



Panelová debata: **Monitorování internetu.
Máme se bát o své soukromí?**

DO WE NEED A

"DIGITAL GENEVA CONVENTION"

IN TIMES OF CYBER (IN)SECURITY?"

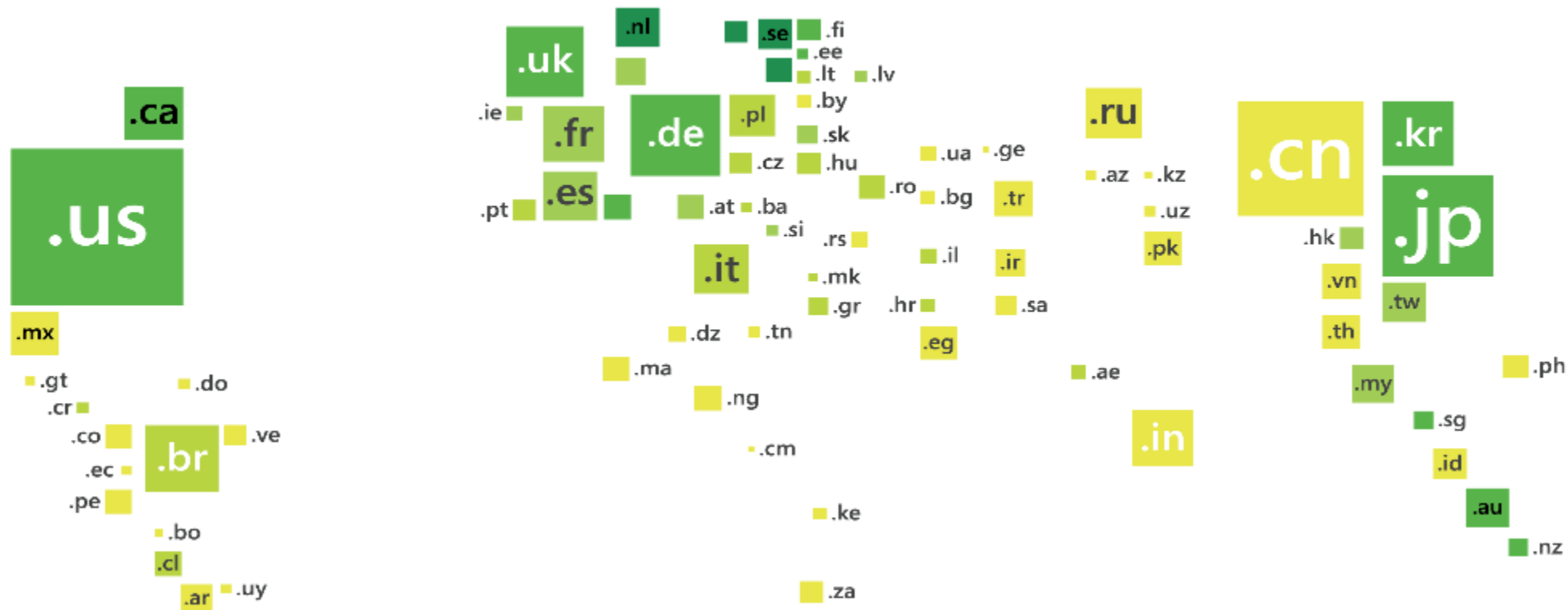
Václav Mach
Microsoft



19. dubna 2017 | 9:00–17:00

Clarion Congress Hotel Prague, Praha

Freyova 33, Praha 9 - Vysočany

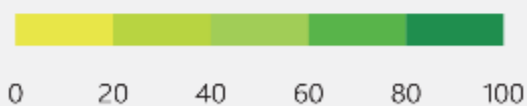


2005 Internet User Map

Sizing Legend

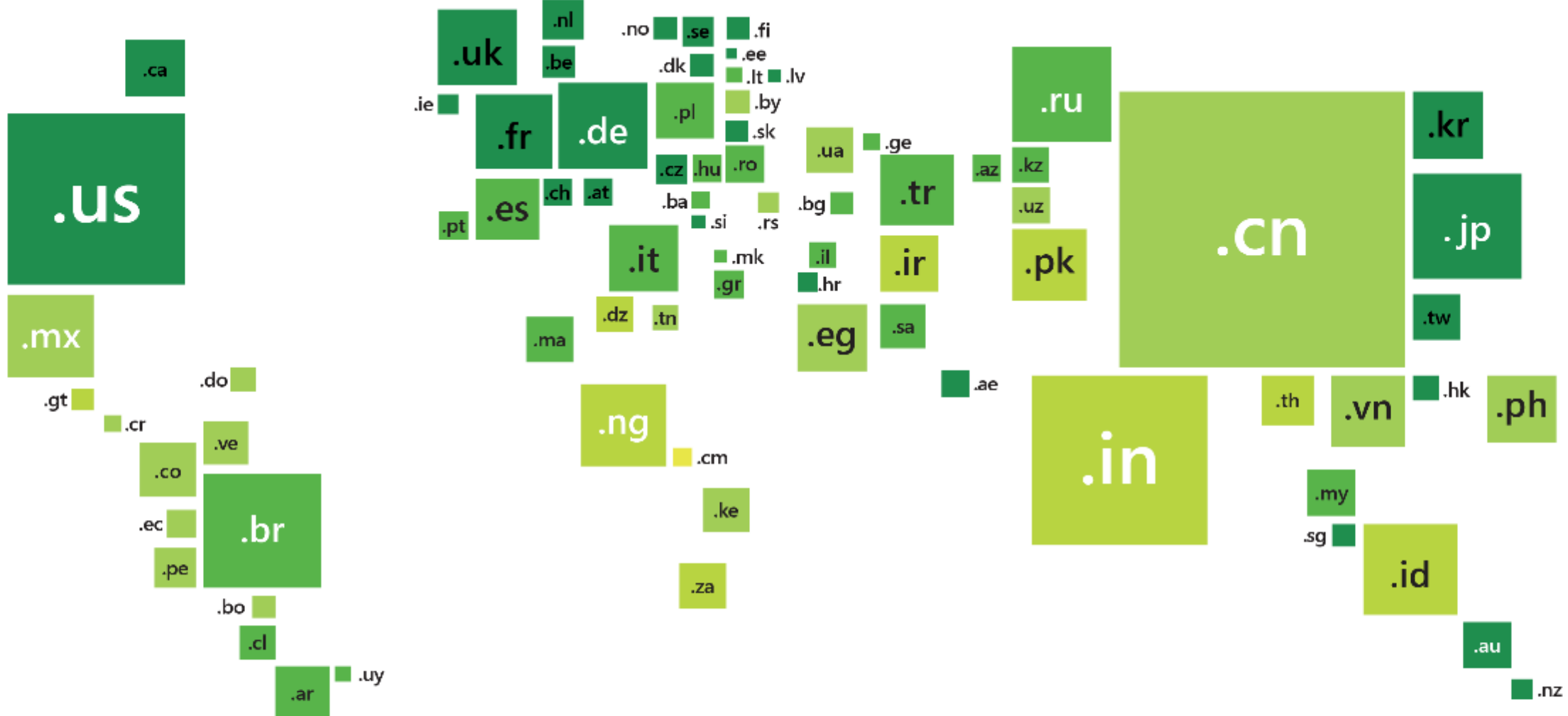
- = 2M Internet Users
- = 5M Internet Users

Percent Penetration of Internet Users



Number of Internet Users

USA	China	Japan	Germany	United Kingdom	Brazil	South Korea	India
201M	111M	86M	57M	42M	38M	35M	26M

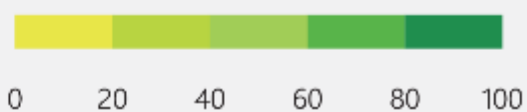


2015 Internet User Map

Sizing Legend

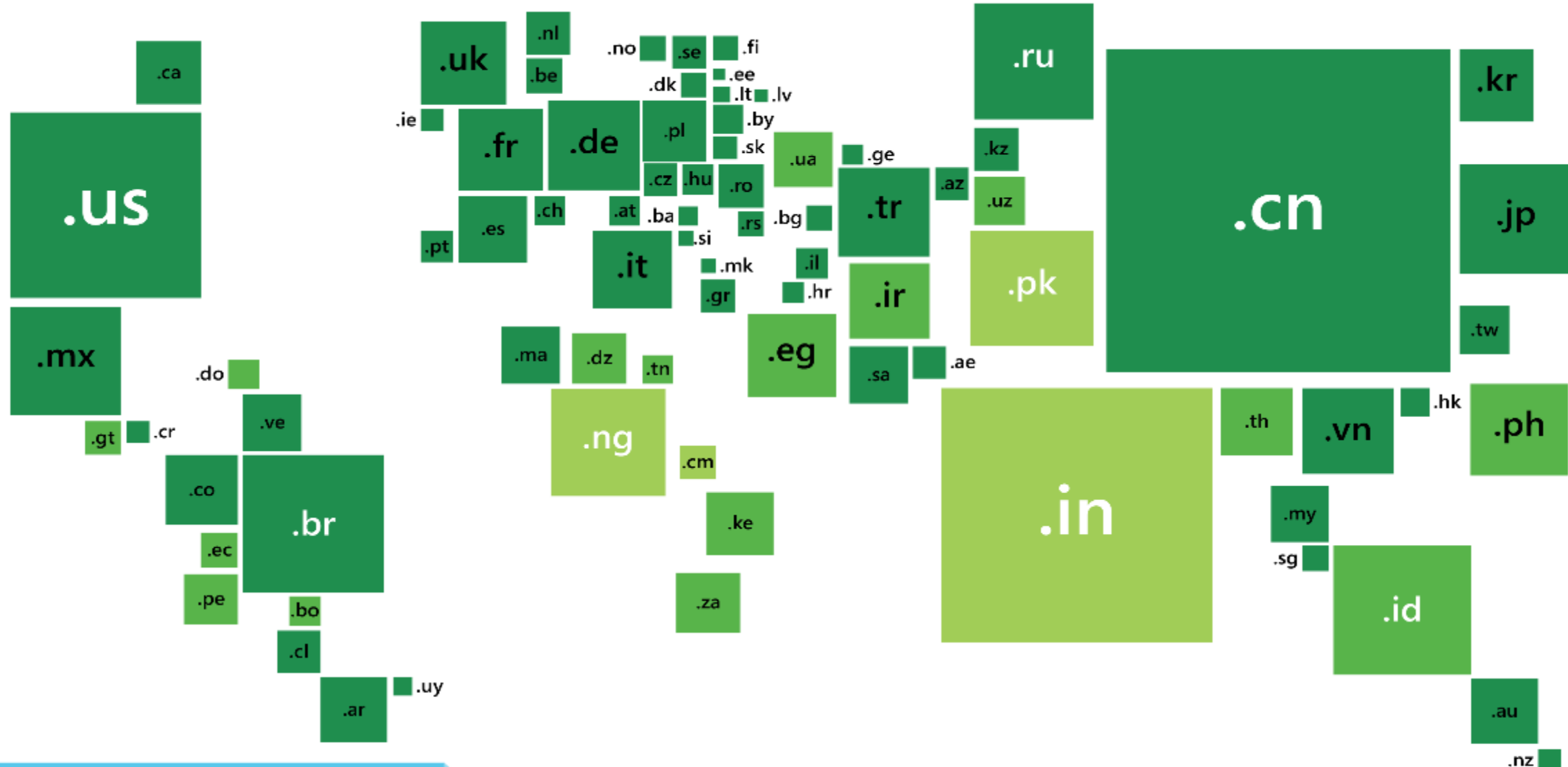
- = 2M Internet Users
- = 5M Internet Users

Percent Penetration of Internet Users



Number of Internet Users

China	USA	India	Brazil	Russia	Germany	Mexico	Nigeria
751M	287M	283M	127M	90M	72M	68M	66M

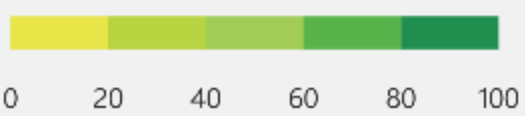


2025 Internet User Map

Sizing Legend

- = 2M Internet Users
- = 5M Internet Users

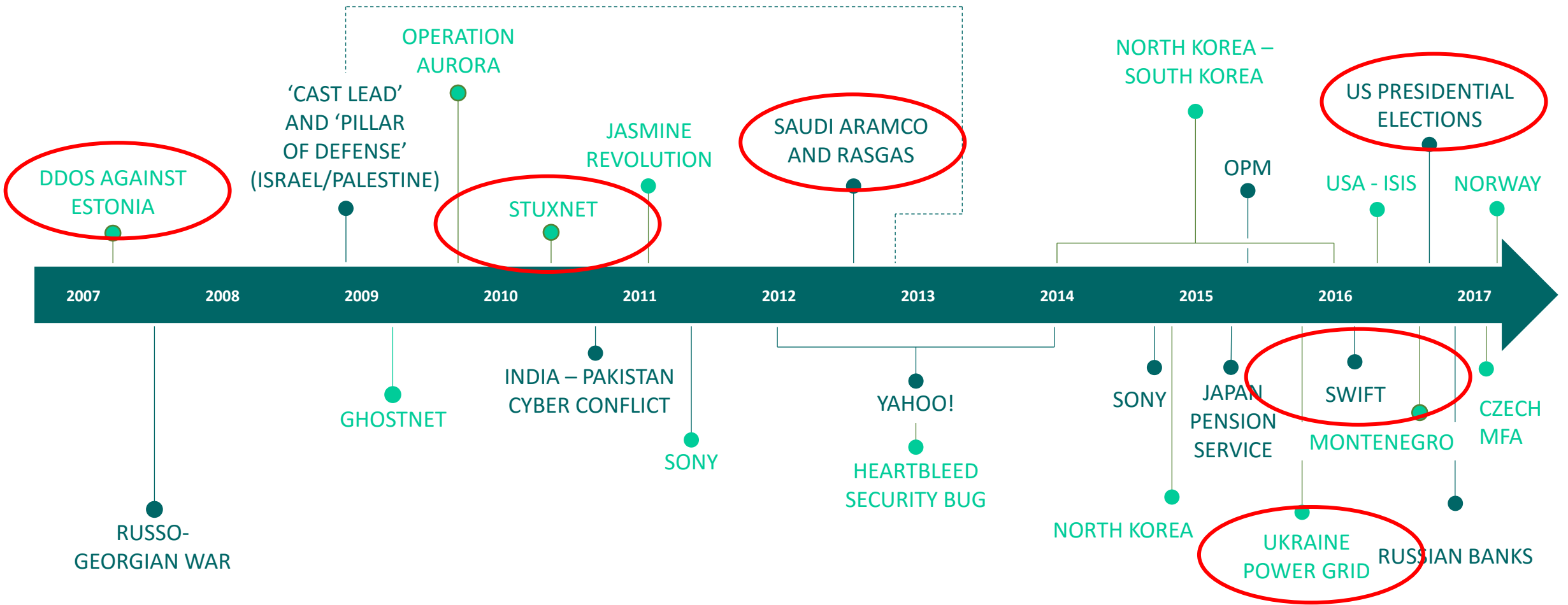
Percent Penetration of Internet Users



Number of Internet Users

China	India	USA	Indonesia	Brazil	Pakistan	Nigeria	Russia
1.1B	708M	317M	183M	173M	146M	126M	124M

Major (alleged) nation-state cyberattacks since 2007



Rise of cyberattacks impacting the global economy



Average days **attackers are present** on a victim network **before detection**



Average cost of a data breach to a company

15% increase YoY

Security



level issue

Impact of cyber attacks could be as much as **\$3 trillion** in **lost productivity and growth**

Job security Customer loyalty

Implications

Brand reputation Civil liability

Intellectual property

What are cybersecurity norms?



"Voluntary, non-binding norms, rules or principles of responsible behavior of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment".

UN Group of Governmental Experts (UNGGE), July 2015

The state of discussions on global norms

Multilateral fora for intergovernmental dialogue



Group of Twenty (G20)	North Atlantic Treaty Organization (NATO)	Organization for Security and Cooperation in Europe (OSCE)	Shanghai Cooperation Organization (SCO)	United Nations (UN)
--------------------------	--	---	--	------------------------

Multi-stakeholder fora



East West Institute (EWI)	London Process	Munich Security Conference (MSC)	World Economic Forum (WEF)	Global Commission for Stability of Cyberspace
------------------------------	----------------	-------------------------------------	-------------------------------	---

Microsoft norms proposal

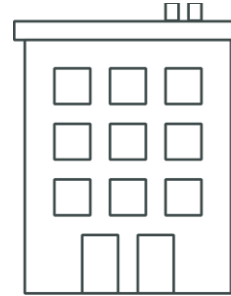
	Nation-states	Global ICT industry
Maintain trust	No targeting of tech companies, private sector or critical infrastructure	No assistance in offensive actions
Support response efforts	Assist private sector to detect, contain, respond to and recover from events	Collaborative remediation after attacks
Coordinated approach to vulnerability handling	Report vulnerabilities to vendors rather than to stockpile, sell or exploit them	Coordinated disclosure practices for vulnerabilities
Mitigate the impact of nation-state attacks	Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise and not reusable	Collaborative and proactive defense
Stop proliferation of vulnerabilities	Commit to non-proliferation activities to cyber weapons	Support for intergovernmental defensive efforts
Prevent mass events	Limit offensive operation to avoid a mass event	No corresponding norm for the global ICT industry.
Patch customers globally	No corresponding norm for nation-states.	Software patches available to all

Microsoft's vision



DIGITAL GENEVA
CONVENTION

GOVERNMENTS



"GLOBAL
TECH ACCORD"

INDUSTRY



ATTRIBUTION
COUNCIL

PUBLIC-PRIVATE
PARTNERSHIP

Microsoft's vision

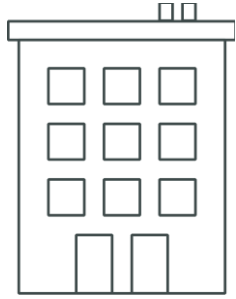


DIGITAL GENEVA
CONVENTION

GOVERNMENTS

- International rules in military and geopolitical areas exist for armed conflicts; cyberspace should be no different
- Legally binding framework to govern states' behavior in cyberspace in peacetime
- Incremental steps to achieve progress in stages
- Important foundations already in place
- Pressing case for launching global dialogue

Microsoft's vision



"TECH ACCORD"

INDUSTRY

- Most of information & technology infrastructure owned by private sector
- Need for civilian trust in technology
- Industry plays a critical role in keeping cyberspace stable, open and secure
- The Tech Accord: a collective industry commitment to cybersecurity, i.e. 100% defense, 0% offense
- While Digital Geneva Convention is crucial, the tech sector need not wait for governments to move forward

Microsoft's vision



ATTRIBUTION
COUNCIL

PUBLIC-PRIVATE
PARTNERSHIP

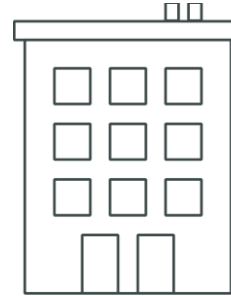
- Establishing an International Cyberattack Attribution Council to strengthen trust online
- Organized cooperation between technology companies can advance attribution
- Independence, transparency and diverse geographic representation will be essential
- The focus must be attribution of major infrastructure attacks, not incident response or enforcement
- A trusted attribution organization is key and work is now underway to help create it

Microsoft's vision



DIGITAL GENEVA
CONVENTION

GOVERNMENTS



"TECH ACCORD"

INDUSTRY



ATTRIBUTION
COUNCIL

PUBLIC-PRIVATE
PARTNERSHIP



Thank you!

@VáclavMach

Václav Mach
Microsoft

