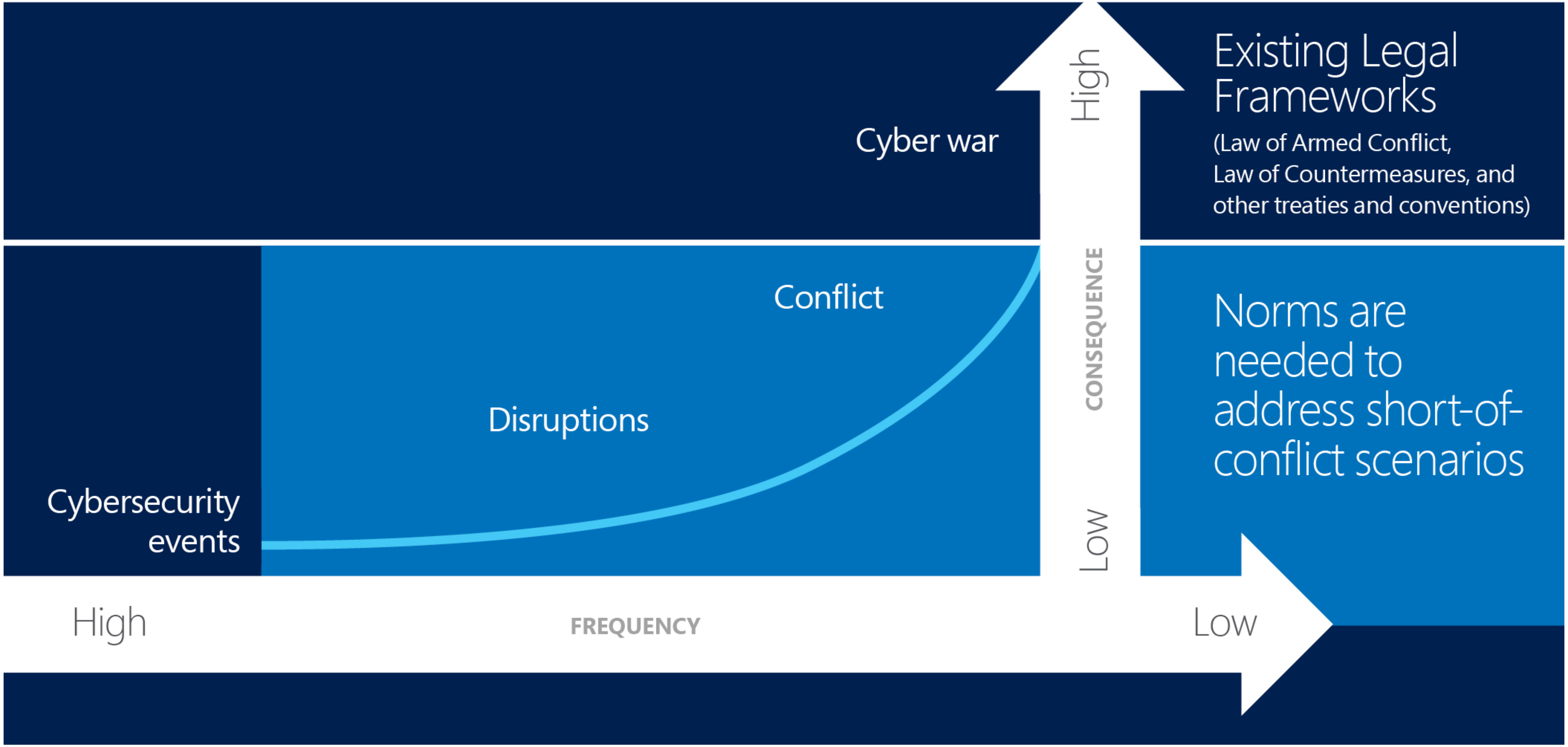
Microsoft

International Cybersecurity Norms

Angela McKay
Director, Government Security Policy and Strategy
Microsoft

Escalating cyber risks

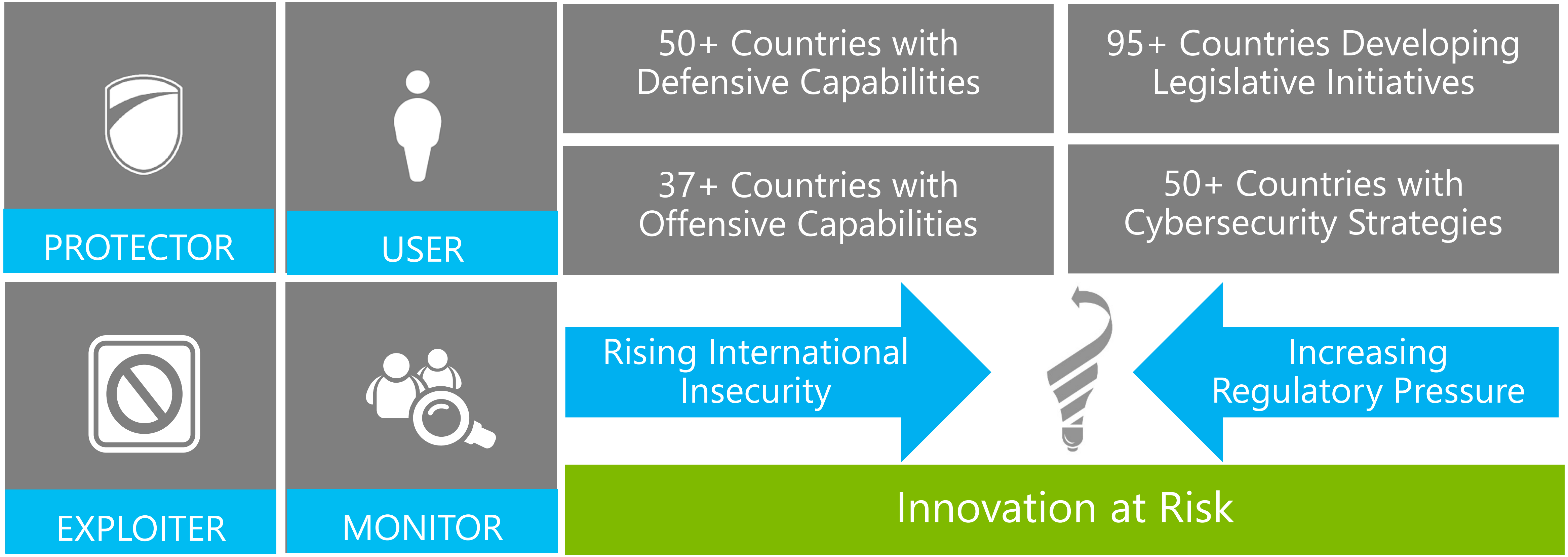


Existing Legal Frameworks

(Law of Armed Conflict, Law of Countermeasures, and other treaties and conventions)

Norms are needed to address short-of-conflict scenarios

Governments' roles in cyberspace



PROTECTOR

USER

EXPLOITER

MONITOR

50+ Countries with Defensive Capabilities

95+ Countries Developing Legislative Initiatives

37+ Countries with Offensive Capabilities

50+ Countries with Cybersecurity Strategies

Rising International Insecurity

Increasing Regulatory Pressure

Innovation at Risk

Relevance to the private sector

Loss of trust in products and services

Complicated response cycles and operational uncertainties

Distorted threat models

Reciprocity costs from state actions

Regulatory costs from dynamic compliance environment

Evaluating behavior in cyberspace

	Actors	Objectives	Actions	Impacts
Offensive Norms	Nation-states, primarily militaries and intelligence agencies	Reduce conflict between states, lower risk of escalation from offensive operations, and prevent unacceptable consequences	Exercise self-restraint in the conduct of offensive operations.	Mitigate unacceptable impacts of ICT use by governments
Defensive Norms	Public and private sector cyber-defense teams	Manage cybersecurity risk through enhanced defense and incident response	Collaboration among defenders (e.g., sharing information, best practices exchange, and response coordination)	Protect government, enterprise, and consumer users of ICT
Industry Norms	Global ICT companies	Deliver secure products and services	Support defense and refrain from offense	Protect ICT users and enhance trust in technology

Microsoft's norms proposals

	Nation-states	Global ICT industry
Maintain trust	States should not target ICT companies to insert vulnerabilities (i.e., backdoors) or take actions that would otherwise undermine public trust in products and services.	Global ICT companies should not permit or enable nation-states to adversely impact the security of commercial, mass-market ICT products and services (e.g. though backdoors).
Coordinated approach to vulnerability handling	States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.	Global ICT companies should adhere to coordinated disclosure practices for handling of ICT product and service vulnerabilities.
Stop proliferation of vulnerabilities	States should commit to nonproliferation activities related to cyber weapons.	Global ICT companies should not traffic in cyber vulnerabilities for offensive purposes, nor should ICT companies embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes.
Mitigate the impact of nation-state attacks	States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.	Global ICT companies should collaborate to proactively defend against nation-state attacks and remediate the impact of such attacks
Prevent mass events	States should limit their engagement in cyber offensive operations to avoid creating a mass event	No corresponding norm for the global ICT industry.
Support response efforts	States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.	Global ICT companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace.
Patch customers globally	No corresponding norm for nation-states.	Global ICT companies should issue patches to protect ICT users, regardless of the attacker and their motives.

Areas of convergence in proposed norms

Areas of convergence	OSCE CBMs (2013, 2016)	Microsoft (2014)	SCO (2015)	US Government (2015)	UN GGE (2015)	G20 (2016)
Maintain Trust	●	●	●		●	
Coordinated approach to vulnerability handling		●			●	
Prevent mass events	●	●	●	●	●	●
Facilitate cross-border law enforcement on cybercrime	●	●	●	●	●	●
Do not impair CSIRTs/CERTs		●		●	●	●
Protect IP from economic espionage				●		●

Constituents for industry norms

Platform and infrastructure providers

Technology manufacturers

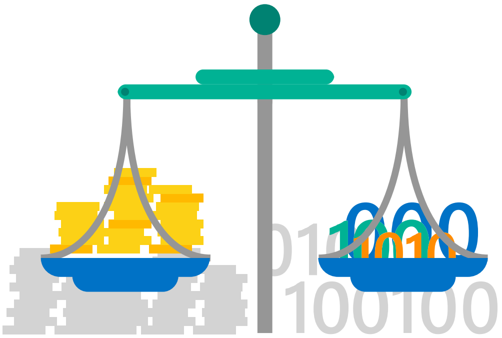
Defenders and responders

Assurance organizations

Challenge: verification of compliance

Technical attribution

- Trade craft
- Artifacts
- Target selection
- Specialized knowledge



Policy options

- Say nothing
- Make a private accusation
- Make a public accusation

Public-private forum for attribution

Deep technical expertise

Geographically diverse

Focused on severe attacks

Subject to peer review

Forums and processes

Bilateral consultations

Regional approaches

International platforms

G20 + ICT20

Resources

Prior white papers available

- From Articulation to Implementation: Enabling Progress on Cybersecurity Norms (2016) (link)
- Five Principles for Shaping Cybersecurity Norms (2013) (link)
- International Cybersecurity Norms (2014) (link)
- Governments and APTs: The Need for Norms (2015) (link)

Additional resources

- *Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cybersecurity Norms* (2014) (link)
- *Securing Cyberspace through International Cybersecurity Norms* (link)

Questions