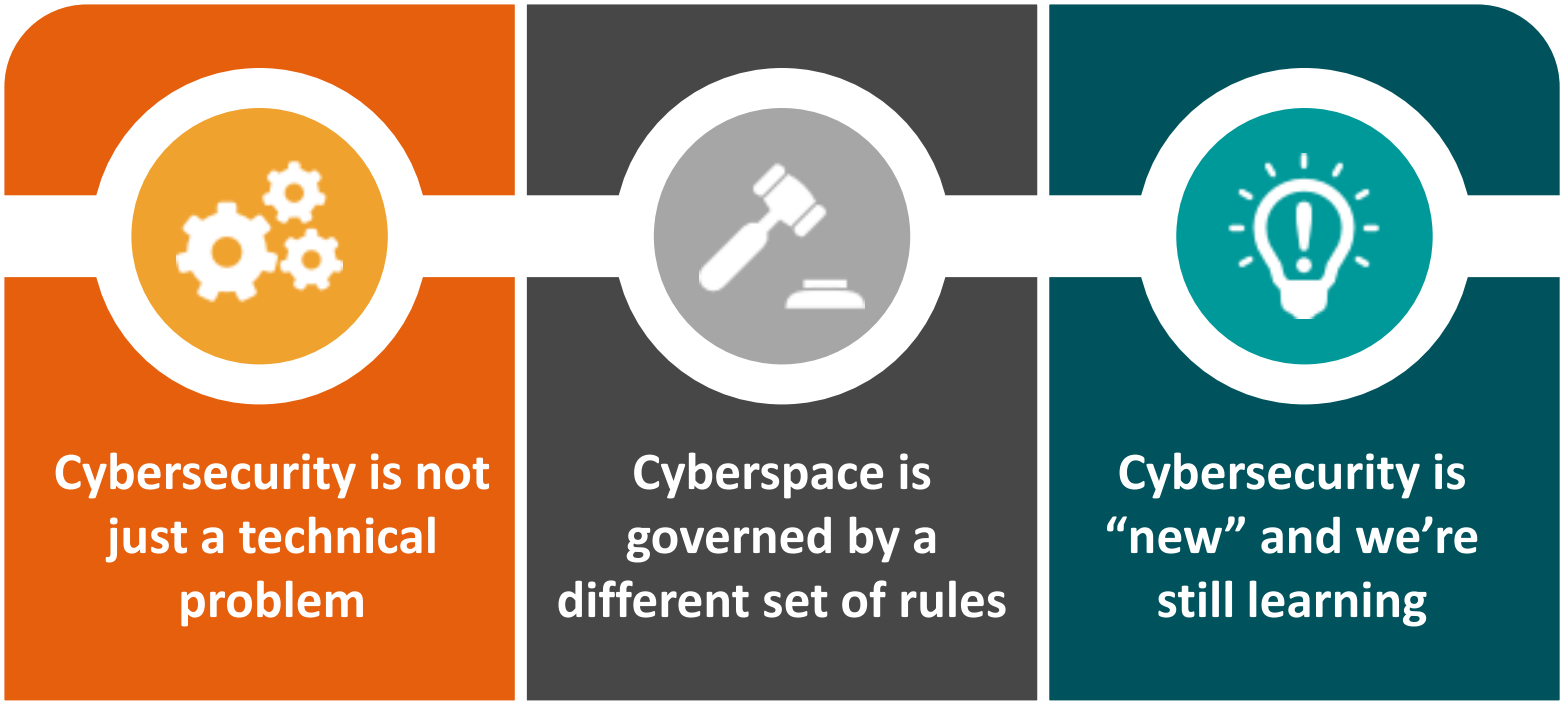
CHANGING THE GAME: A DIFFERENT APPROACH TO CYBERSECURITY

CYBER THREAT ALLIANCE

Michael Daniel
President & CEO

WHY IS CYBERSECURITY A HARD PROBLEM?



Cybersecurity is also an economic, psychological, and human behavioral challenge

The concepts of distance, borders, and proximity all operate differently in cyberspace compared to the physical world

We haven't had the time or the experience to develop the comprehensive frameworks required to address cyber risk

HOW IS THE CYBER THREAT EVOLVING?

Four primary types of cyber adversaries

Hactivists
Act in support of a cause

Criminal Organizations
Profit off malicious activity

Terrorists
Leverage cyberspace to recruit

Nation States
Pursue their national interests

Volume and diversity of connected devices increases complexity

Low barriers to entry and high ROI incentive actors

More broad
The attack surface is exponentially increasing

More frequent
Volume of malicious cyber activity is increasing

Because of these actors, the cyber threat is becoming….

More dangerous
Actors are increasingly moving to more destructive activity

More disruptive
Potential impacts of a cyber incident are increasing

Critical infrastructure is at the center of actors' malicious activity

Digital dependence is making society increasingly vulnerable

CYBER THREAT ALLIANCE

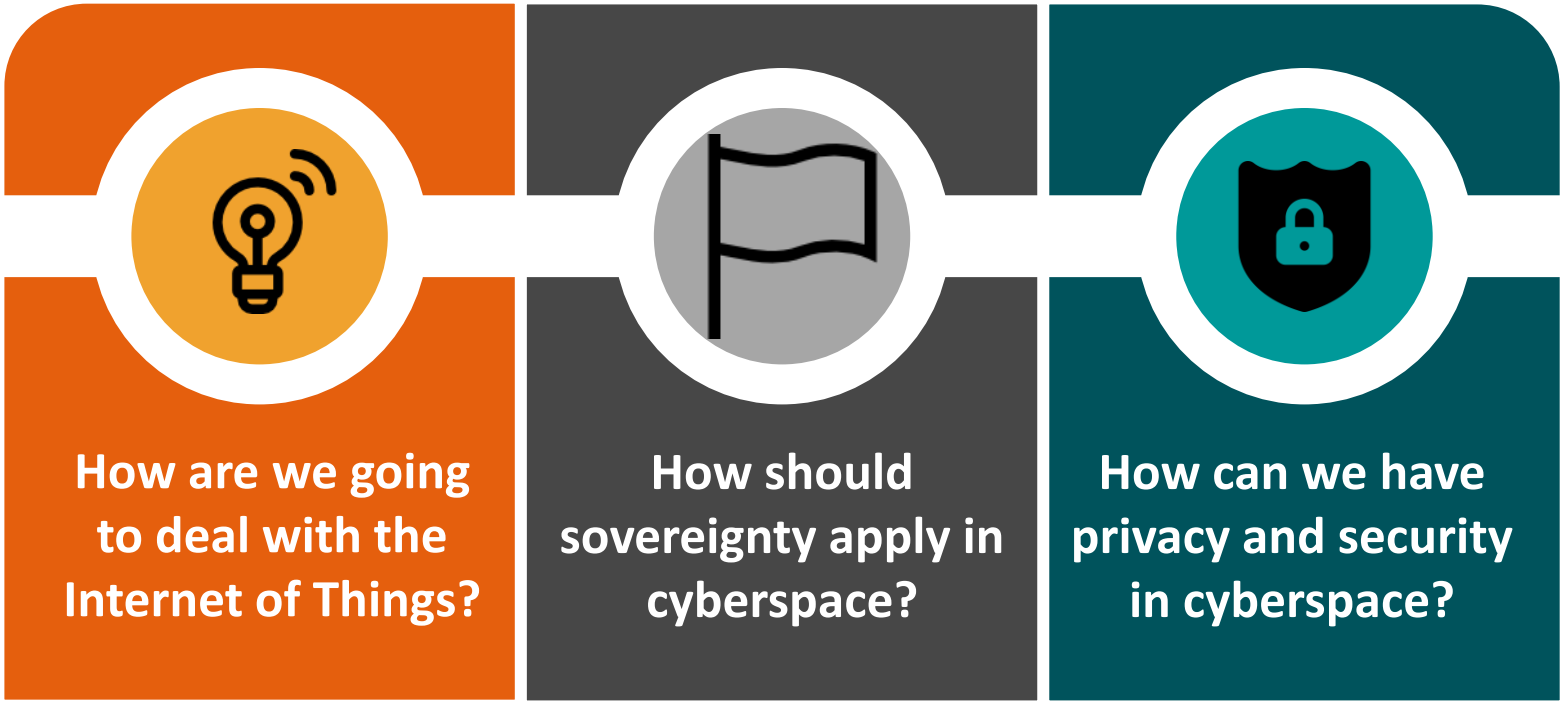
BUT IT'S NOT ALL BAD

All malicious actors face limitations:

- Hollywood ≠ real life
- Capacity constraints
- Limited number of paths to achieve their goals
- Operations occur on defender's networks

These limitations provide the openings for better cybersecurity.

WHAT ARE SOME KEY ISSUES DRIVING GLOBAL CYBERSECURITY POLICY?

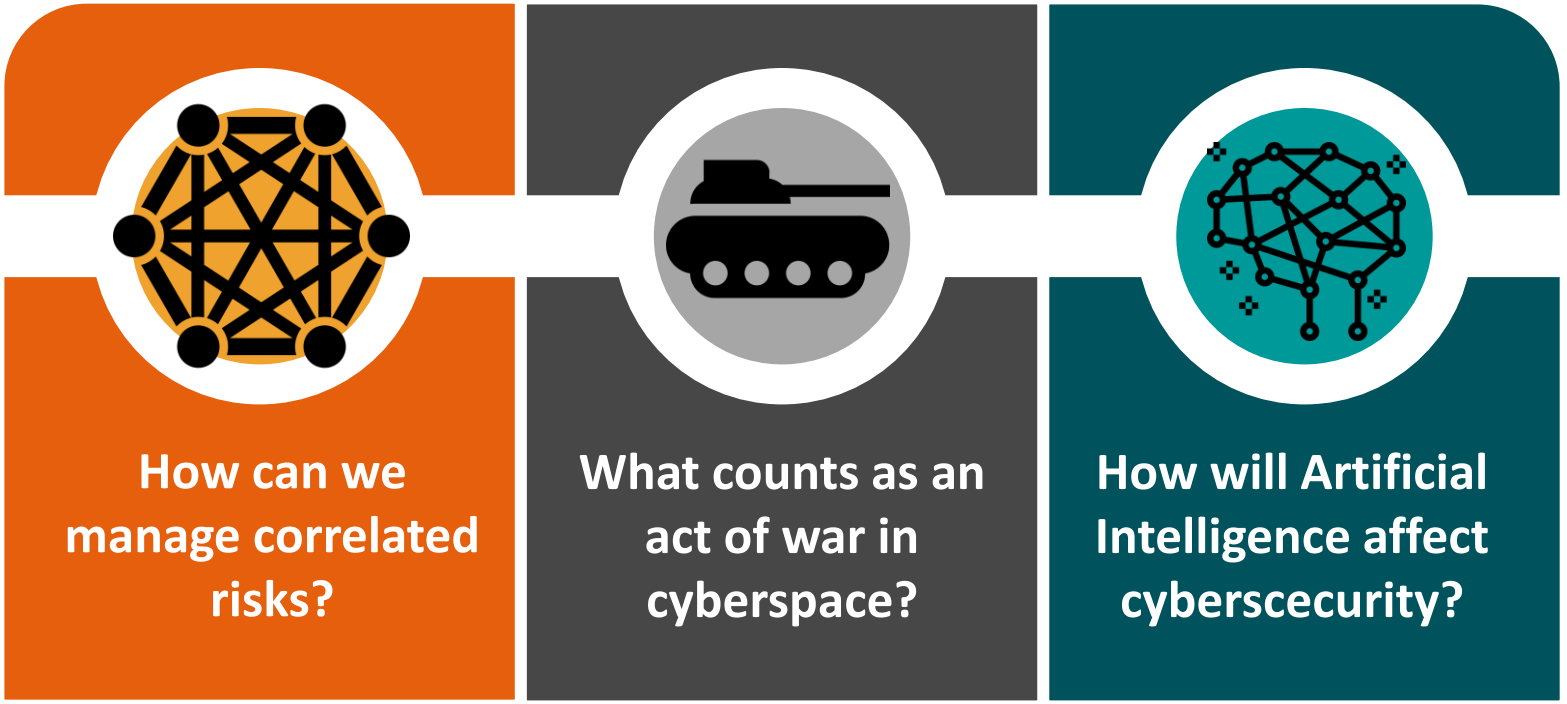


Once connected devices can kill people, regulation is inevitable.

We need new tools to manage friction in cyberspace.

Privacy and security should reinforce each other, but can be mutually destructive.

WHAT ARE SOME KEY ISSUES DRIVING GLOBAL CYBERSECURITY POLICY?



Interconnections, common software, and malware reuse reduce risk independence.

We need new definitions that work for cyberspace.

AI's impact could be good, bad, or indifferent.

TAKE ACTION INTERNALLY: BUILD A CYBER TOOL BOX

Each element depends on the others to be effective

TAKE ACTION EXTERNALLY: DON'T GO IT ALONE

Organizations must reach across boundaries and engage with external actors

TAKE ACTION COLLECTIVELY: COORDINATE AND COLLABORATE

Enable robust threat sharing with the cybersecurity industry

Cybersecurity companies need information to inform defenses

Undermine the criminal business model systematically

Make them undertake business process re-engineering

Coordinate disruption and response activities between governments and private sector actors

Not "hackback" but focus on comparative advantage

CYBER THREAT ALLIANCE

QUESTIONS?

BACK UP SLIDES

NATION-STATE CYBER CAPABILITIES:
BENEFITS, CONSTRAINTS, AND RISKS

Benefits

- Effective
- Relatively cheap and fast
- Levels the playing field
- Deniability

Constraints

- Intelligence dilemma
- Third country conundrum
- Bureaucratic challenges
- Collateral damage uncertainty
- Tool reuse

Systemic Risks

- Attribution difficulties
- Offense favored over defense
- Unintended consequences

NATION-STATE CYBER CAPABILITIES:
DEALING WITH THE SYSTEMIC RISK

Analogies that don't apply:

Border security

Missile defense

Nuclear deterrence

Approaches having some promise:

Operational Collaboration

Transparency

International Norms

Confidence-building measures

Resilience

CYBER THREAT ALLIANCE