Cybersecurity
The Rough Road Beyond Awareness

MAJLINDA ZHEGU PHD, DR.
Professor of Innovation Management
Interuniversity Center of Science, Technology and Society
University of Quebec in Montreal

Digital Transformations

Drivers

Four drivers

- Accessibility
- Connectivity
- Datafication
- Automation

Digital innovation

A **dozen** key, enabling technologies

Ex.

- Mobile/Internet
- Cloud computing
- Big data
- IOT
- Wearables
- Robotics
- Additive manufacturing

Technology convergence

An **endless** number of applications

Ex.

- Drones
- Autonomous vehicles
- Forth party logistics
- E-commerce
- Remote maintenance
- Data-based routing
- Demand forecast

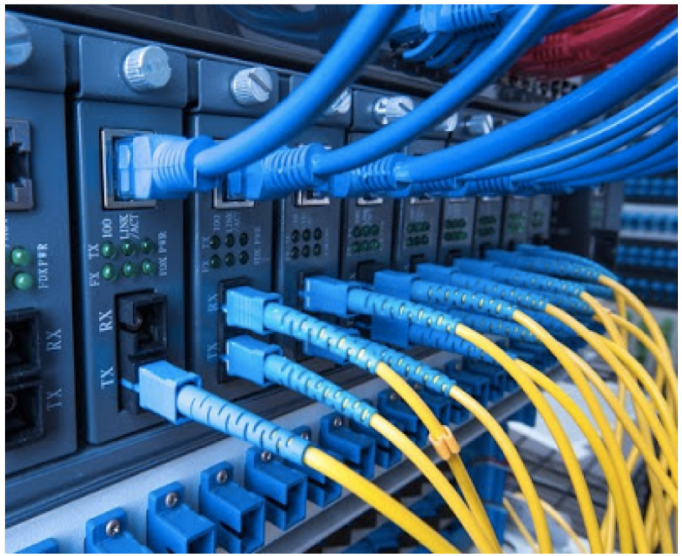
Digitization: Source of Strength or Vulnerability?

- Cybersecurity is the number one problem of humankind

  (Warren Buffett, 2017).

- Cybersecurity threats are outpacing abilities of governments and companies

  (World Economic Forum, 2018)



Sources:
http://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5
https://www.weforum.org/

Cyber Crime the Greatest Threat to Every Company in the World

- **Cyber crime damage costs: $6 trillion annually by 2021**
  - *More profitable than the global trade of all major illegal drugs combined.*

(Source: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

- **Global spending on Cybersecurity will exceed $1 trillion over the next five years**:
  - *More than 4,000 ransomware attacks every day since 2016.*

(Source:https://cybersecurityventures.com/cybersecurity-market-report

- **Awareness**
  - *78% of people claim to be aware of the risks of unknown links in emails but they click anyway.*
  - *52% of companies that suffered cyber attacks in 2016 no changes to their security in 2017*

(Source: Cyber security breaches 2017)

Cybersecurity is a Shared Responsability

Cybersecurity is the **CAPABILITY** to protect digital information and other assets by:

- Enhancing the ability to mitigate cyber threats
- Facilitating the identification and operational response of cyber attacks
- Developing fast recovery and resiliency

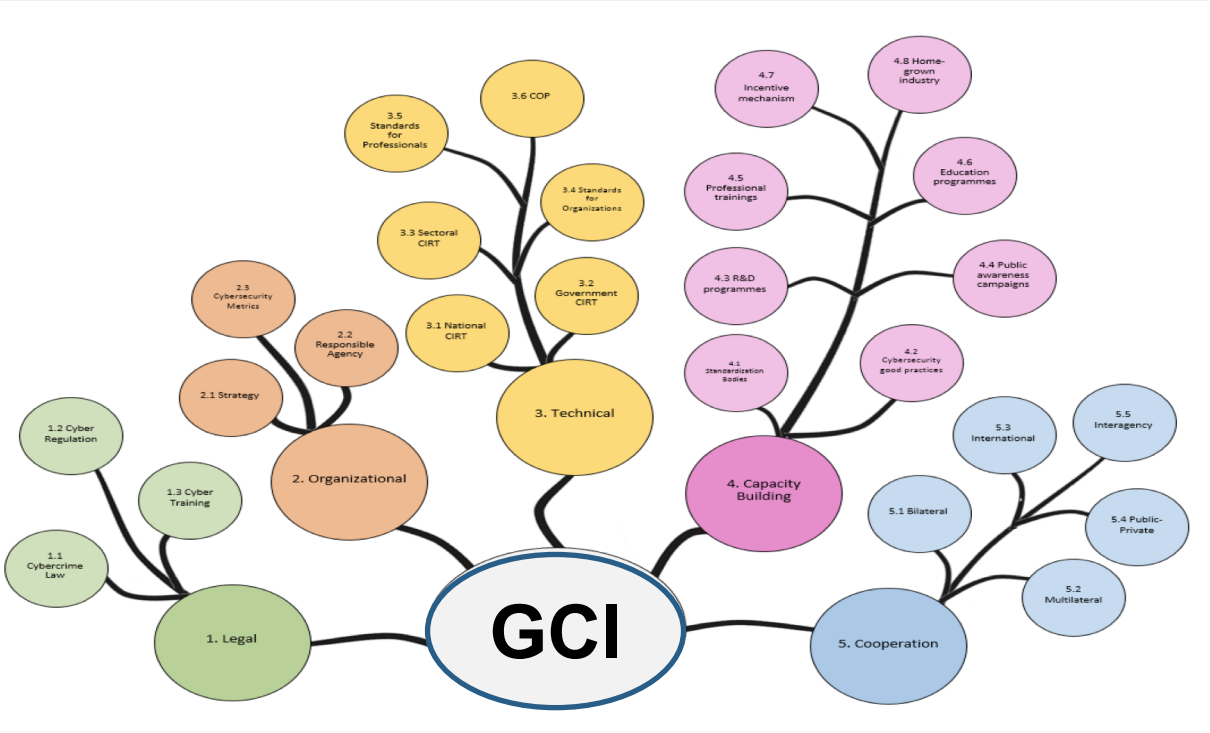
Cybersecurity stakeholders

Threats	• Hacktivism • Corporate espionage • Government-driven • Terrorism • Criminal
Vulnerabilties	• Accidental • Poor practice • Technology/processes/ • People
Values at risk	• Information and communication (data & infrastructure) • Assets • Reputation
Respones	• Policies / Regulations • Governance • Information sharing • Mutual aid • Coordinated actions • Risk markets • Embedded security

Cybersecurity Awareness: A multifaceted phenomenon

- Cognitive awareness is the capacity of :
  - Perception of the cyber threat elements
  - Comprehension of their meaning
  - Projection of their status in the future
- Technical (operational) awareness comprehends the capacities to :
  - Compile- Process-Fuse data
- Institutional
  - Governmental; Corporational; Individual
- Geographical
  - National/ International

Supermodularity in action

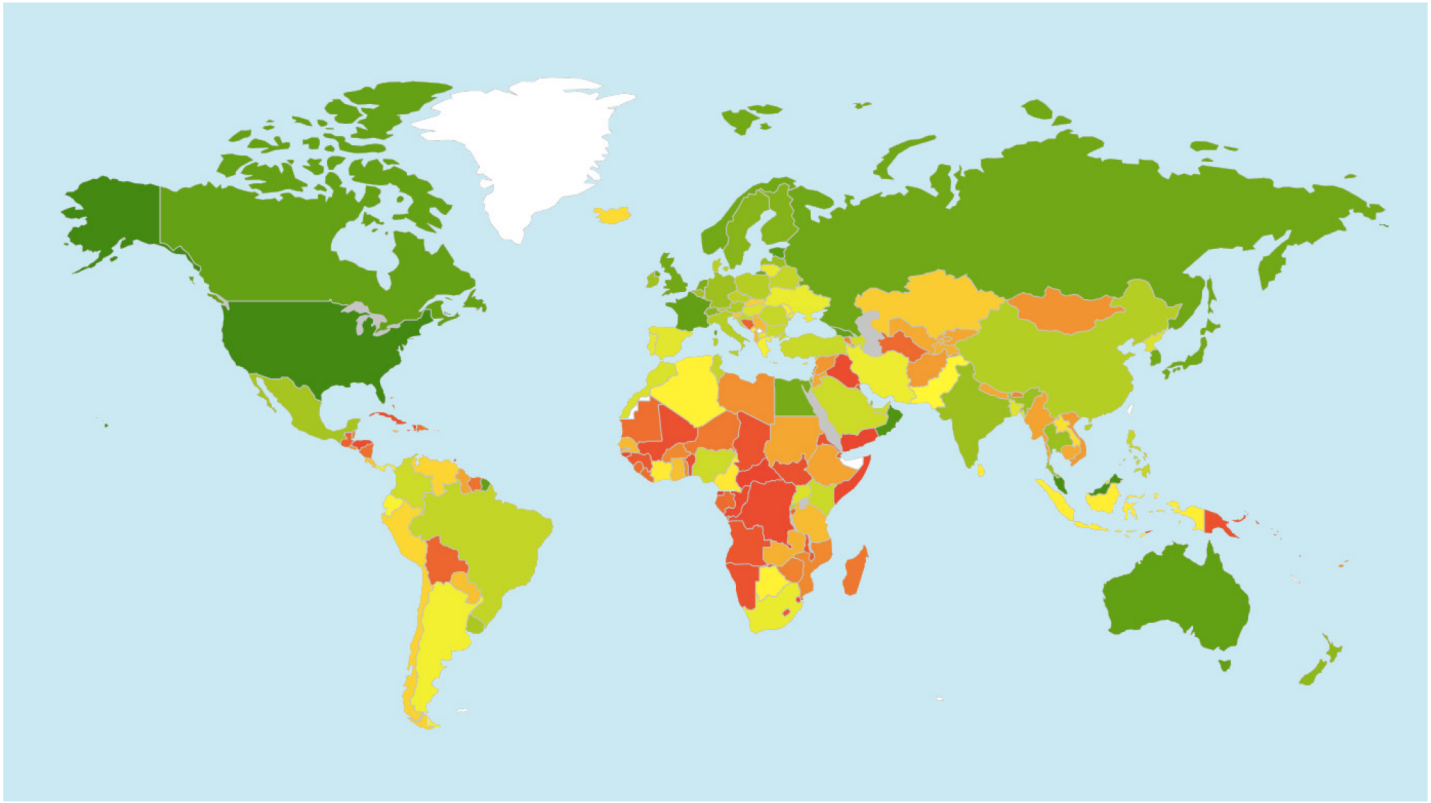


Source: International Telecommunication Union.

The pillars of
Global Cybersecurity Index

- Legal
- Technical
- Organizational
- Capacity building
- Cooperation

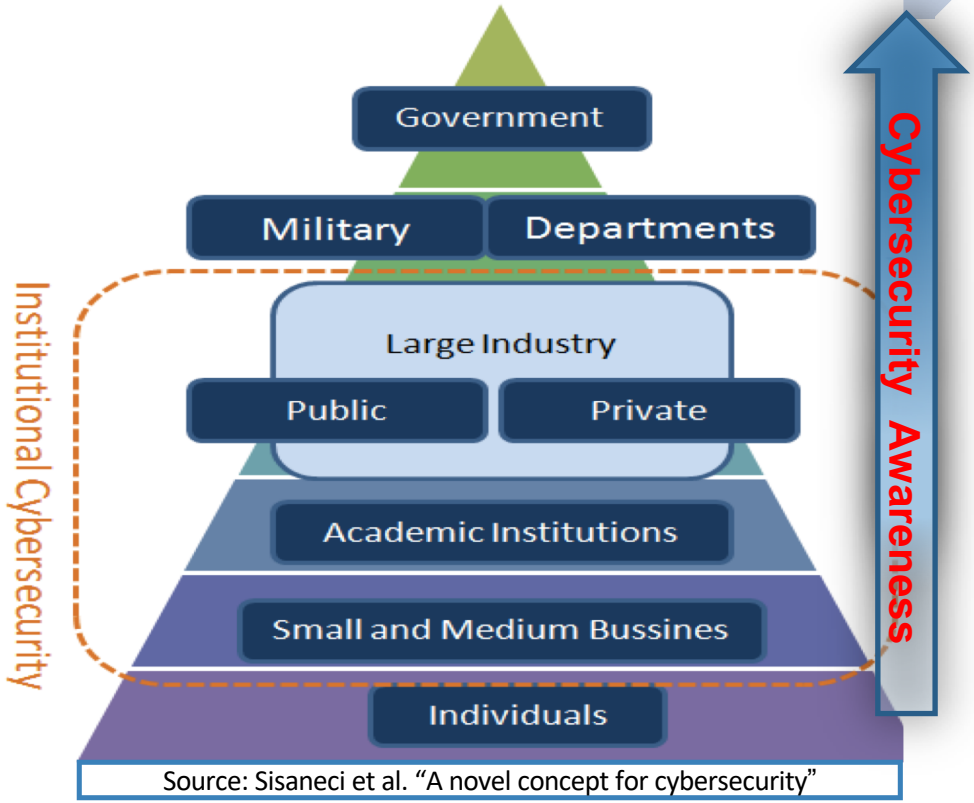
Global Cybersecurity Index (GCI)



Level of commitment: from Green (highest) to Red (lowest)

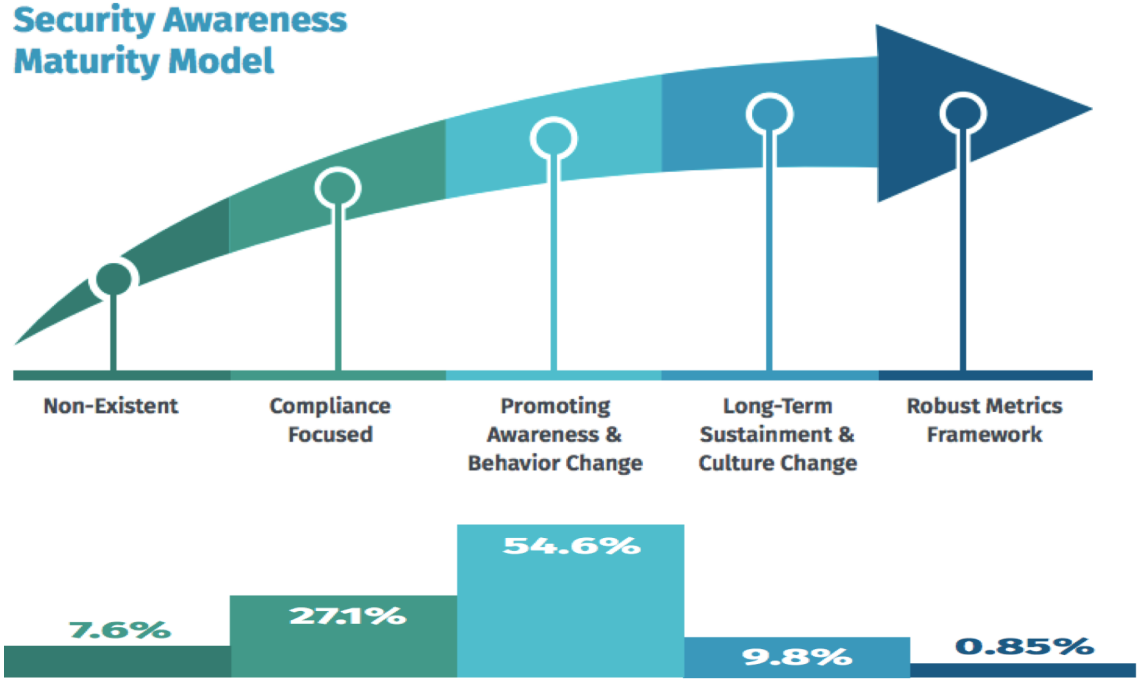
Source: International Telecommunication Union, 2017

National Systems of Cybersecurity



Source: Sisaneci et al. “A novel concept for cybersecurity”

Beyond Awareness, Toward Resiliency



Source: SANS. Cybersecurity Awareness Report, 2017

	Citizens	*SME*	*ISP*	*Large organisations*	*CI operators*	*The state/national security*	*Global infrastructure and issues*
AUS	■	■	■	■	■	■	□
CAN	■	□	□	■	■	■	□
CZE	■	■	■	■	■	■	
DEU	■	■	■	□	■	■	■
ESP	□	□	□	□	■	■	
EST	■	■	■	■	■	■	■
FRA	■	■	□	■	■	■	□
GBR	■	■	■	■	■	■	■
IND	■	■	□	■	■	■	
JPN	□	□		□	■	■	□
LTU	■				■	■	
LUX	□	□	□	□	■	■	
NLD	■	■	□	■	■	■	□
NZL	■	■	■	■	■	■	
ROU	■				■	■	
UGA	■	■		■	□	■	
USA	■	■	□	■	■	■	■
ZAF	□	□		□	■	■	

Notes: □ = when discussed in the NCSS but limited set of related actions/activities

Source: Luiijf & Besseling " Nineteen national cyber security strategies "

The future of Cybersecurity

Human approach

- Cybersecurity education
- A culture of cybersecurity

Artificial Intelligence approach

- The quantum computer
- The block chain technology

Cooperation imperative

- National
- International

Let’s recapitulate

- Cyber threats: exponential growth, permanent risk
- Cybersecurity: scale, scope and complexity
- The disjoint nature of national and global discussions and actions

Building Bridges toward Cybersecurity Resiliency

- A joint commitment
- Cooperation
  - Time
  - Space
  - Communication
  - Leadership
- A symbolic step?

  OSCE Cybersecurity **Resilience** Day

Thank you for your attention!

Questions & Comments?

For further contacts:
zhegu.majlinda@uqam.ca