOPICS

Global Edition Privacy & Security

Healthcare leads in third-party data breaches, says new report

In 2023, 35% of third-party breaches affected healthcare organizations with application security presenting the broadest attack surface, according to a new cybersecurity analysis of the largest healthcare companies.

By Andrea Fox | June 25, 2024 | 11:24 AM

Reuters My News

Healthcare & Pharmaceuticals | White Collar Crime | Healthcare Providers | Health | Data Privacy

UK's NHS says hackers have published data stolen in ransomware attack

By Muvija M

June 24, 2024 4:45 PM EDT · Updated 3 mo

Recent Cyber Attacks

Sensitive NATO Data Leaked After Cyber Attack On Portugal's Armed Forces

CNBC
https://www.

America's drinking water is facing attack by China, Russia ...

Jun 26, 2024 — The cyberattack, which targeted water metering, billing and payment processing, followed the targeting of water utilities across the US in recent years.

euro news.

The analysis showed that between January 2021 and March 2023, the EU health sector witnessed frequent cyberattacks, with 53% affecting healthcare providers and 42% hospitals.

DARKREADING NEWSLETTER SIGN-UP

Infrastructure Cyberattacks, AI-Powered Threats Pummel Africa

Convincing phishing emails, synthetic identities, and deepfakes all have been spotted in cyberattacks on the continent.

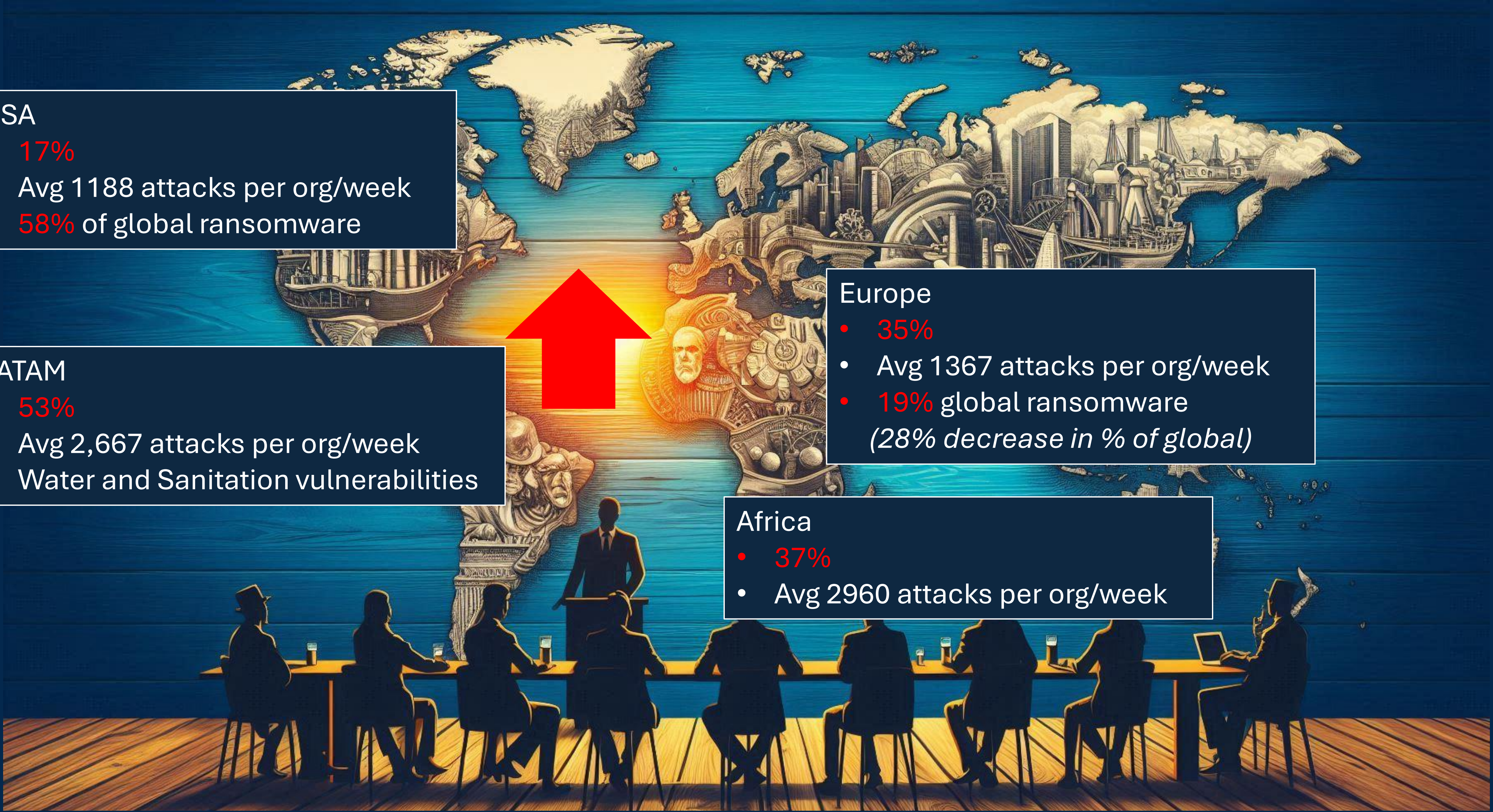
NEXTGOV FCW

More than 70% of surveyed water syst standards

Hackers target Arkansas City water treatment plant, prompting federal investigation

SEPTEMBER 24, 2024

Growth of Cyber Threats – 2024 Q2 Yearly Increase



USA

- 17%
- Avg 1188 attacks per org/week
- 58% of global ransomware

LATAM

- 53%
- Avg 2,667 attacks per org/week
- Water and Sanitation vulnerabilities

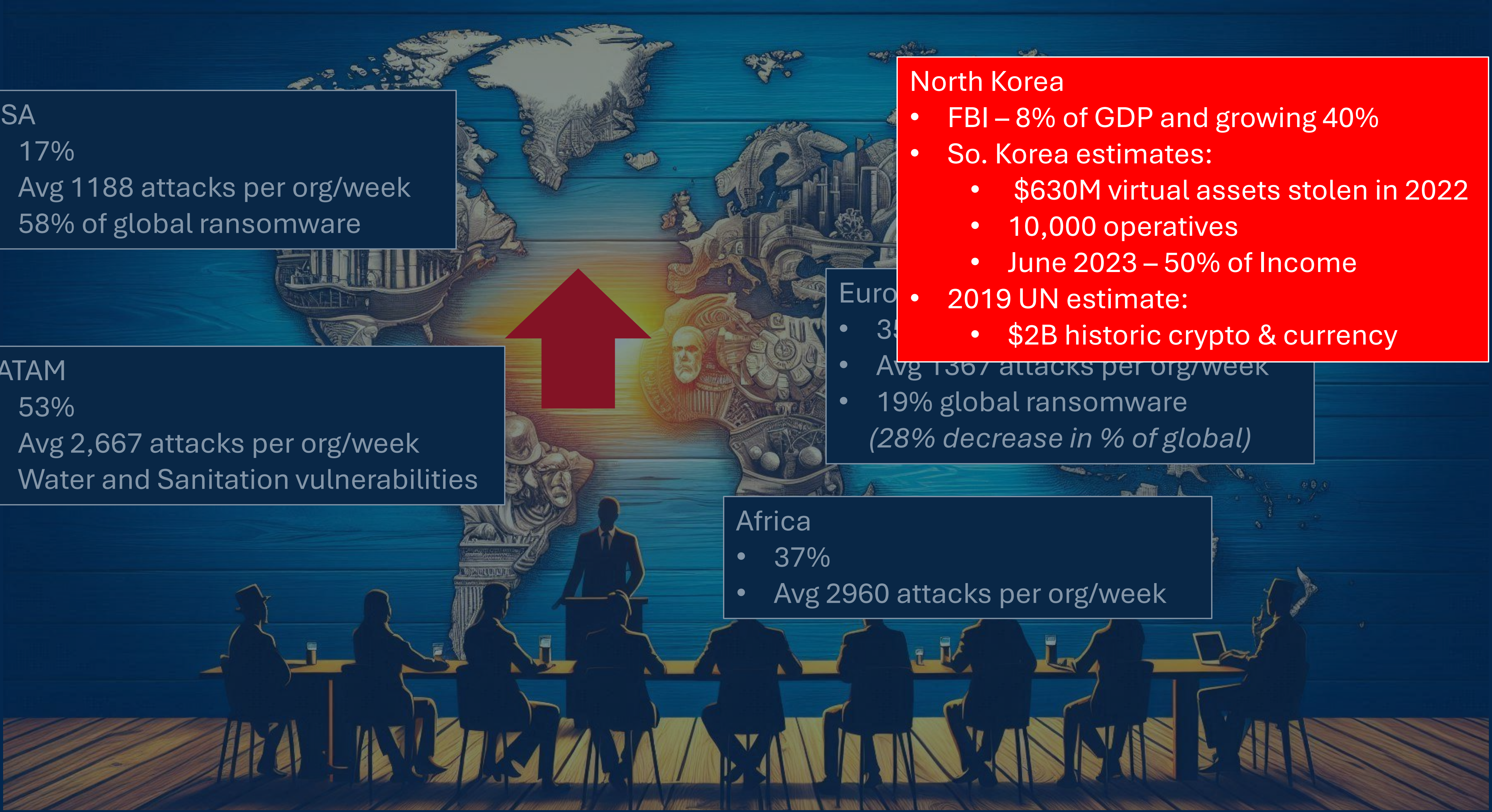
Europe

- 35%
- Avg 1367 attacks per org/week
- 19% global ransomware
  (28% decrease in % of global)

Africa

- 37%
- Avg 2960 attacks per org/week

Growth of Cyber Threats – 2024 Q2 Yearly Increase



USA

- 17%
- Avg 1188 attacks per org/week
- 58% of global ransomware

LATAM

- 53%
- Avg 2,667 attacks per org/week
- Water and Sanitation vulnerabilities

Euro

- 35
- Avg 1367 attacks per org/week
- 19% global ransomware

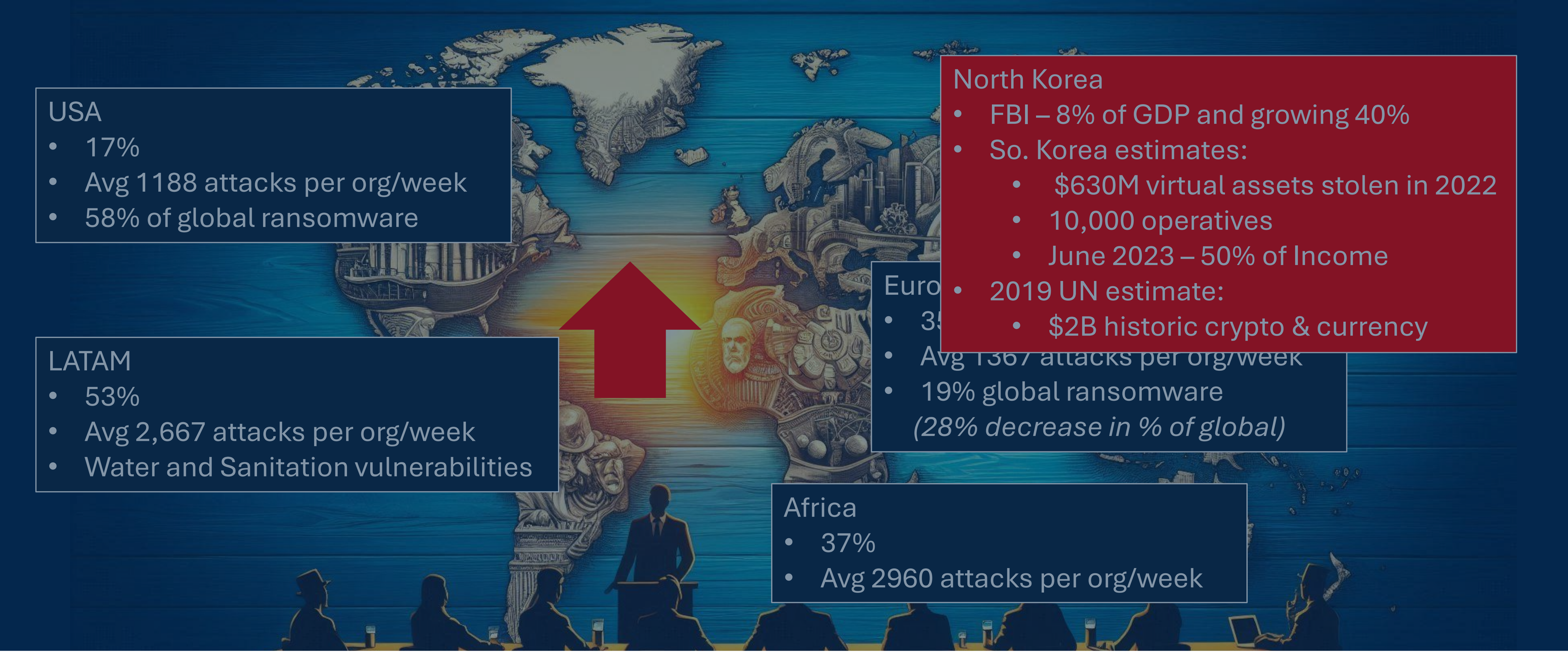
  (28% decrease in % of global)

Africa

- 37%
- Avg 2960 attacks per org/week

North Korea

- FBI – 8% of GDP and growing 40%
- So. Korea estimates:
  - $630M virtual assets stolen in 2022
  - 10,000 operatives
  - June 2023 – 50% of Income
- 2019 UN estimate:
  - $2B historic crypto & currency



USA

- 17%
- Avg 1188 attacks per org/week
- 58% of global ransomware

LATAM

- 53%
- Avg 2,667 attacks per org/week
- Water and Sanitation vulnerabilities

North Korea

- FBI – 8% of GDP and growing 40%
- So. Korea estimates:
  - $630M virtual assets stolen in 2022
  - 10,000 operatives
  - June 2023 – 50% of Income
- 2019 UN estimate:
  - $2B historic crypto & currency

Euro

- 35
- Avg 1367 attacks per org/week
- 19% global ransomware

(28% decrease in % of global)

Africa

- 37%
- Avg 2960 attacks per org/week

GLOBAL

- Cybersecurity Ventures predicts Global Cyber Crime Growth **15%** year over year
- **$9.5** Trillion in 2024
- **$10.5** Trillion in 2025

USA
- 17%
- Avg 1188 attacks per org/week
- 58% of global ransomware

North Korea
- FBI – 8% of GDP and growing 40%
- So. Korea estimates:
  - $630M virtual assets stolen in 2022
  - 10,000 operatives
  - June 2023 – 50% of Income
- 2019 UN estimate:
  - $2B historic crypto & currency

Euro
- 35
- Avg 1367 attacks per org/week

LATAM
- 53
- Avg
- Wa

WHAT IS DRIVING THIS CYBER CRIME & VULNERABILITY GROWTH?

GLOBAL
- Cybersecurity Ventures predicts Global Cyber Crime Growth **15%** year over year
- **$9.5** Trillion in 2024
- **$10.5** Trillion in 2025

Reasons for Vulnerable Infrastructure

1. Aging SCADA and ICS
   [Supervisory Control and Data Acquisition & Industrial Control Systems]
2. Increased Digitalization & Data Growth
3. Lack of Cybersecurity Expertise and Training
4. Social Engineering & Phishing
5. Inadequate Investment in Cybersecurity
6. Growing Sophistication of Attackers
7. Rapid Adoption of IoT Devices
8. Counterfeit or Compromised Network Devices
9. Unpatched Software & Delayed Response
10. Lack of Monitoring
11. Vulnerable Access Points
12. Weak Credentials and Encryption
13. Unsupported Hardware

Reasons for Vulnerable Infrastructure

Antiquated SCADA and IDS

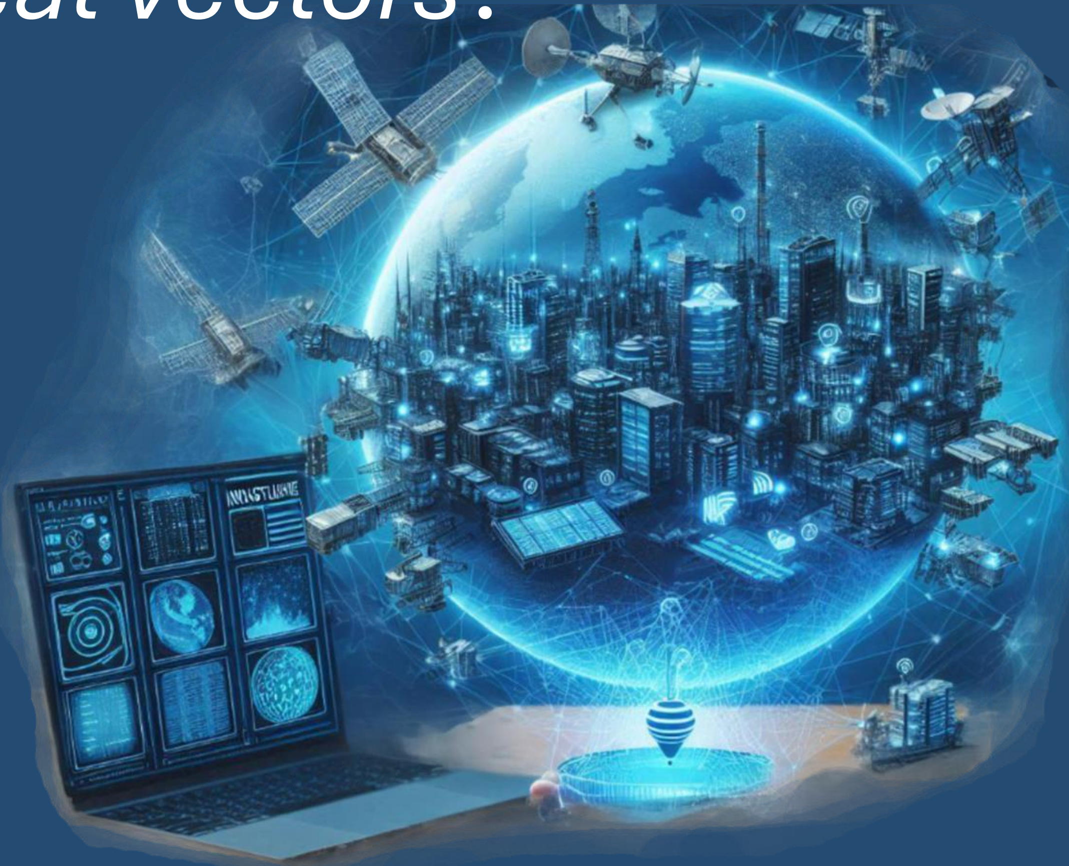
[Supervisory Control and Data Acquisition & Industrial Control Systems]

Region	Antiquated SCADA/ICS Systems	Most Vulnerable Systems & Utilities
North America	40-50%	Power grids, water treatment plants, oil & gas, transportation
LATAM	60-70%	Energy, oil & gas, water systems, transportation
EU	30-40%	Power grids, manufacturing, telecommunication, transport
UK	35-45%	Water utilities, energy (electricity and gas), transport
Nordics	25-35%	Power distribution, telecommunications, healthcare
Africa	70-80%	Energy, water management, agriculture, telecommunications

Vulnerable Infrastructure – Targeted Industry Sectors

1. **Education:** *53% increase in attacks*
2. **Government/Military:** *2,084 attacks/week*
3. **Healthcare:** *1,999 attacks/week*
4. **Utilities:** *186% increase in ransomware (Power/Water) SCADA*
5. **Manufacturing:** *Most ransomware, 29% of attacks*
6. **Communications:** *177% increase in ransomware*
7. **Transportation:** *Vulnerable due to connectivity and automation*

Infrastructure is Evolving Quickly
Will this introduce new threat vectors?



Telecom Infrastructure

- Satellite-based networks growth
- Integration of terrestrial and satellite
- Wider efficiency and coverage

Energy Grid

- Distributed energy resources (DERs)
- Smart Grids

IoT and Edge AI

- Increase in IoT and Tiny AI utilizing local data
- Reduced latency and bandwidth requirements

Infrastructure is Evolving

AI-Powered Chips at the EDGE, IoT and Next Gen SCADA

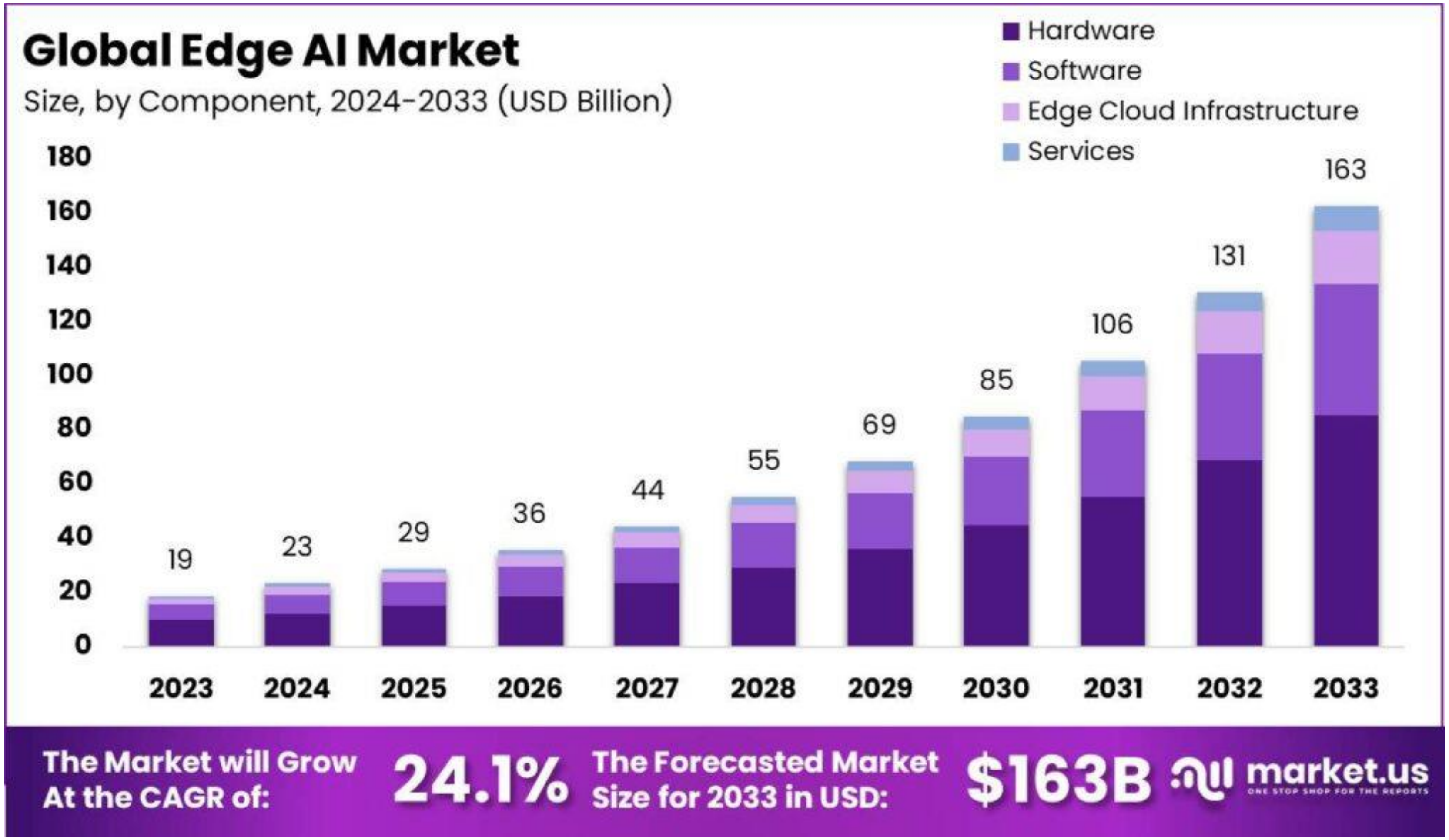
1. Enhanced local processing
2. Local data (Web 3.0)
3. Improved data security
4. Improved speed
5. Reduced data transfer
6. Less Physical Tampering Risks
7. New Attack Vectors

Infrastructure is Evolving

Root Key - Secure Networked IoT and Systems Components

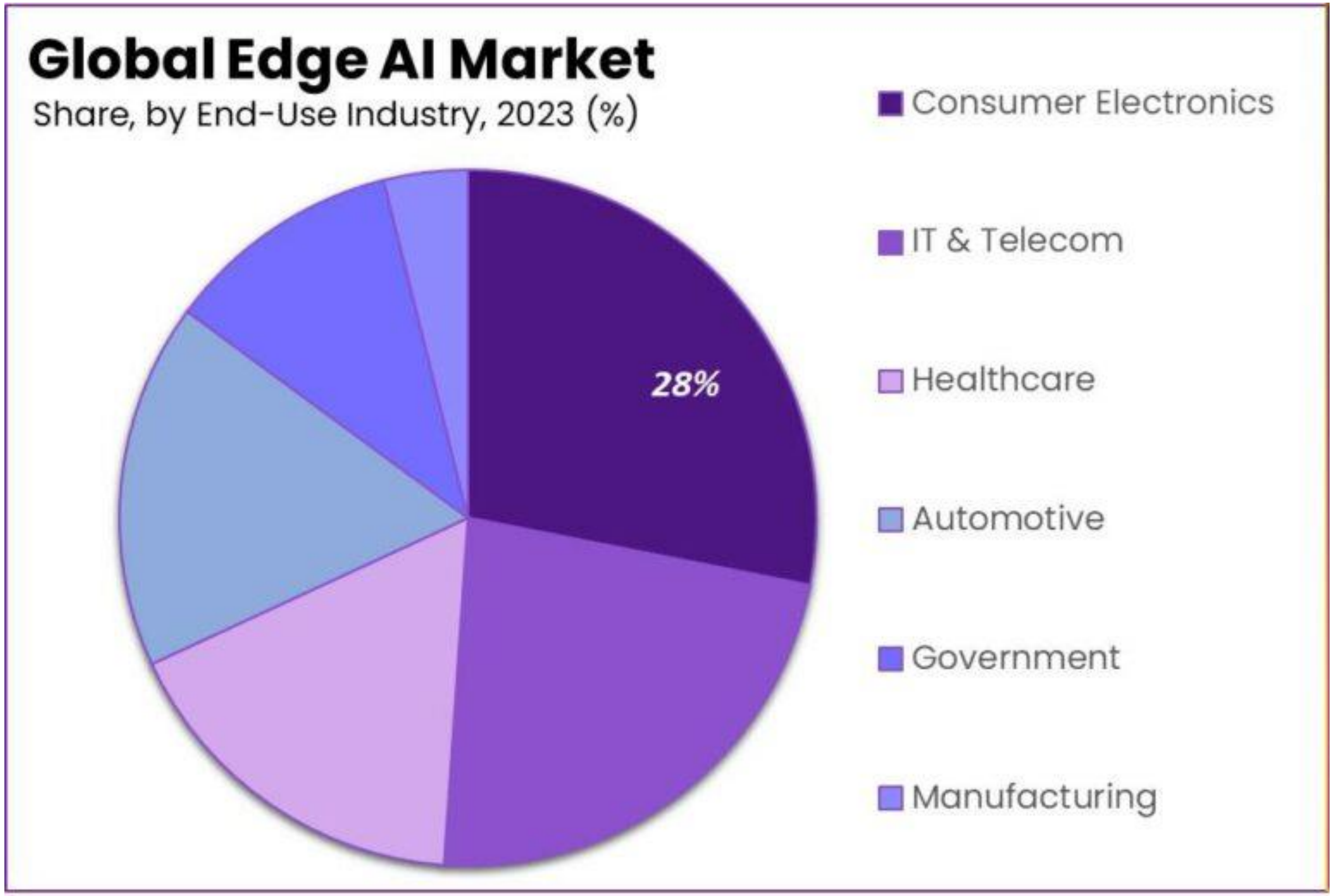
- The Early 2000s
- Device Authentication
- Encryption
- Firmware Integrity
- Key Management
- Secure IoT Networks
- System Components:
  - Hardware Security Module
  - Trusted Platform Module
  - Secure Boot Loader
  - Key Management
  - Cryptographic Libraries

Global Edge AI, IoT, and Industrial Systems



Global Edge AI, IoT, and Industrial Systems

24.1% CAGR 2024-2033

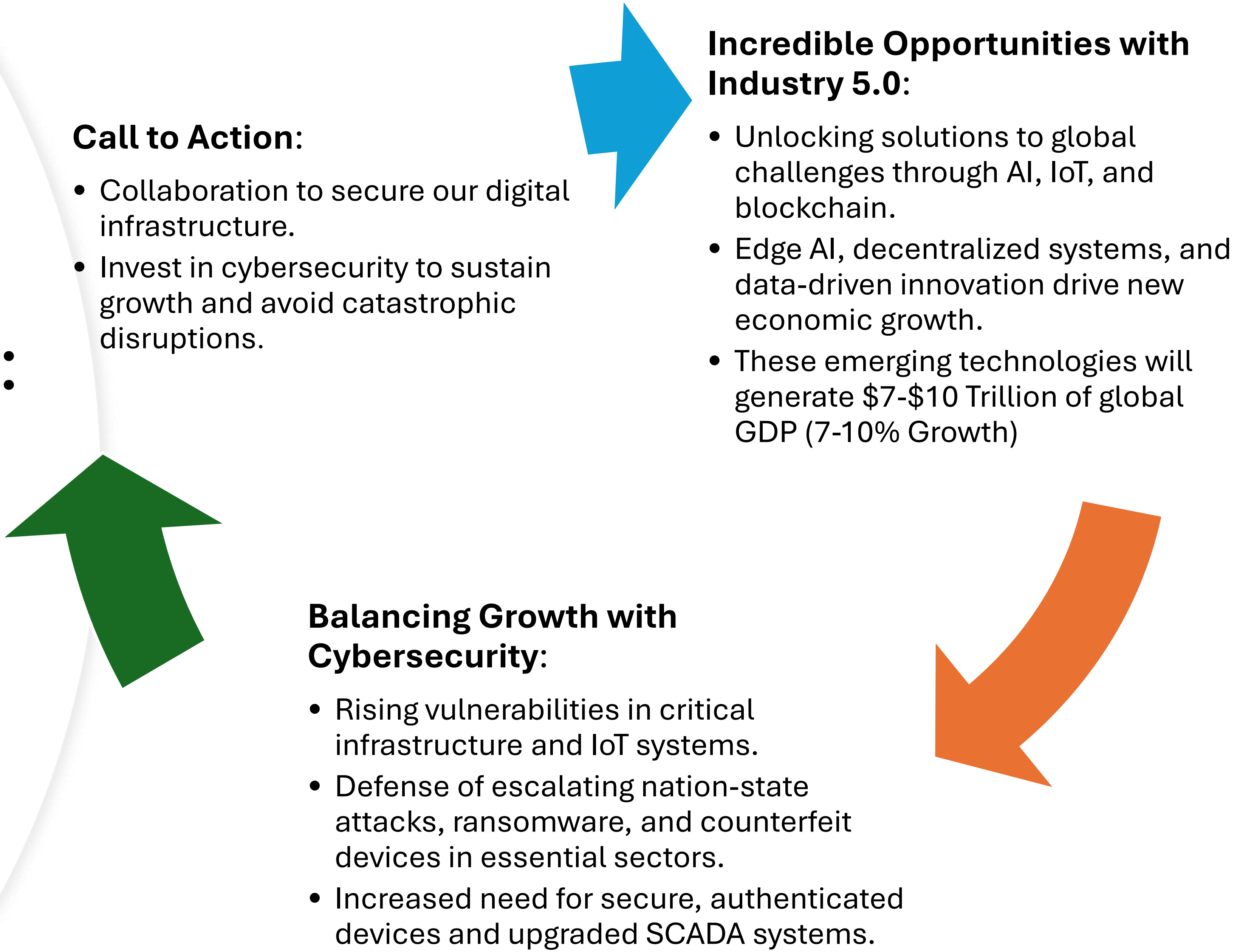


market.us

Cyber Risk Mitigation Strategies

- Update old SCADA/ICS/IoT Devices
- Reduce Human Vulnerabilities with Training
- Multifactor Authentication
- Least Privilege Control
- Unique Passwords
- Network Segmentation of SCADA/ICS Networks
- Continuous Monitoring and Threat Detection
- Vulnerability Assessments
- Supply Chain Security Monitoring
- 3rd Party Risk Assessments
- Encryption and Secure Communications
- Incident Response Planning

The Path Forward: Innovation and Vigilance



Call to Action:

- Collaboration to secure our digital infrastructure.
- Invest in cybersecurity to sustain growth and avoid catastrophic disruptions.

Incredible Opportunities with Industry 5.0:

- Unlocking solutions to global challenges through AI, IoT, and blockchain.
- Edge AI, decentralized systems, and data-driven innovation drive new economic growth.
- These emerging technologies will generate $7-$10 Trillion of global GDP (7-10% Growth)

Balancing Growth with Cybersecurity:

- Rising vulnerabilities in critical infrastructure and IoT systems.
- Defense of escalating nation-state attacks, ransomware, and counterfeit devices in essential sectors.
- Increased need for secure, authenticated devices and upgraded SCADA systems.

Industry 5.0 versus The Growing Threat Landscape

Balancing Innovation versus Security Threats

https://www.linkedin.com/in/cdolan/

Cristina Dolan

Prof. Columbia University
Crimson Vista (Cybersecurity)
Board Director -NASDAQ: SEALSQ & GRIID