Microsoft

A Digital Geneva Convention:

Why it is needed and how it can be created

Alaa Ajweh
Financial Sector Lead
Microsoft QSTP LLC.

Agenda

Microsoft

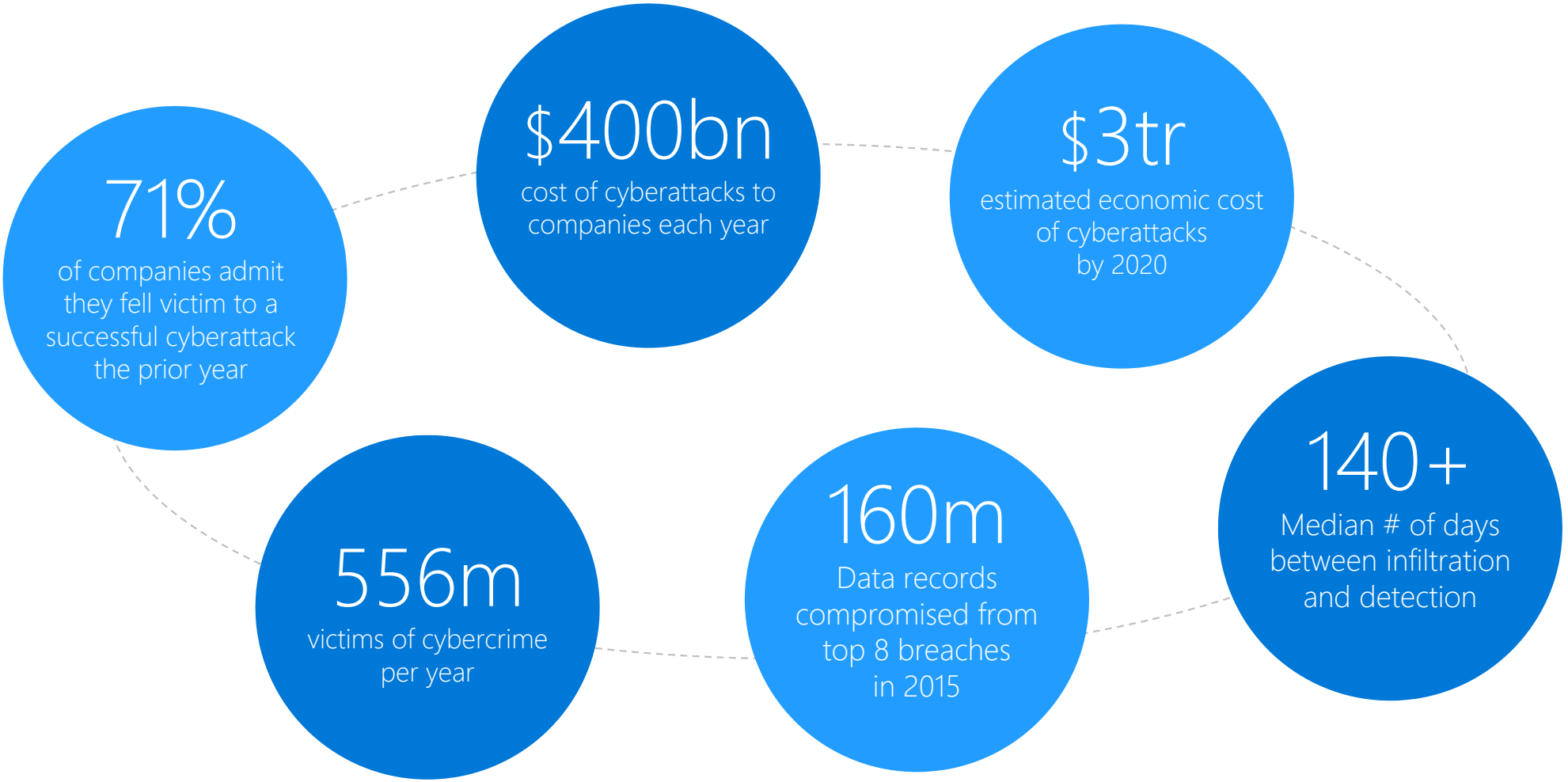
1. The need for a Digital Geneva Convention
2. Where the discussions are today
3. The importance of multi-stakeholder dialogue
4. Three essential parts of a Digital Geneva Convention
5. What next?

Microsoft

The need for a Digital Geneva Convention

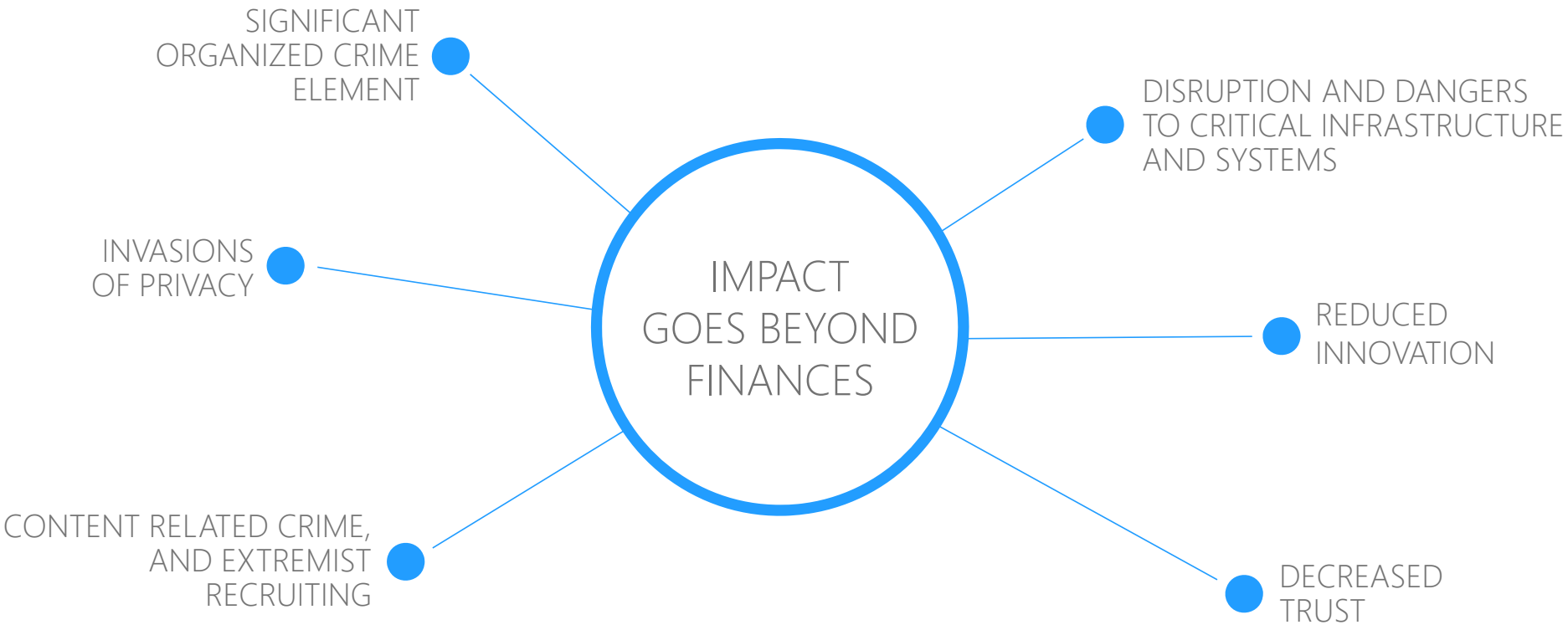
Cyberattacks cause immense costs

Microsoft



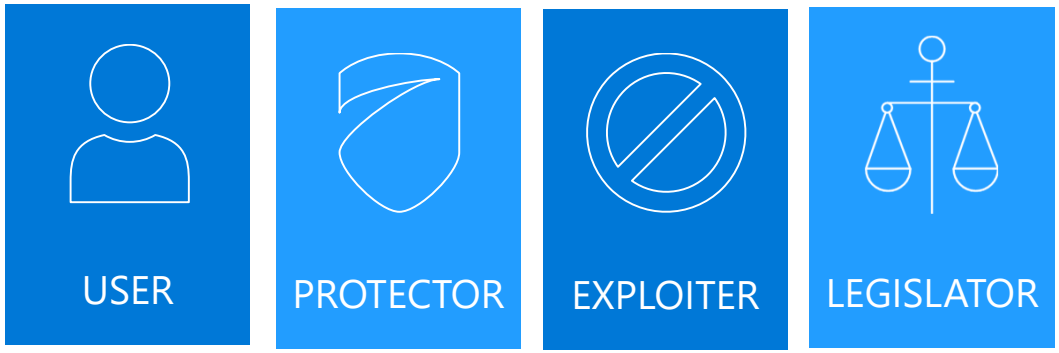
Cyberattacks also create wider problems

Microsoft



Governments heavily involved in cyberspace

Microsoft



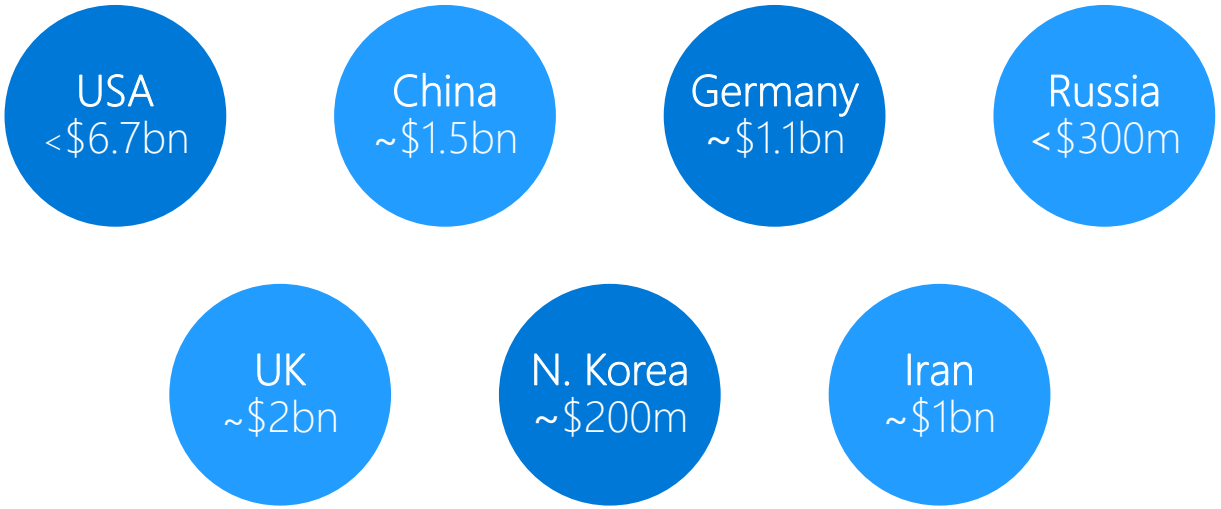
50+ Countries with Defensive Capabilities

38+ Countries with Offensive Capabilities

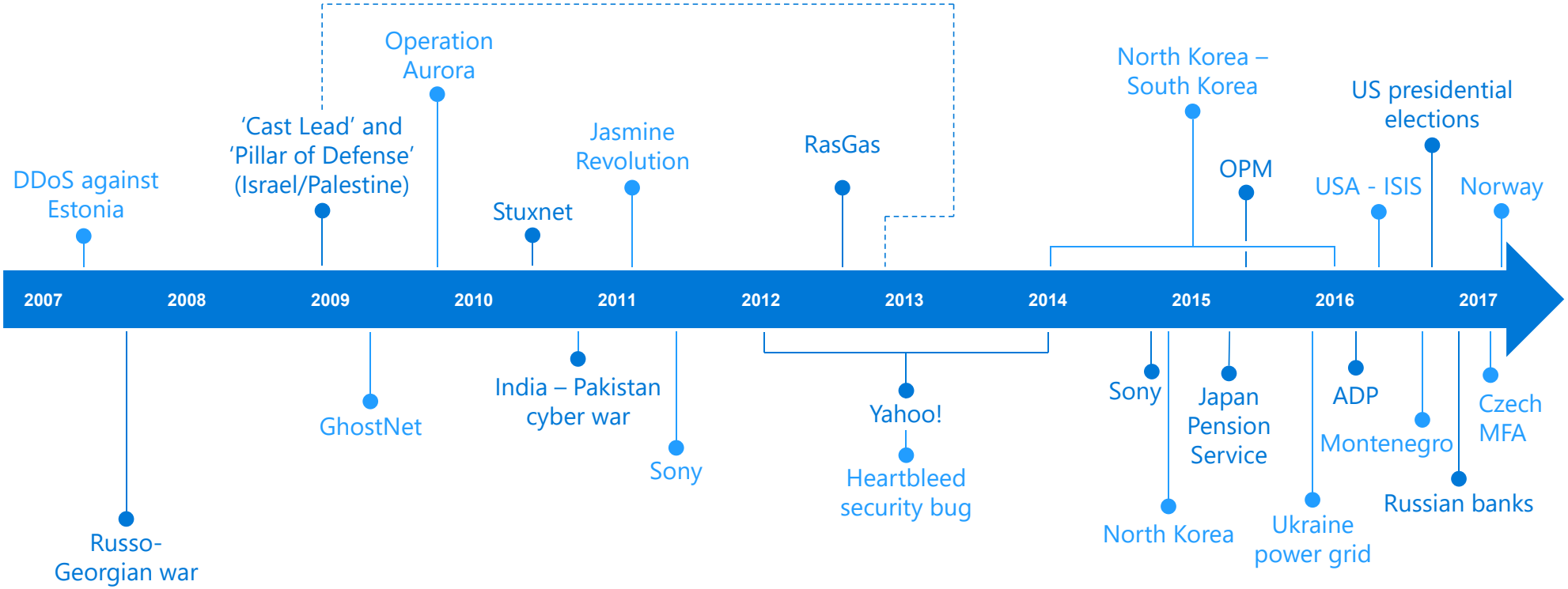
95+ Countries Developing Legislative Initiatives

70+ Countries with Cybersecurity Strategies

ESTIMATED SPENDING ON CYBER OPERATIONS

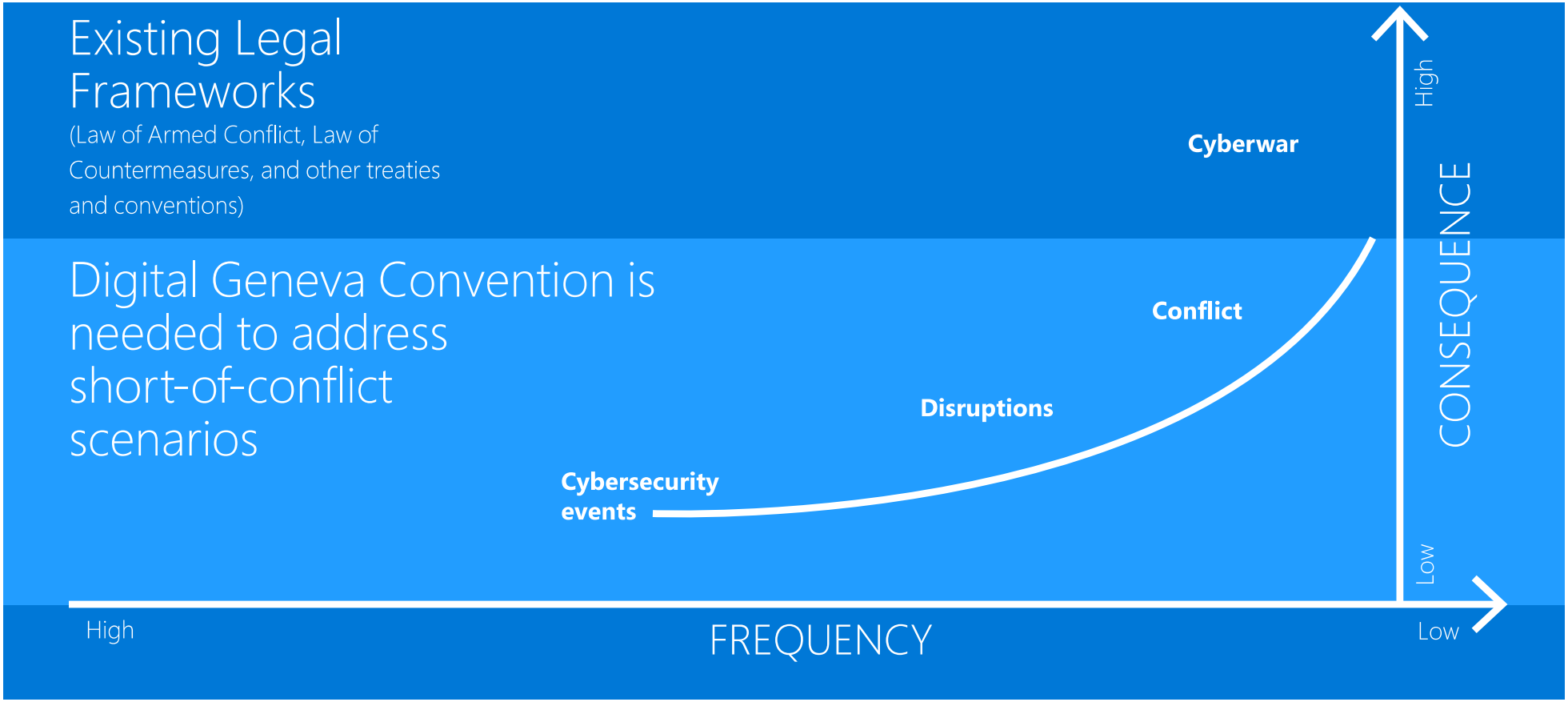


Government sponsored cyberattacks are increasing



Risk to civilians from cyber-conflict needs a response

Microsoft

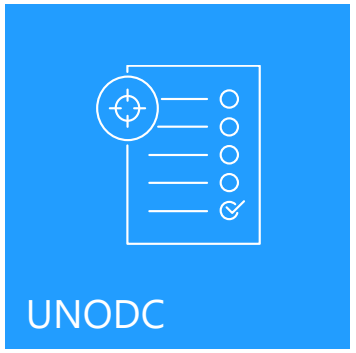


Microsoft

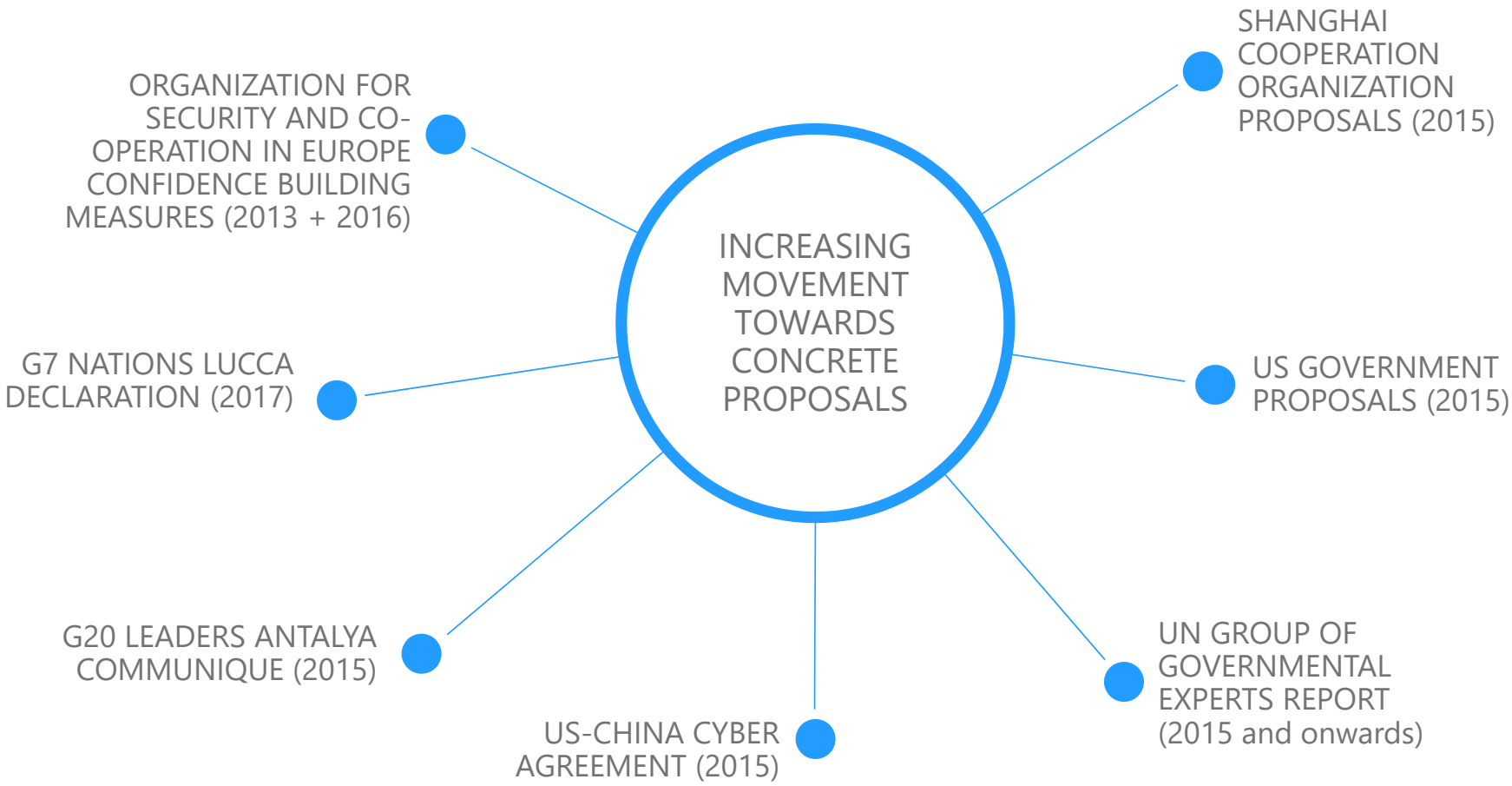
Where the discussions are today

Existing intergovernmental discussions and fora

Microsoft



7 major and relevant inter-governmental proposals



G7 declaration was positive but needed to go further

- April 11, 2017 declaration on "Responsible state's behavior in cyberspace".
- Sees urgent need for rules in cyberspace to prevent conflict and promote stability.
- But needs to move beyond voluntary approach to binding agreements.
- And needs to more fully endorse a role for the private sector, especially the tech sector.

G7 2017 ITALIA

G7 DECLARATION
ON RESPONSIBLE STATES BEHAVIOR IN CYBERSPACE

LUCCA, 11 APRIL 2017

INTRODUCTION

We remain committed to an accessible, open, interoperable, reliable and secure cyberspace. We recognize the enormous benefits for economic growth and prosperity that we and all others derive from cyberspace as an extraordinary tool for economic, social and political development.

We are concerned about the risk of escalation and retaliation in cyberspace, including massive denial-of-service attacks, damage to critical infrastructure, or other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public. Such activities could have a destabilizing effect on international peace and security. We stress that the risk of interstate conflict as a result of Information and Communication Technology (ICT) incidents has emerged as a pressing issue for consideration. Furthermore, we are increasingly concerned about cyber-enabled interference in democratic political processes.

We encourage all States to engage in law-abiding, norm-respecting and confidence-building behaviour in their use of ICT. Cooperative approaches would also contribute to the fight against the use of cyberspace by non-State actors for terrorist and other criminal purposes.

For these reasons, the G7 set an ambitious course in promoting security and stability in cyberspace and the protection of human rights, through *"The Principles and Actions on Cyber"* endorsed in Ise-Shima on 26 and 27 May 2016.

We continue to call upon all States to be guided in their use of Information and Communications Technologies (ICTs) by the cumulative reports of the United Nations Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN-GGE).

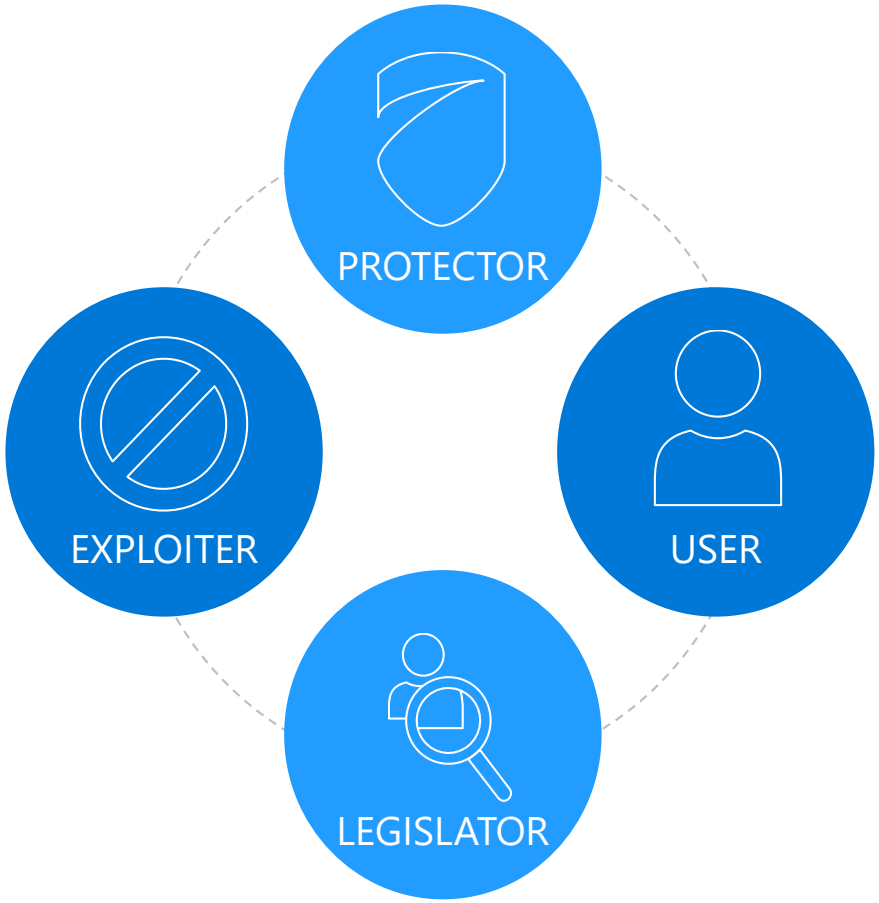
Reaffirming our commitment to contribute to international cooperative action and the protection against dangers resulting from the malicious use of ICTs, we support the following Declaration, and encourage similar commitments from other States:

Microsoft

The importance of multi-stakeholder dialogue

Governments' many roles & challenges in cyberspace

Microsoft



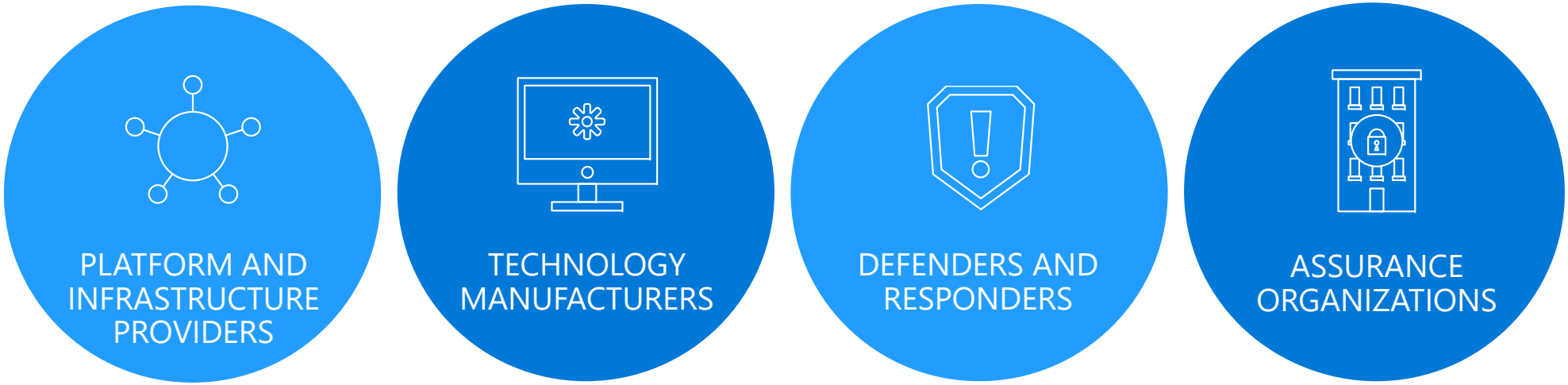
Rising International Insecurity

Increasing Regulatory Pressure

INNOVATION AT RISK

Private sector constituents are many and varied

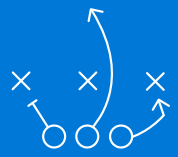
Microsoft



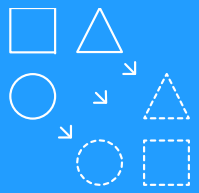
The tech sector's specific relevance

Microsoft

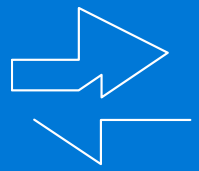
Loss of trust in products and services



Complicated response cycles and operational uncertainties



Distorted threat models

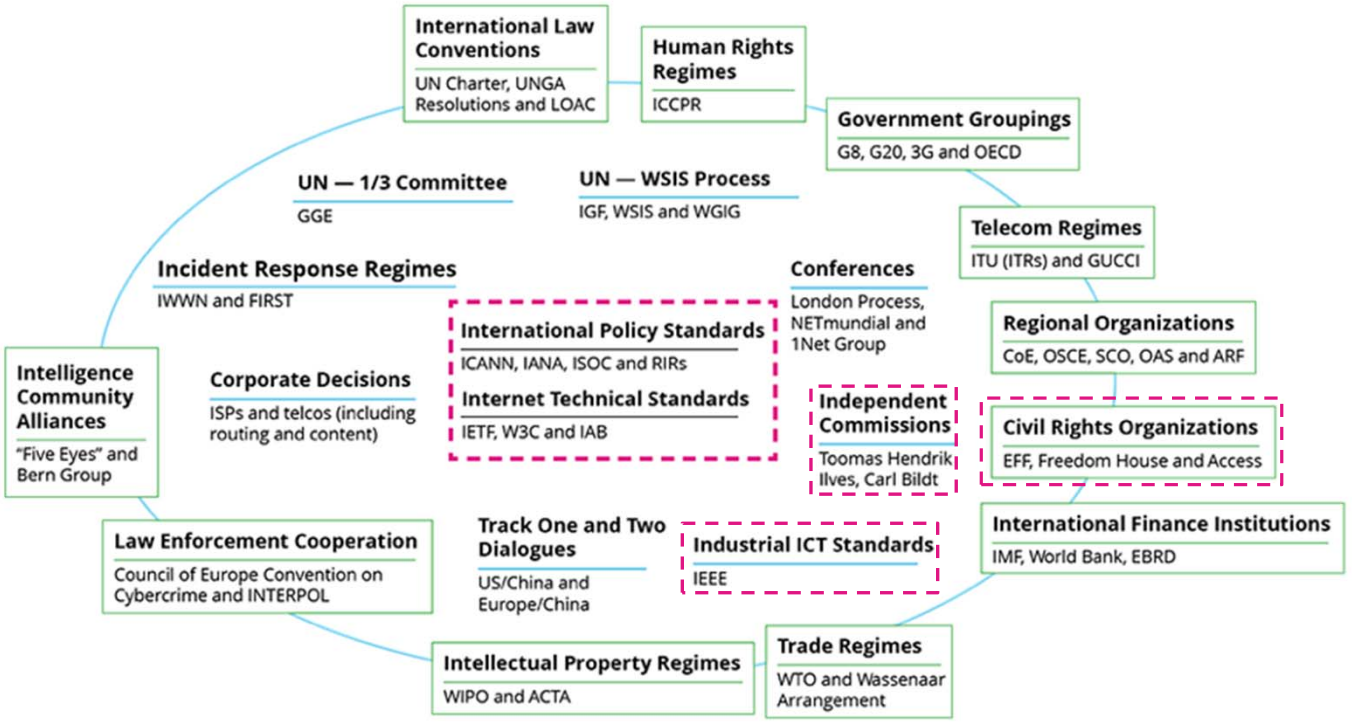


Reciprocity costs from state actions

Regulatory costs from dynamic compliance environment

The essential civil society perspective

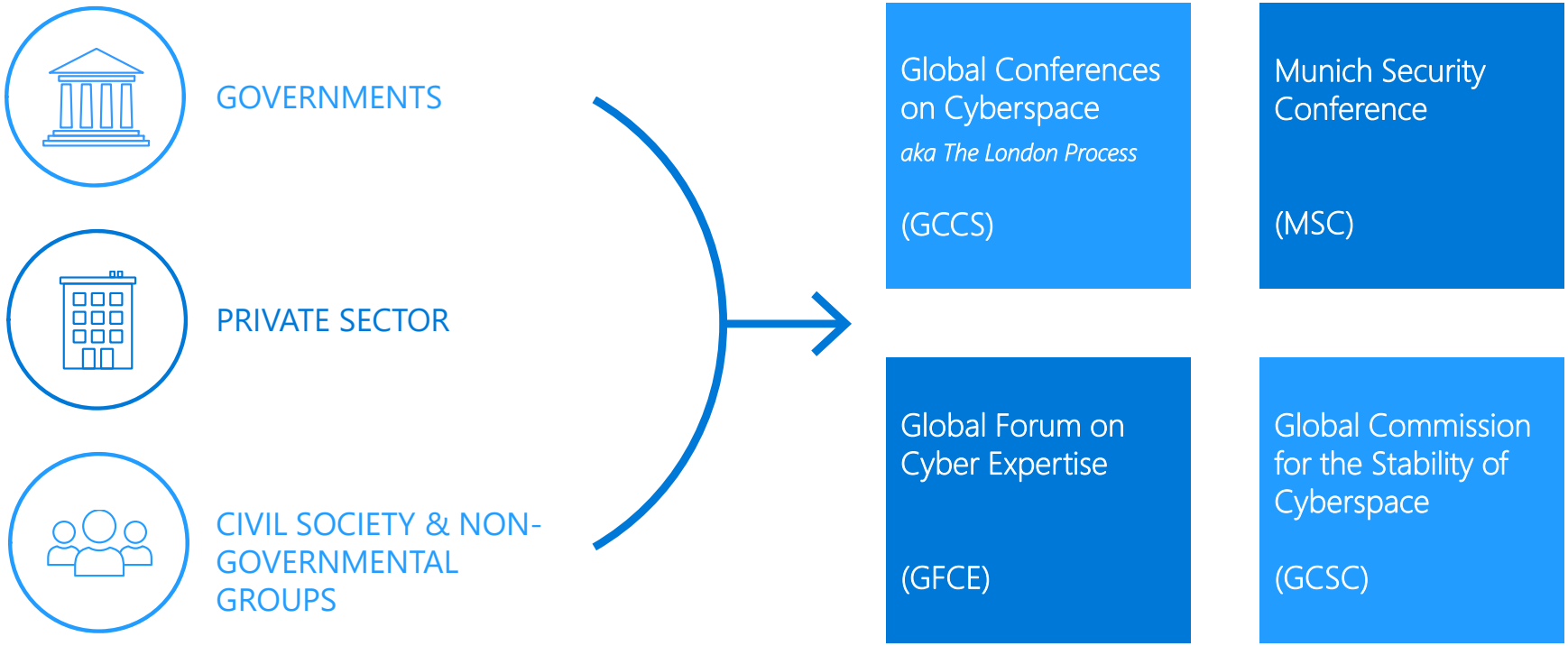
- Variety of relevant civil society groups and non-governmental organizations already engaged:
  - Standards bodies;
  - Advocacy groups;
  - Think tanks.
- Providers of essential third party, expert or holistic perspectives.
- Strongly influential at national level, some even internationally.



The Regime Complex for Managing Global Cyber Activities
(Joseph S. Nye Jr., 2014)

Limited number of public-private platforms

Microsoft



Microsoft

The three essential parts of a Digital Geneva Convention

Three essential components are required

Microsoft

DIGITAL GENEVA CONVENTION

BINDING GOVERNMENT AGREEMENTS

TECH SECTOR ACCORDS

ATTRIBUTION ORGANIZATION

Binding government agreements need to be crafted

Microsoft

LEGALLY BINDING FRAMEWORK GOVERNING STATES' BEHAVIOUR

CAN START AS VOLUNTARY OR POLITICALLY BINDING

SHOULD AIM TO CONSTRAIN AND/OR PREVENT CYBER-CONFLICT

PRECEDENTS EXIST FOR NUCLEAR AND CHEMICAL WEAPONS.

10 key commitments within those agreements

Microsoft

DO NOT ACT AGAINST:

- Safety and security of private citizens
- Mass-market commercial tech products by inserting "backdoors"
- Systems key to global economy
- Intellectual property or confidential business information
- Journalists and private citizens involved in electoral processes

ACT IN ORDER TO:

- Have clear policy re. vulnerabilities in mass market products and services
- Assist private sector detection, containment, response, and recovery
- Develop limited, precise, non-reusable cyber weapons
- Avoid mass damage to civilian infrastructure in cyber offensives
- Limit proliferation of cyber weapons

The tech sector needs its own common accords

Microsoft

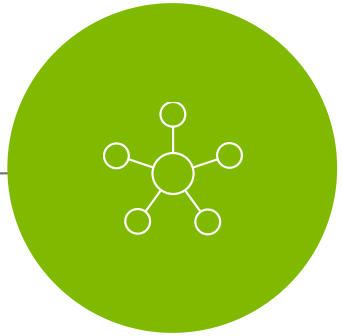
Individuals and organizations need to trust cyberspace before they fully commit to it…

…which means they need to be able to trust the technology underpinning cyberspace…

…and to be able to trust those who make the technology…

… therefore, tech companies must act to create a trustworthy environment for users and to reassure states of their neutrality…

…and, in the face of growing state activity in cyberspace, individual companies can draw strength from a collective "tech sector" approach.



6 possible common tech sector objectives

Microsoft

Critical elements for an attribution organization

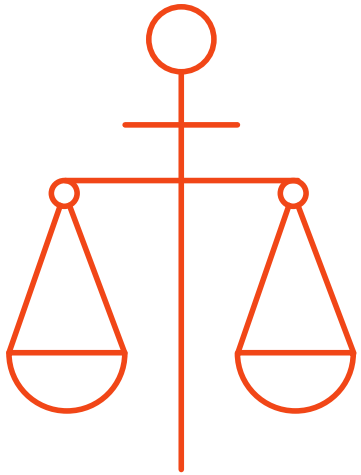
Microsoft

Striking a technical and political balance in attribution

Microsoft

TECHNICAL ATTRIBUTION

- Trade craft
- Artifacts
- Target selection
- Specialized knowledge



POLICY OPTIONS

- Say nothing, do nothing
- Say nothing, use covert options
- Make a private accusation
- Make a public accusation

Microsoft

What next?

Our call to action

Microsoft

Undertake to create politically binding then legally binding agreements committing governments to certain, acceptable behaviors in cyberspace.

Drive forward a tech sector accord that commits the ICT industry to objectives and actions that will protect users and the wider internet, and will ensure the sector's neutral status in any cyber-conflict.

Support the establishment and operation of politically-neutral, independent, transparent and peer-reviewed attribution organization.

Identify and provide avenues for multi-stakeholder input and involvement in the development of cyberspace policies and agreements.


Microsoft