Coproduction of Societal Cyber Resilience

Leaving no one behind in cyber security and resilience

MAMELLO THINYANE

Session: safe and secure resilient network solutions
Emerging Technology Week - ITU

Tuesday 6th July 2021, 11h00 – 12h00 (UTC+7)

UNITED NATIONS UNIVERSITY
Institute in Macau

SUSTAINABLE DEVELOPMENT GOALS

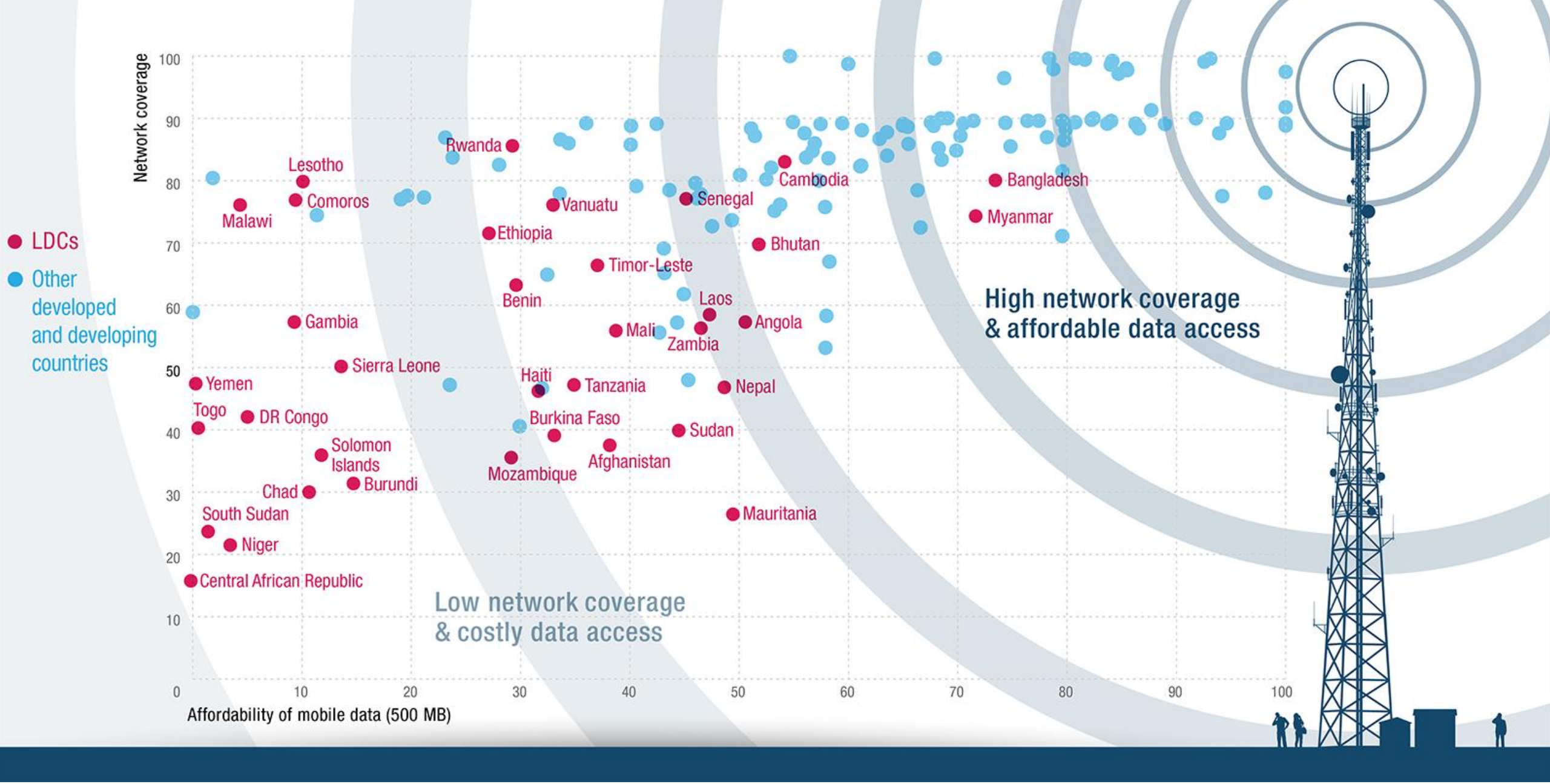
"Leave No One Behind"

JAN 2020

THE 'NEXT BILLION': UNCONNECTED AUDIENCES

THE NUMBER OF PEOPLE (IN MILLIONS) IN EACH REGION WHO ARE NOT CONNECTED TO THE INTERNET

SOURCES: ITU; GLOBALWEBINDEX; GSMA INTELLIGENCE; EUROSTAT; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; APJII; KEPIOS ANALYSIS (ALL LATEST DATA AVAILABLE IN JANUARY 2020).



Source: UNCTAD – 1st April 2021


Opportunities
Risks

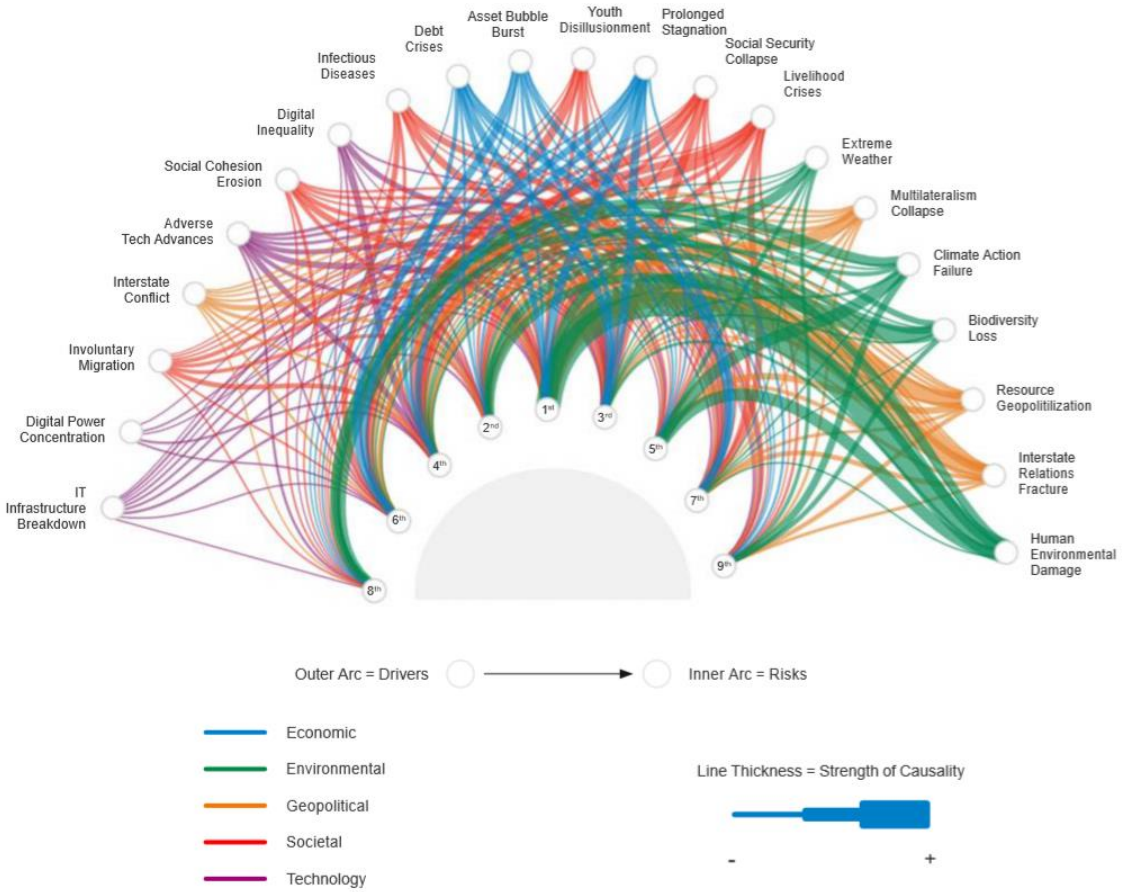
Top Risks
by likelihood

1. Extreme weather
2. Climate action failure
3. Human environmental damage
4. Infectious diseases
5. Biodiversity loss
6. Digital power concentration
7. Digital inequality
8. Interstate relations fracture
9. Cybersecurity failure
10. Livelihood crises

Top Risks
by impact

1. Infectious diseases
2. Climate action failure
3. Weapons of mass destruction
4. Biodiversity loss
5. Natural resource crises
6. Human environmental damage
7. Livelihood crises
8. Extreme weather
9. Debt crises
10. IT infrastructure breakdown

8th	6th	4th	2nd	1st	3rd	5th	7th	9th
Extreme Weather	Debt Crises	Social Cohesion Erosion	Infectious Diseases	Climate Action Failure	Livelihood Crises	Biodiversity Loss	Prolonged Stagnation	Human Environmental Damage



Source: World Economic Forum – Global Risk Report

RESILIENCE FOR THE NATION

“… ability to adapt, withstand and rapidly recover from emergencies.”

CRITICAL INFRASTRUCTURE RESILIENCE

“…ability to reduce the magnitude of disruptive events.”

COMMUNITY RESILIENCE

“… ability to **prepare** for hazards, **adapt**, withstand and rapidly **recover** from disruptions”

INFORMATION SYSTEM RESILIENCE

“…ability of the system to function under adverse conditions or stress.”

NETWORK RESILIENCE

“…ability of network to provide and maintain acceptable level of services in face of faults

RESILIENCE ENGINEERING

ability to build systems that can anticipate, survive, adapt and recover from disruptions

CYBER RESILIENCE

E-RESILIENCE

“… ability of ICT systems to withstand, recover from and change in the face of external disturbances."

CYBER RESILIENCE

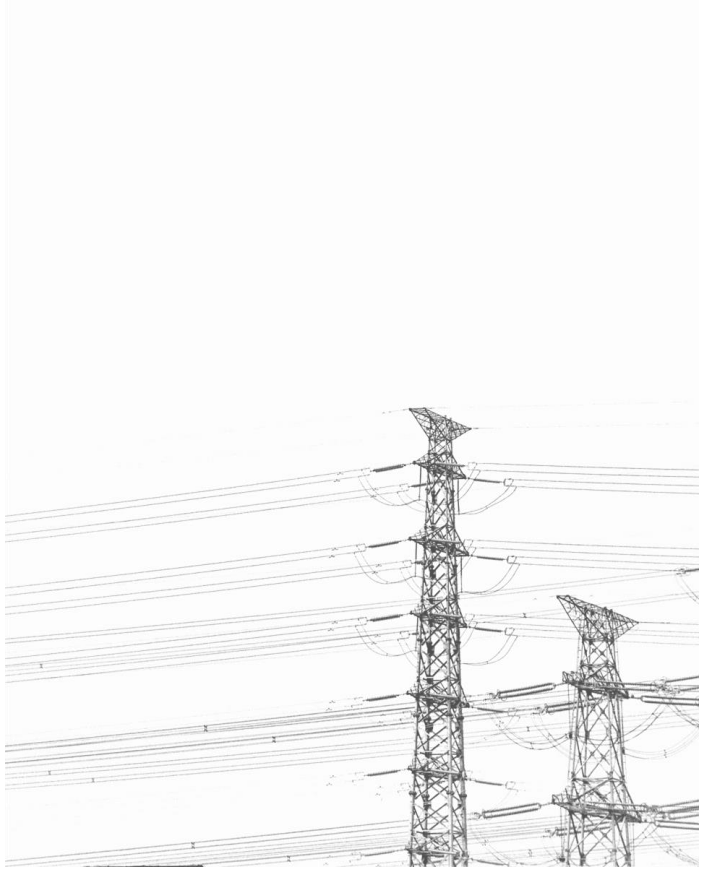
the ability to continue functioning and achieving the desired outcomes in the face of disruptions due to adverse cyber events

DIGITAL RESILIENCE

“… ability to harness digital resources to sustain wellbeing.”

TECHNICAL / SYSTEMS

Focus on information systems, ICT infrastructure, technology tools and platforms



CRITICAL INFRASTRUCTURE

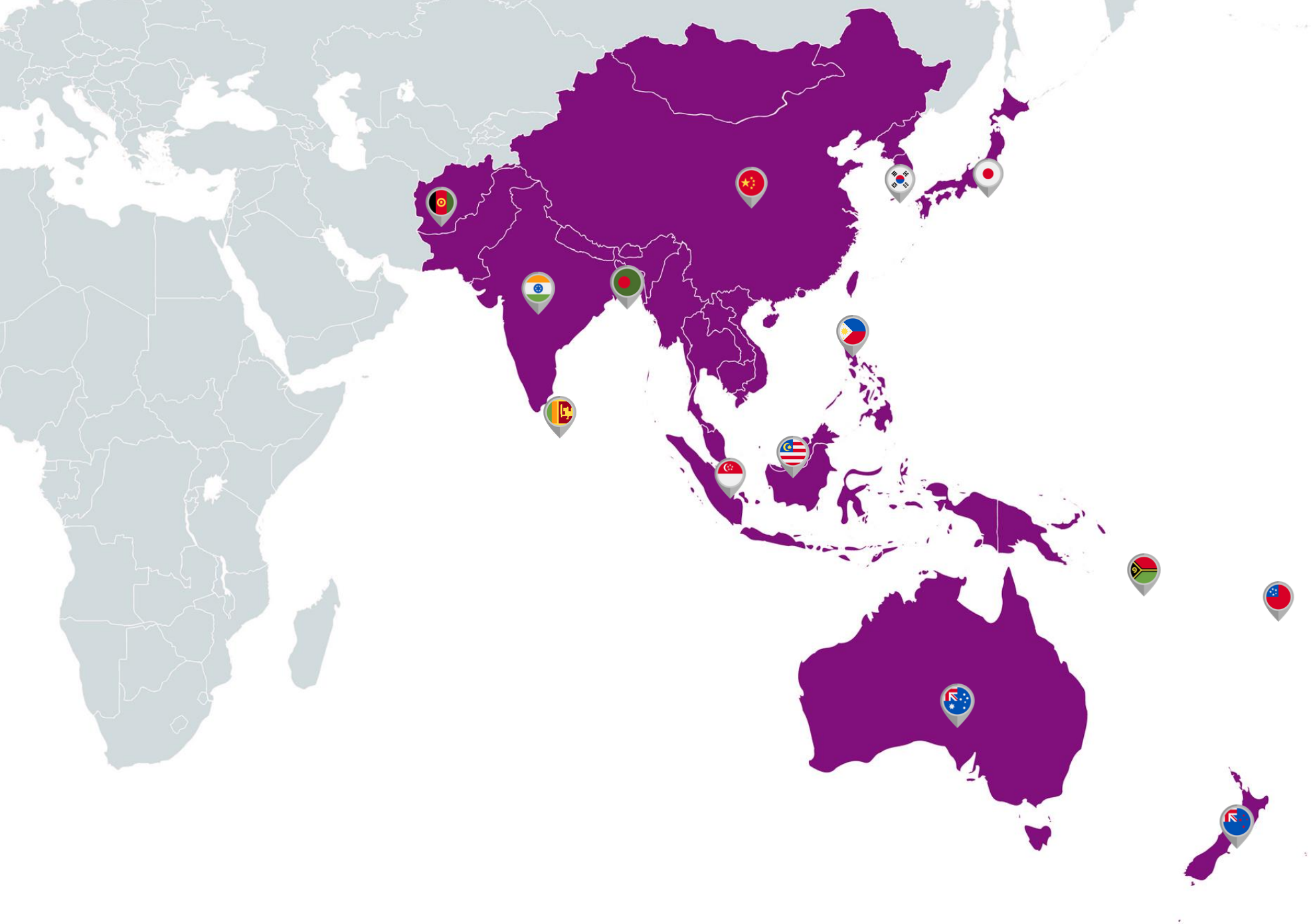
Due to the high impact of failure of critical information infrastructure / SCADA systems

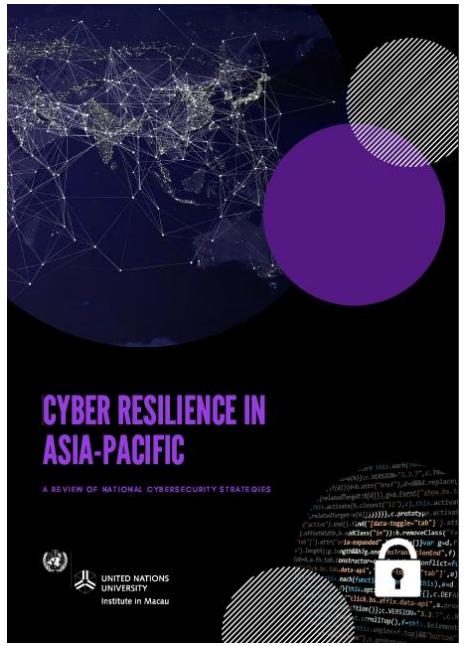
GOVERNMENT & BUSINESS

Focus on government and private sector; better interaction between governments and businesses

To what extent do national cyber security strategies incorporate a resilience perspective and a whole-of-society cyber resilience perspective?

In the Asia-Pacific region

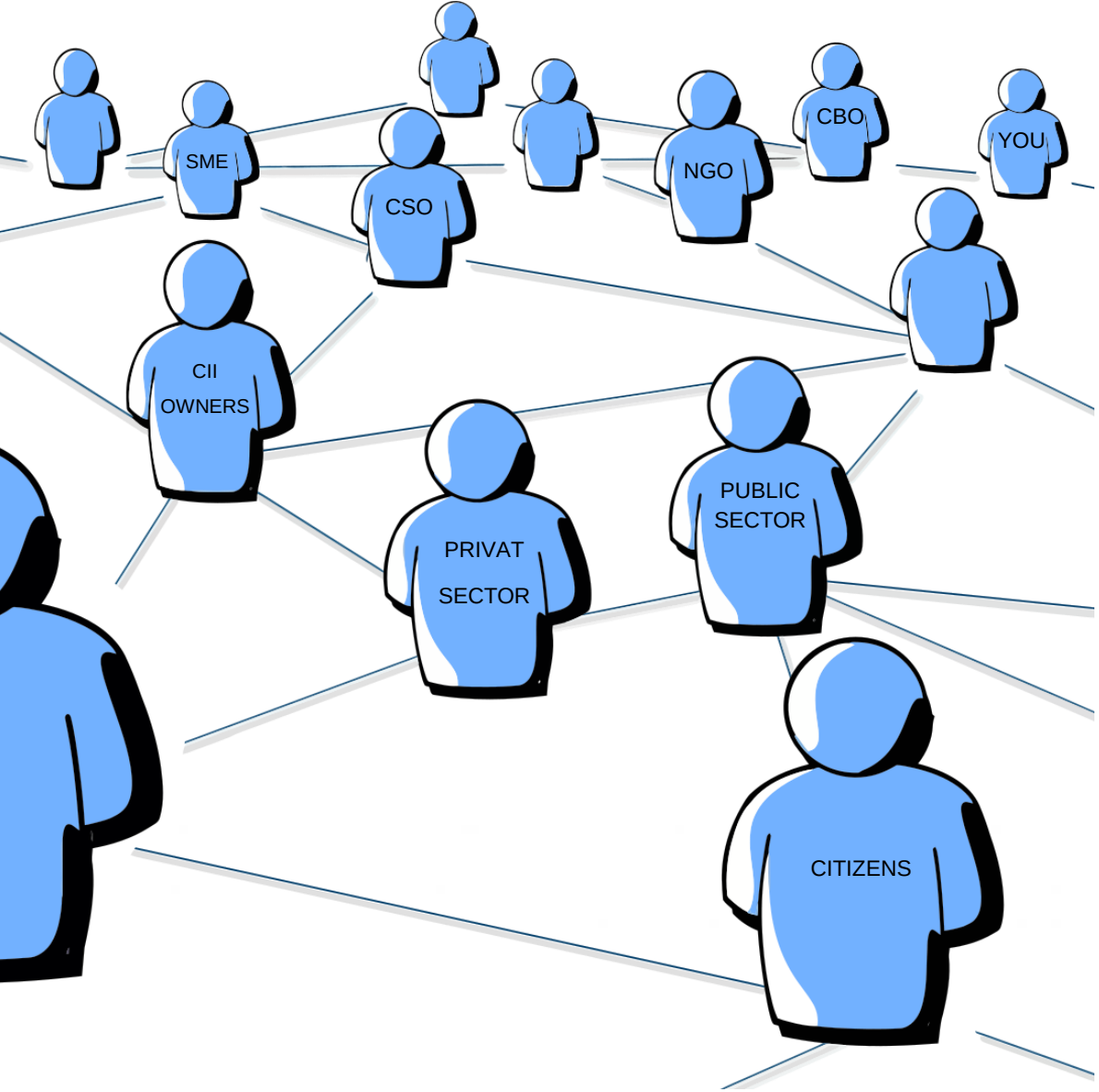



CYBER RESILIENCE IN
ASIA-PACIFIC
A REVIEW OF NATIONAL CYBERSECURITY STRATEGIES
UNITED NATIONS
UNIVERSITY
Institute in Macau

KEY FINDINGS:

The full report available at
https://collections.unu.edu/view/UNU:7760

- Several countries include resilience thinking in their strategies
- Few countries give elaborate framing and operationalization of cyber resilience
- All countries acknowledge cyber security as a shared duty of all stakeholders
- However, there are limited avenues for citizen co-production of cyber security
- Citizens largely framed as recipients of cyber security
- There is better engagement and well-defined roles and modalities for certain sectors e.g., government and private sector



WHY CONSIDER CIVIL SOCIETY FOR NATIONAL CYBER RESILIENCE?

- Resilience is a systemic attribute and requires whole-of-society approach
- Multi-dimensionality of cyber resilience
- Important responsibility of civil society as active cybersecurity agents
- Increasing cyber risks to individuals and communities
- People are the key attack surface and vector
- Current cybersecurity frameworks are difficult to operationalize for civil society

Recommendations

- Frame cyber resilience as a holistic, systemic, and whole-of-society goal.
- Provide a multi-dimensional framing of cyber risks and countermeasures, beyond the technical.
- Consider the different needs and capacity of all the stakeholders in cybersecurity.
- Clearly articulate the roles of all stakeholders within the cybersecurity ecosystem, and the legal avenues and means of engagement for civil society stakeholders.
- Enable instrumental and representative participation of civil society stakeholders.

THANK YOU

UNITED NATIONS UNIVERSITY
INSTITUTE IN MACAU
Estrada do Engenheiro Trigo No 4, Macau SAR

CONTACT
mamello@unu.edu

Emerging Technology Week

Safe and Secure Resilient Network Solutions:

The Impact of Emerging Technologies on Personal Privacy and National Sovereignty

Aaron Boyd
Managing Partner
Welchman Keen
aboyd@welchmankeen.com

WELCHMAN KEEN

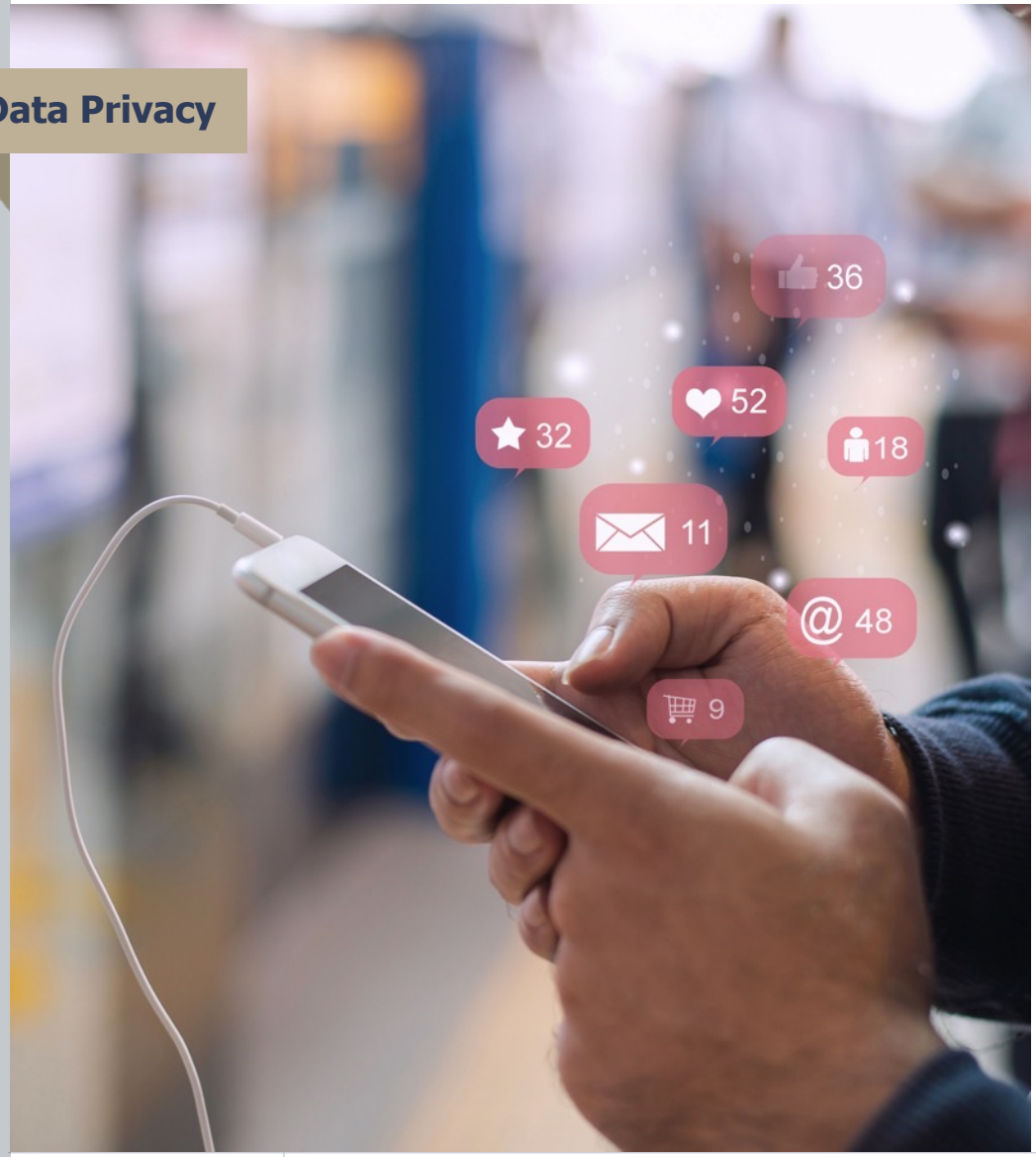
DATA PRIVACY

Personal Privacy and Data Sovereignty

- ✓ Privacy refers to the degree of control that a person has concerning access to and use of his/her personal information. Most e-mail and Internet users assume that personal information will not be used without permission and that information exchanges are private and secure. The reality, however, is very different. *81% of users feel that they have no control over their data.**
- ✓ Every time you access a website, post content on social media or send an e-mail, you leave information about yourself that could include your physical and computer address, telephone and credit card numbers, consumer pattern data and much more.
- ✓ Personal Data Sovereignty (not speaking of data residency/sovereignty definition) refers to the idea that individuals should have ownership over their information by default, and that any collection, use or sale of personal data should not occur without explicit authorization of the original owner.

*Pew Research Center: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Data Privacy



Is Data Privacy a Myth?

- ✓ The reality is that over the past 25 years, connected humanity has shown that it will tolerate a free market exchange in personal data outside of their control in favor of free or discounted goods and services.
- ✓ Even while this awareness builds resistance to this process is relatively small and fleeting.
- ✓ The ultimate cost is evidenced in terms of unprecedented amount and granularity of personal information available to influence our choices and behaviors for economic or political gain, resulting in an erosion of personal sovereignty.
- ✓ External influence can be measured in terms of individual and collective behaviors that would not have taken place in the absence of directed efforts such as marketing or political campaigns.
- ✓ 128 countries, including 66 developing countries have put data and privacy protection in place. In Asia 57% of countries have a law in place and 27% have no legislation.*

*UNCTAD: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Privacy and Security

- ✓ Because our data is aggregated and stored in multiple locations, we have very little control over each iteration, how it can be accessed and used, and how that information is secured. Data breaches in any one of these thousands of servers can result in small to highly disruptive and life changing identity theft and fraud.
- ✓ Only 2% 0f firms that have reported a data breach have been fined.*
- ✓ Effort to overcome these (for those who care) include purchasing goods and services which value privacy, do not store personal data, adopt open-source software models and do not profit from the use of personal data.

*IAPP: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/

Data Privacy

National Data Sovereignty

- ✓ At a national level, the current state of individual data collection and use is certainly impactful in terms of collective behavior, thoughts and attitudes.
- ✓ Governments worldwide are grappling with their own cybersecurity and privacy laws and how to deal with a rapid evolution in technology.
- ✓ There is an additional layer of consideration to national security and sovereignty where it comes to how important or sensitive data flows and is managed which has risen to occupy international dialogue and debate.
- ✓ "[Local] data centres reduce the necessity of sending traffic abroad, not only saving on expensive international bandwidth but also enhancing data sovereignty over sensitive information."*
- ✓ While some may be comfortable with the flexibility of avoiding blanket policies or determining who would be the ultimate arbiter of various international norms, others are warning of the potential dangers of the status quo.

Wk.

**Achieving universal and affordable Internet in the least developed countries*, ITU Thematic Report, 2018 ISBN 978-92-61-25461-2

Emerging Technologies

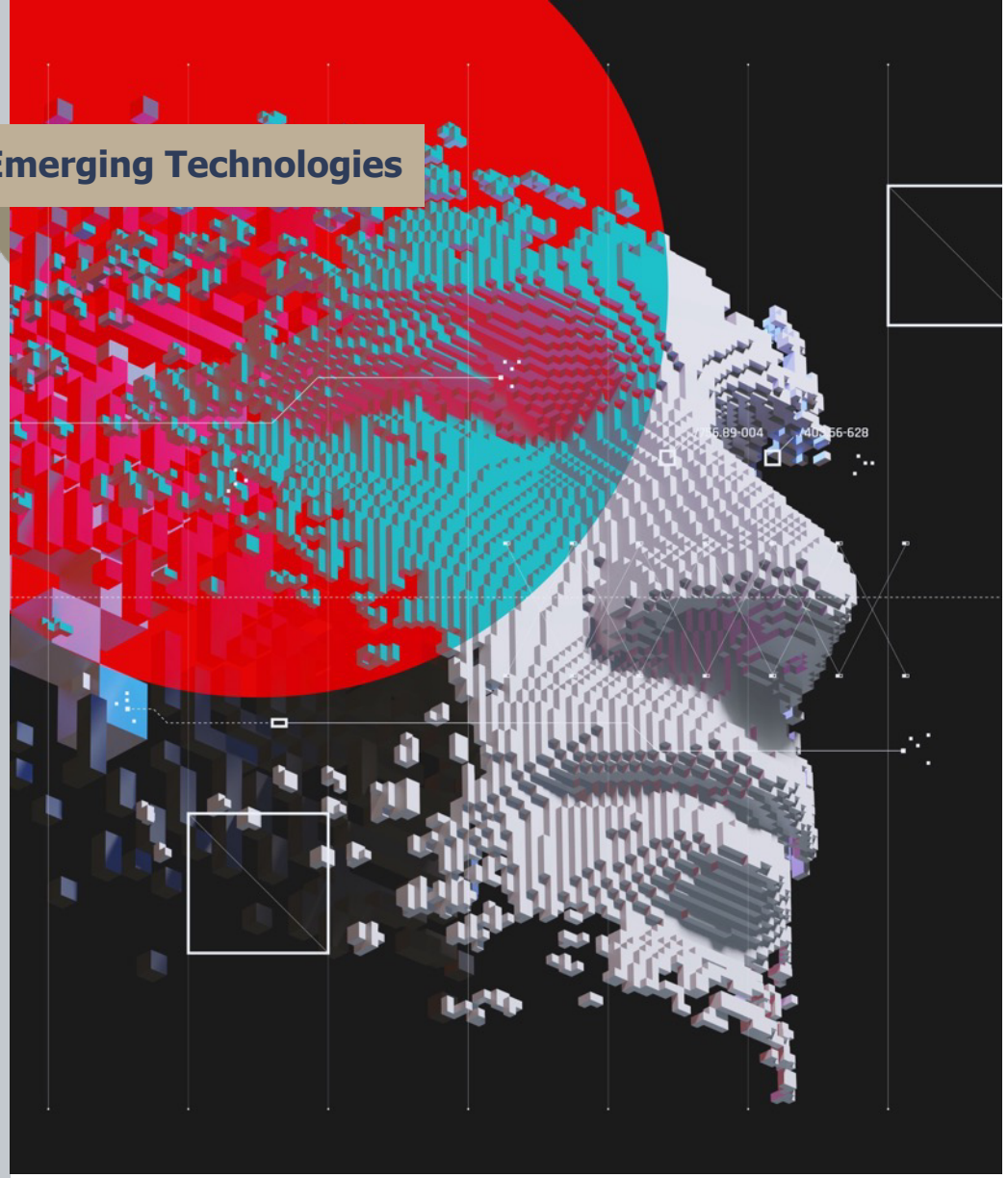
- ✓ There is no reason to believe that an increasingly interconnected world that is established on the current set of rules and norms would be any different from the challenges we face today.
- ✓ Emerging technologies that will connect increasingly more things and people are advancing faster than the conversation about how to govern and secure them.
- ✓ The advantage will go to those who can leverage the complexity of advanced systems over those who do not. We should endeavor to ensure that governments and populations are equipped to deal with the effects of connectivity even as we champion its growth.
- ✓ With the understanding that there are many competing business, economic, social and national interests, companies, governments, IGOs and NGOs should endeavor to work together to build a trust-but-verify system of data governance that ensures the greatest degree of personal and national data sovereignty while accounting for lawful intercept, legal parameters and a variety cultural norms. Not an easy task.

Wk.

Blockchain

- ✓ Should build trust at its core due to the ledger, but is treated with suspicion
- ✓ Cryptocurrencies: Personal privacy around encryption but associations with risk, criminality
- ✓ May eventually stabilize and have greater impact on international currency trades: Imaging a national currency using or pegged to cryptocurrency
- ✓ Potential impact on national tax revenue, legal implications

Emerging Technologies



Artificial Intelligence

- ✓ Already leveraged to take advantage of personal data and interact accordingly. The more it knows, the better it can profile and follow human psychological algorithms intended to produce the desired effect.
- ✓ AI bias is an increasing concern.
- ✓ Who's AI? Who's values, priorities and ethical standards? 70% of global population lives in developing countries.
- ✓ Those producing AI technologies may optimize toward profit or national interests at the expense of LDC, LLDC, SIDs citizens.
- ✓ *90% of AI research takes place in just five countries.**

The Global AI Talent tracker: https://macropolo.org/digital-projects/the-global-ai-talent-tracker/

IoT

- ✓ Technologies increasingly interwoven and invisible
- ✓ Too many access points to manage and protect
- ✓ Increased attack surface area
- ✓ Access to control systems and critical infrastructure
- ✓ Increased risk of physical harm from virtual attacks
- ✓ Increased opportunities for surveillance and data farming – both corporate and state

Satellite

- ✓ Access to frequencies and launch tech make this a very real game-changer
- ✓ Rural and far-flung communities will have access to data and feeds at similar speeds to urban centers
- ✓ Close the digital divide
- ✓ But - Impact of social media and importance of discerning real from fake or misleading information - a growing global problem.
- ✓ National Sovereignty – concerns over lack of government control at gateways as in ground-based Internet.

Conclusion

Recommendations

- ✓International dialogue on privacy standards have an impact LDCs, LLDCs and SIDs
- ✓These counties should have full awareness of how their citizen's data is obtained, used, stored and shared.
- ✓Governments should examine their own national cybersecurity and privacy laws and ensure it reflects their own objectives and values.
- ✓Governments should ensure connecting the unconnected is accompanies by education on COP, cybersecurity and misinformation around important public health and security topics like COVID
- ✓International vendors should rally around open-source standards that prioritize individual privacy and national sovereignty such as GDPR, O-RAN etc.

Wk.

END OF SESSION

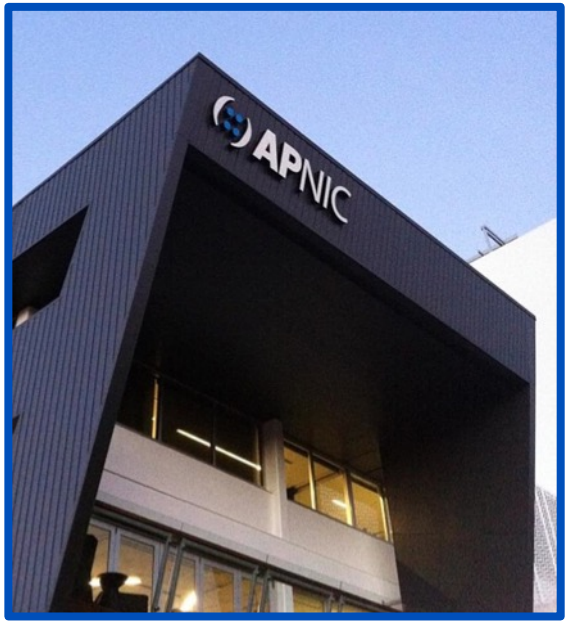
QUESTIONS

Building Cyber Resilience – Internet of Communities

Joyce Chen
Senior Advisor – Strategic Engagement
APNIC

Internet of ~~Things~~ Communities

*"A global, open, stable and **secure** Internet that serves the entire Asia Pacific community"*

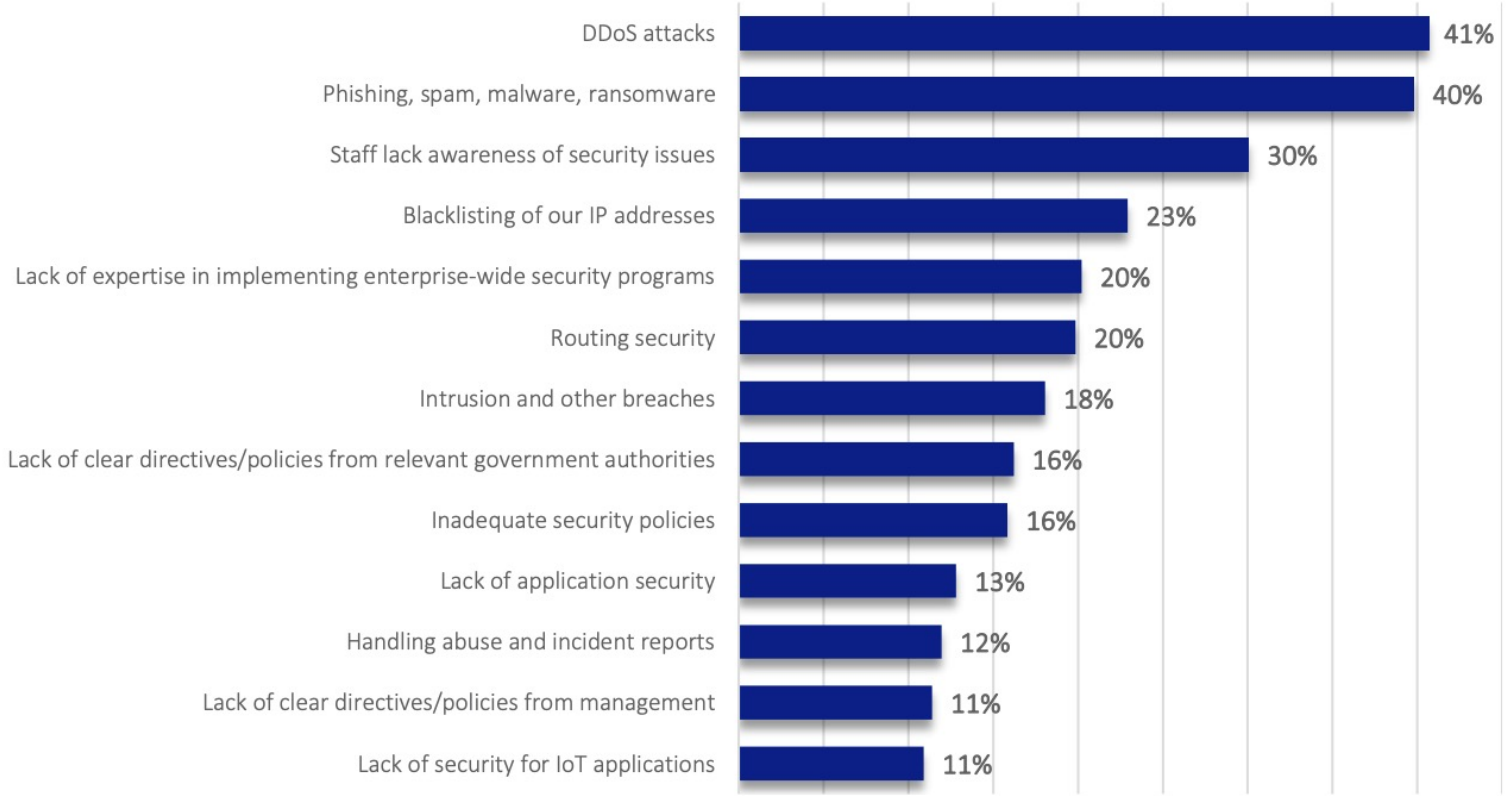


APNIC at a Glance

- Regional Internet Registry (RIR) for the Asia Pacific Region
- Delegate Internet number resources that enable devices to connect
  - IP addresses (IPv4 & IPv6) and
  - AS Numbers
- Internet Development work as part of the Internet infrastructure
  - Policies / Governance
  - Capacity Development
  - Engagements
- More about us: https://www.apnic.net

APNIC Membership Survey 2020

Thinking about network security, what are the MAIN challenges facing your organisation?



Experts estimate that cybercrime will cost the world $10.5 trillion annually by 2025

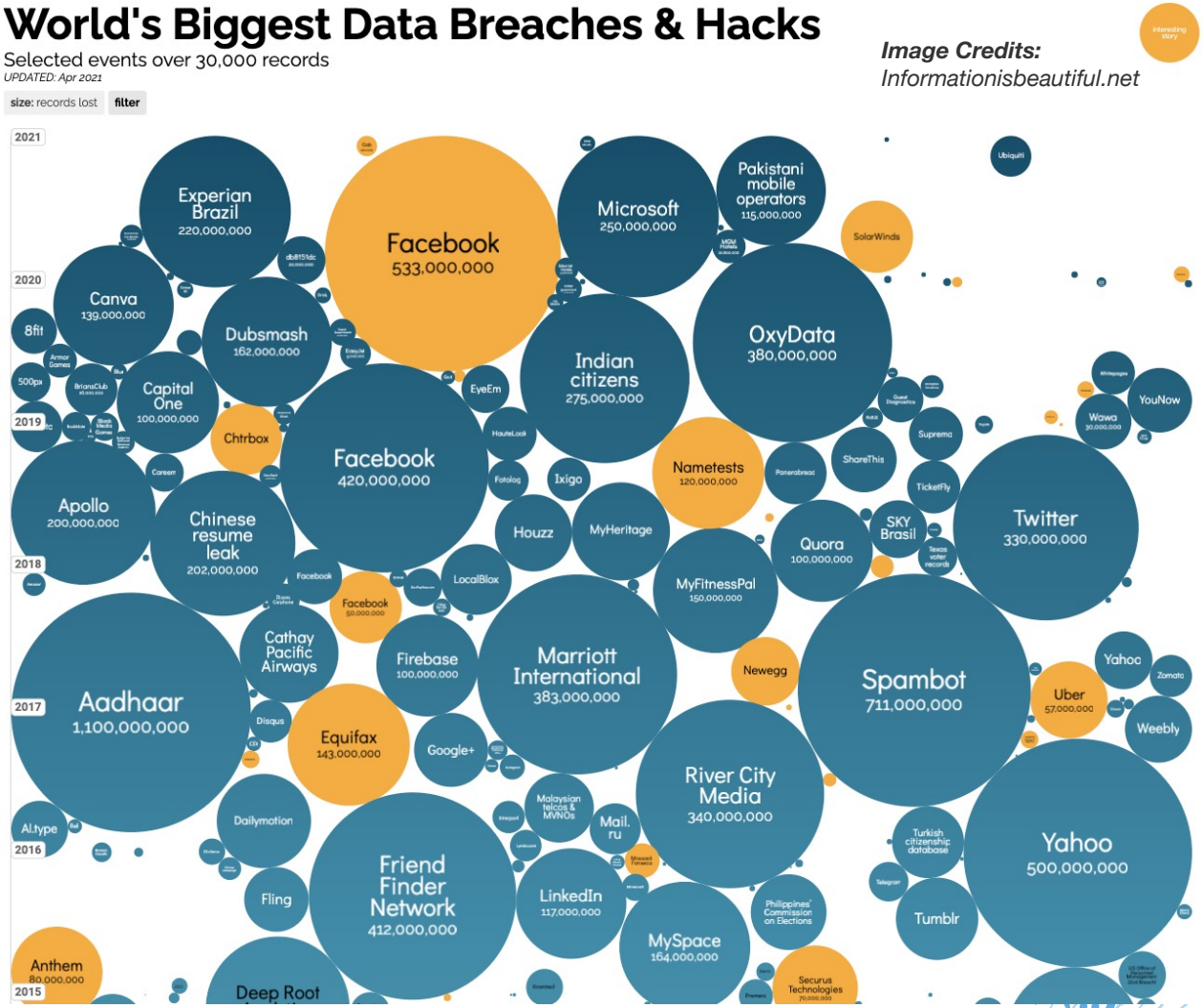


Image Credits:
Informationisbeautiful.net

Common Causes of Data Breaches

- Ransomware
- Malware
- Phishing
- Denial of Service (DoS)

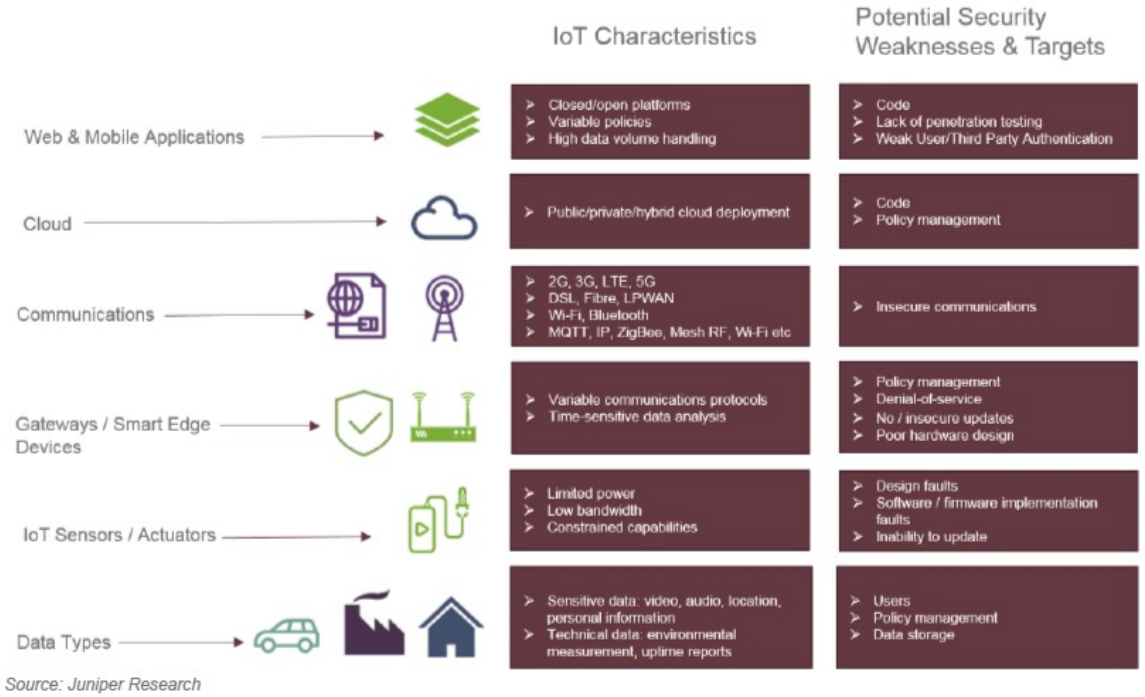
Supply Chain Attacks - SolarWinds

- Large and broad scale attack by hackers
- Affected multiple government organisations and companies in the US
- Single point of entry – SolarWinds
- Infiltrated:
  - 425 of US Fortune 500
  - Top 10 US telecommunications companies
  - Top 5 US accounting firms
  - US Military, Pentagon, State Department
  - Hundreds of universities and colleges worldwide
  - FireEye cybersecurity firm

Image Credits: *David Wolpoff*

Internet of Things

- Bigger attack surface
- Unsophisticated devices -> greater vulnerabilities
- Users “forget” it’s connected
- Multiple points of entry for attacks to happen



Source: Juniper Research

“Infrastructure” – Internet Infrastructure

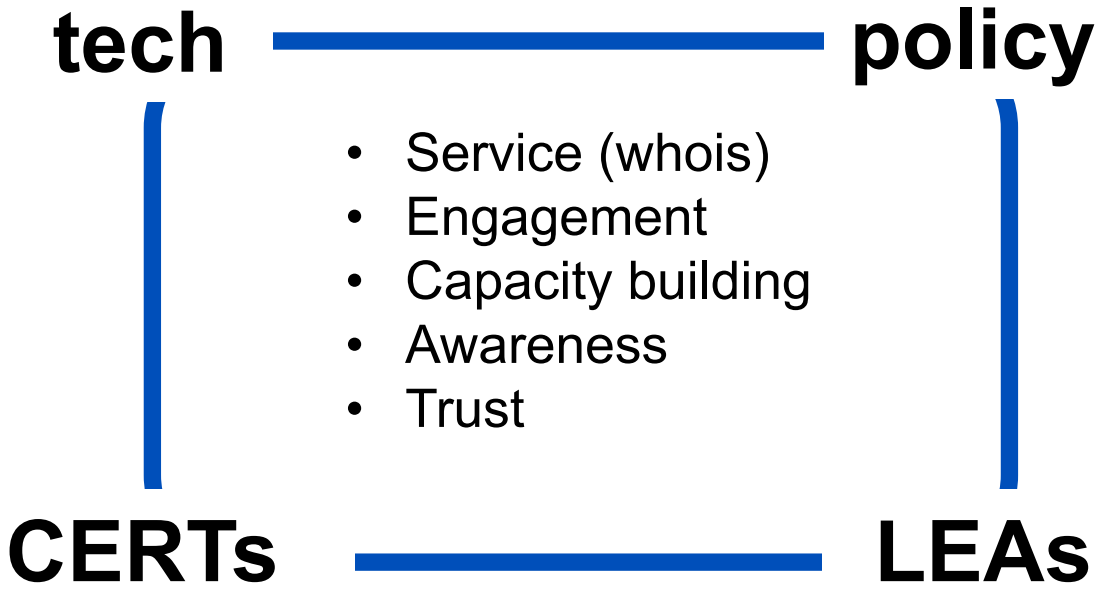
- Underlying “infrastructure” that enables (trusted) communication and utilized by all
- Broader in term of context, beyond specific economies
- Infrastructure:
  - Distributed Systems
  - Communications Protocols
  - Physical
- Exposure to network risks
  - Traffic Redirection, Denial of Service (Outages)
- Security, Stability and Safety of the Infrastructure must be ensured
- Critical role Network Operators and Service Providers

Internet of ~~Things~~ Communities

Stakeholders in the Cyber Ecosystem

- Network operators
- Security Ops, CERTs/CSIRTs
- Law enforcement
- Policy Makers
- End-Users
- Universities and NRENs (National Research and Education Networks)
- Civil society

Security @ APNIC

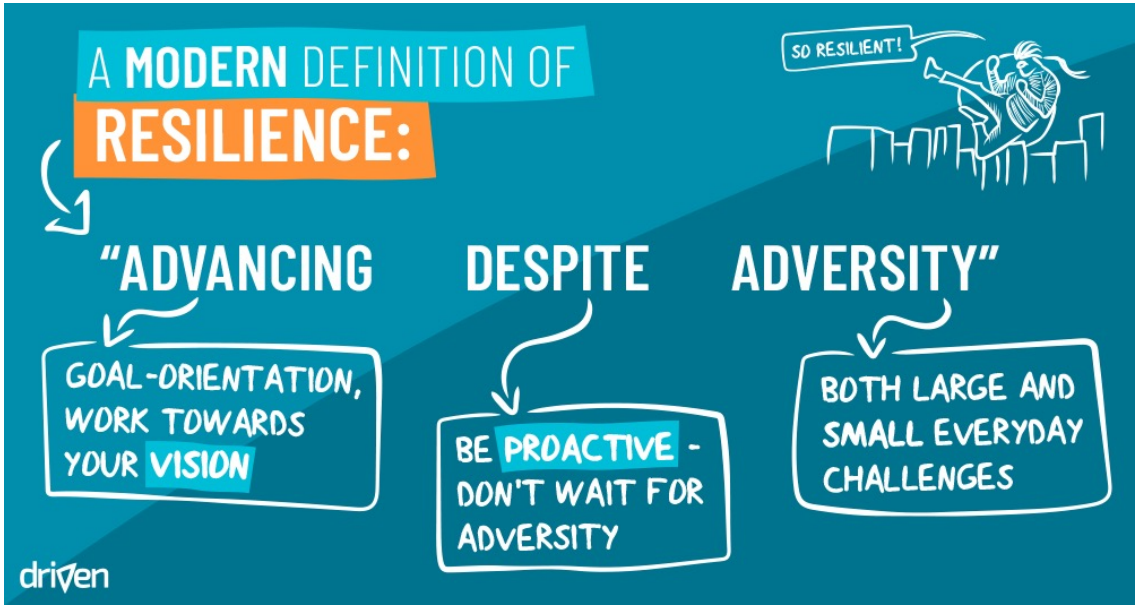


Security @ APNIC

- Security training and capacity building for Network Operators
- Awareness raising and deployment of best practices
- Development of the Asia Pacific security community
- Bridges between security community and network operators
- Follow cyberpolicy discussions

The Art/Science of Being Resilient

- Being Resilient
  - “The Ultimate Goal”
- What it means
  - Adapt to change
  - Business Continuity – attacks are bound to happen
  - Capabilities



How We Can Support

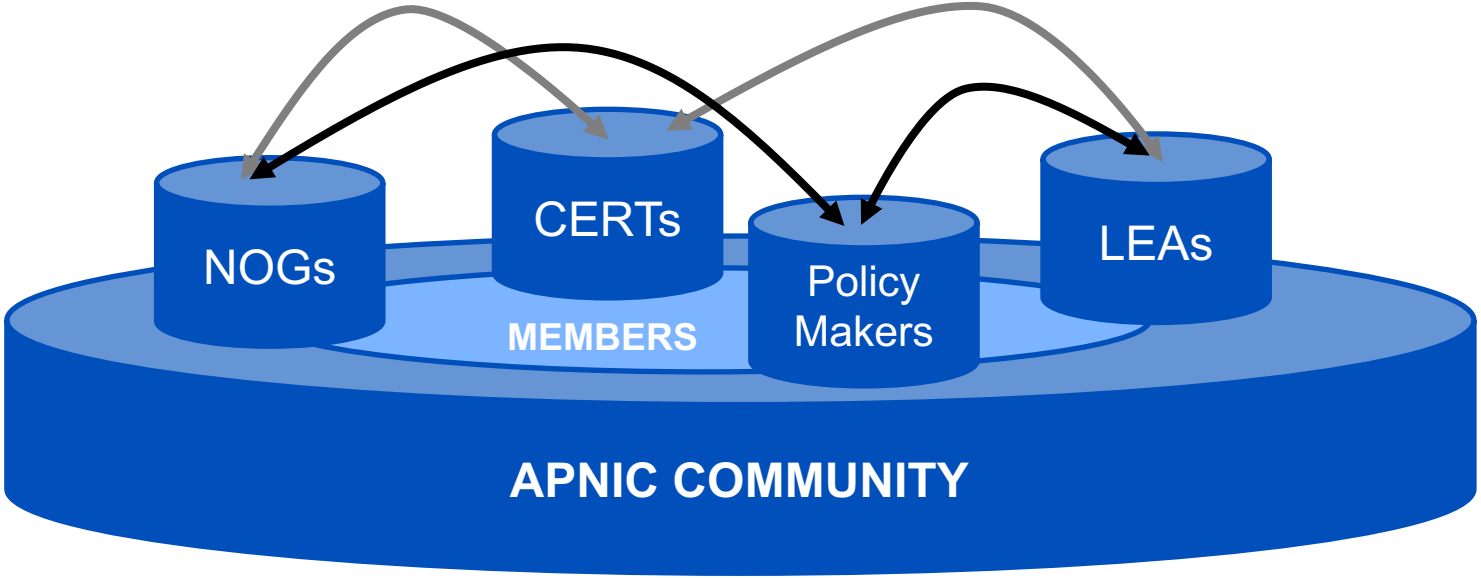
- Invest in your technical and security communities – capacity building
- Invest in infrastructure development and maintenance
- Develop robust policies and engage critical infrastructure providers
- Develop and empower CERT/CSIRT teams – trust them to do their work!
- Encourage collaboration beyond borders and sectors – the Internet does not stop at your borders and attacks don't work in silos
- Increase overall resilience, preparedness, awareness

APNIC Training & Technical Assistance

In 2020,

- 18 Open eTutorials and eWorkshops
- 18 Webinars
- Covered more than half of Asia Pacific region
- Delivered over 107 days
- 2,678 instructor-led physical and online students
- 5 new Community Trainers – total 24
- Provided technical assistance to 12 Members on IXP operations, IPv6, and routing security

Our Community Approach



Building Resilience - Internet of Communities

- Open, inclusive and multistakeholder approach means to engage community directly
- Every element is part of a bigger Internet ecosystem
- Expertise must be obtained, and maintained
- Cybersecurity: strong as the weakest link
- Trust, collaboration and neutrality are PARAMOUNT

Thank You

Let’s Connect!

joyce@apnic.net