CHANGING THE GAME: A DIFFERENT APPROACH TO CYBERSECURITY

Michael Daniel
President & CEO
WHY IS CYBERSECURITY A HARD PROBLEM?

- Cybersecurity is not just a technical problem
  - Cybersecurity is also an economic, psychological, and human behavioral challenge

- Cyberspace is governed by a different set of rules
  - The concepts of distance, borders, and proximity all operate differently in cyberspace compared to the physical world

- Cybersecurity is “new” and we’re still learning
  - 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
- **Terrorists**: Leverage cyberspace to recruit
- **Criminal Organizations**: Profit off malicious activity
- **Nation States**: Pursue their national interests

- **More broad**: The attack surface is exponentially increasing
- **Volume and diversity of connected devices increases complexity**
- **Low barriers to entry and high ROI incentive actors**

- **More dangerous**: Actors are increasingly moving to more destructive activity
- **Critical infrastructure is at the center of actors’ malicious activity**

- **More disruptive**: Potential impacts of a cyber incident are increasing
- **Digital dependence is making society increasingly vulnerable**

- **More frequent**: Volume of malicious cyber activity is increasing

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

How are we going to deal with the Internet of Things?

Once connected devices can kill people, regulation is inevitable.

How should sovereignty apply in cyberspace?

We need new tools to manage friction in cyberspace.

How can we have privacy and security in cyberspace?

Privacy and security should reinforce each other, but can be mutually destructive.
WHAT ARE SOME KEY ISSUES DRIVING GLOBAL CYBERSECURITY POLICY?

How can we manage correlated risks?
- Interconnections, common software, and malware reuse reduce risk independence.

What counts as an act of war in cyberspace?
- We need new definitions that work for cyberspace.

How will Artificial Intelligence affect cybersecurity?
- 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.
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
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