Security Collaboration Beyond Your Traditional Borders

Adli Wahid

Senior Internet Security Specialist, APNIC

Let’s Connect!

Email: adli@apnic.net

LinkedIn: Adli Wahid

Twitter & Instagram: @adliwahid

- Regional Internet Registry for the Asia Pacific Region (56 Economies)
- Manage and distribute IP addresses & AS Numbers
- Whois Database
- Capacity development, Policy, Multistakeholder engagement
- Based in Brisbane, Australia
- https://www.apnic.net

- Association of CERTs/CSIRTs around the world
- 442 Teams in 90 countries
- Trusted community, volunteers
- Enable information sharing, awareness raising, support for incident response teams
- Capacity development
- https://www.first.org

8th APCERT AGM & Conference **2009** Kaoshiung, TW

Photo Credits: Keisuke Kamata

The Plan

- Reflection
- Share Experience
  - CSIRT Establishment in the Pacific
  - Engagement with Policy Makers

Borders – Physical and Invisible

Threatbutt Internet Hacking Attack Attribution Map

twn (123.24.24.114) uses BUTTER PANDA against rus (136.16.209.246) -- We'll just call it a "glitch"
irn (225.225.83.83) uses Heartbleed virus against usa (142.87.15.204) -- UPGRADE TO PREMIUM FOR MORE INFO$
nzl (139.148.211.80) uses EXTRABACON against bra (214.126.59.231) -- it didn't work so good
chn (207.209.194.90) uses Metasploit against kor (213.15.48.155) -- IT'S CYBER POMPEII !
chl (134.37.84.126) uses QUANTUM LEAP against usa (161.140.128.3) -- We'll just call it a "glitch"
bra (75.204.76.200) uses V.E.N.O.M. against jpn (234.136.115.14) -- it didn't work so good

Organisation A

Our Organisation

Organisation C

Organisation D

Organisation B


Community V


Our Community


Community X


Community U


Community Z


Community Y

Adversary's Perspective

“Attack Map”

Profile
DNS
AS Numbers
IP Address

The Internet

Attacker

Image Source: https://imgur.com/gallery/7ok4g

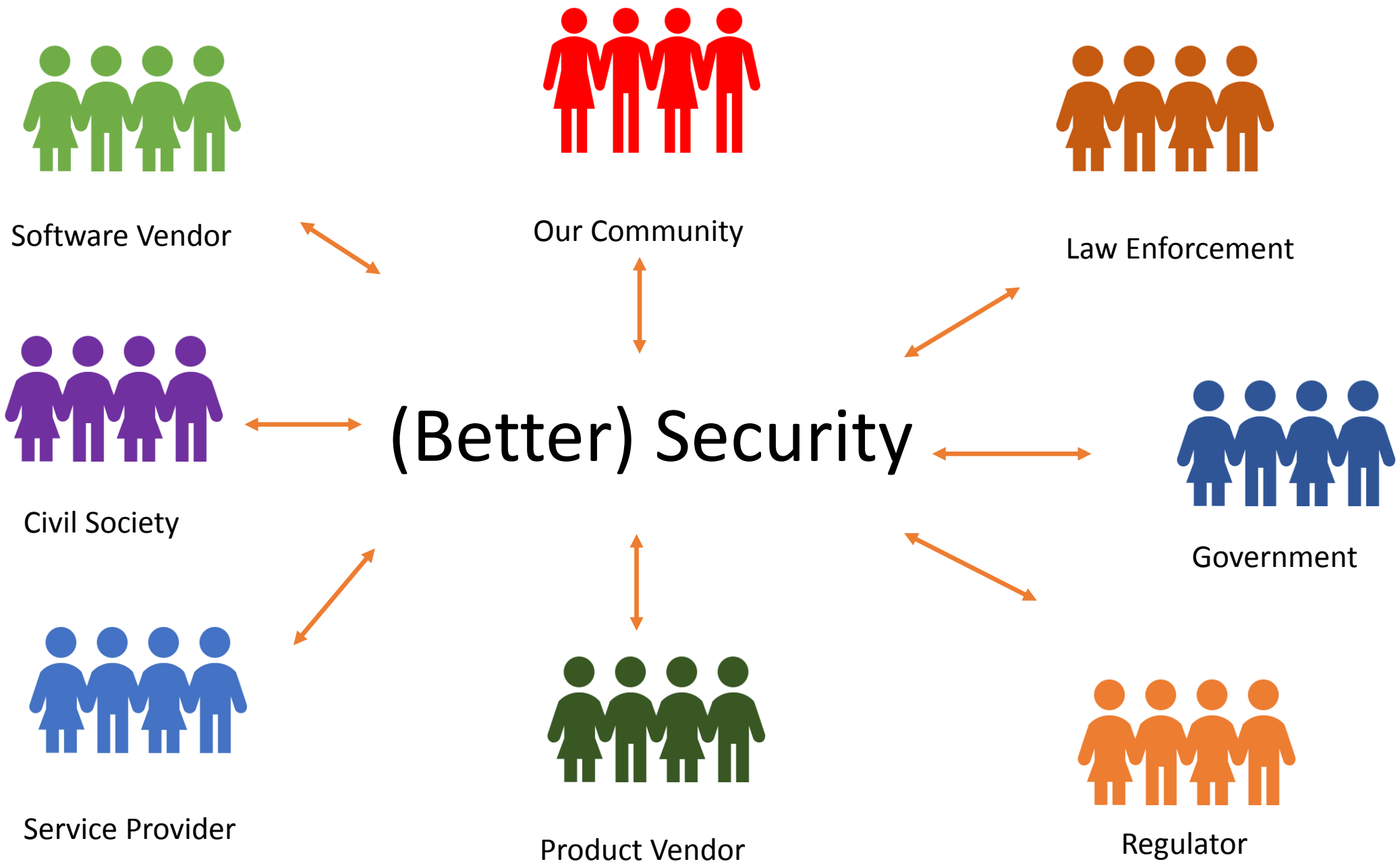
Cloud Provider
~~Organisation A~~

The Target
~~Our Organisation~~

Vendor for Finance System
~~Organisation C~~

Vendor for HR System
~~Organisation C~~

IT Solutions Provider
~~Organisation B~~


Software Vendor
Our Community
Law Enforcement
Civil Society
(Better) Security
Government
Service Provider
Product Vendor
Regulator

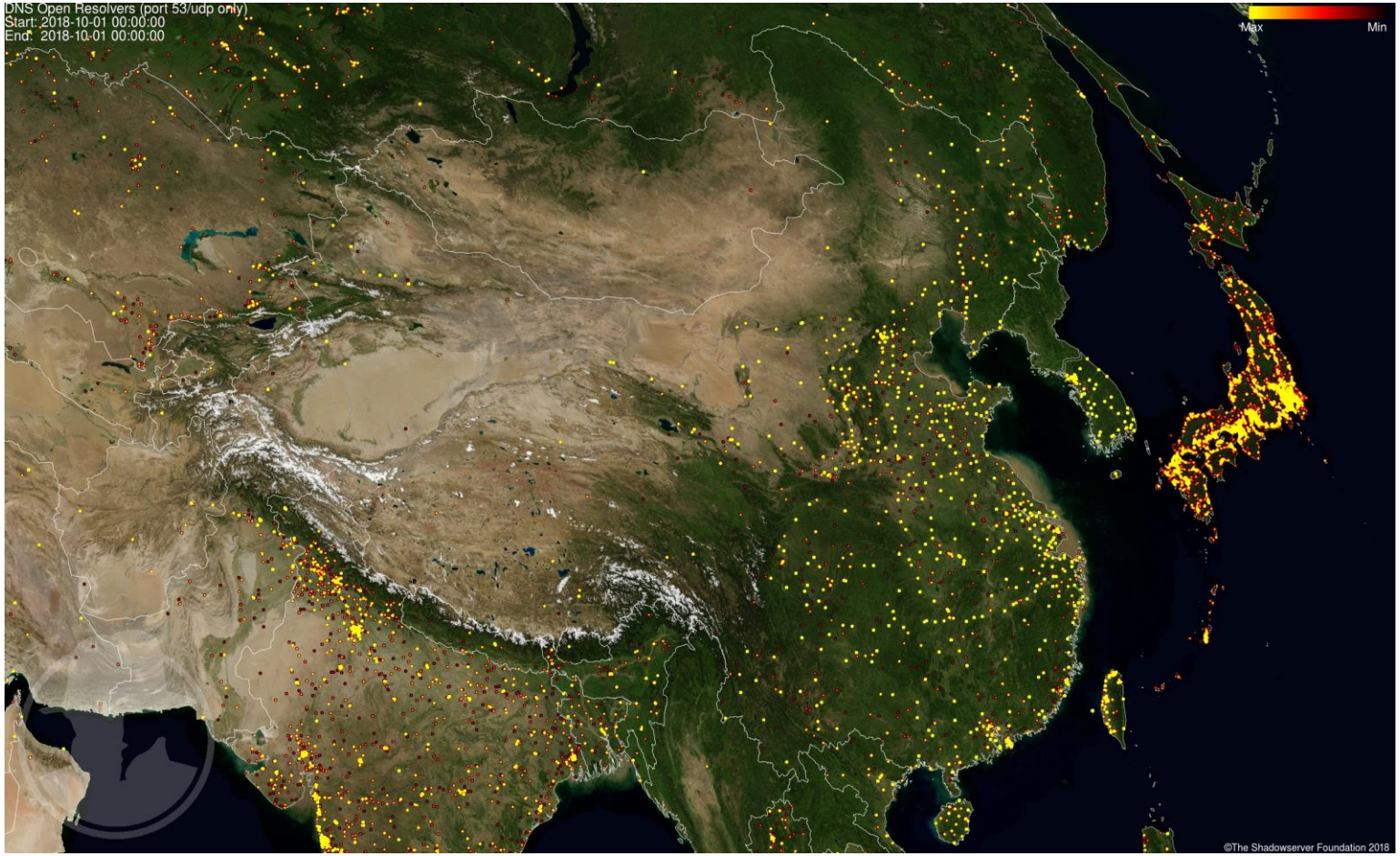
Problems with Borders

- May disrupt information flow & sharing
  - Speed
  - Bureaucracy
- Trust
  - (Fear) Risk of Sharing
- Consequences
  - Gaps between practice & capabilities (sectors / players. Economies
  - Isolate certain stakeholders
  - Basic security issues unresolved – recurring incidents
  - Affects success in other areas (i.e CyberCrime)

Open DNS Resolver

Top 20 Countries With Recursive DNS Servers

Country	Total
China	1,298,427
United States	315,027
Korea, Republic of	162,599
Russian Federation	141,194
Taiwan	115,570
Brazil	99,458
India	90,287
Poland	63,082
Turkey	62,349
Indonesia	60,138
Japan	41,352
Romania	38,009
Iran, Islamic Republic of	34,406
Bulgaria	31,983
Ukraine	29,476
Australia	28,431
Morocco	28,088
South Africa	27,695
Italy	27,054
France	26,662

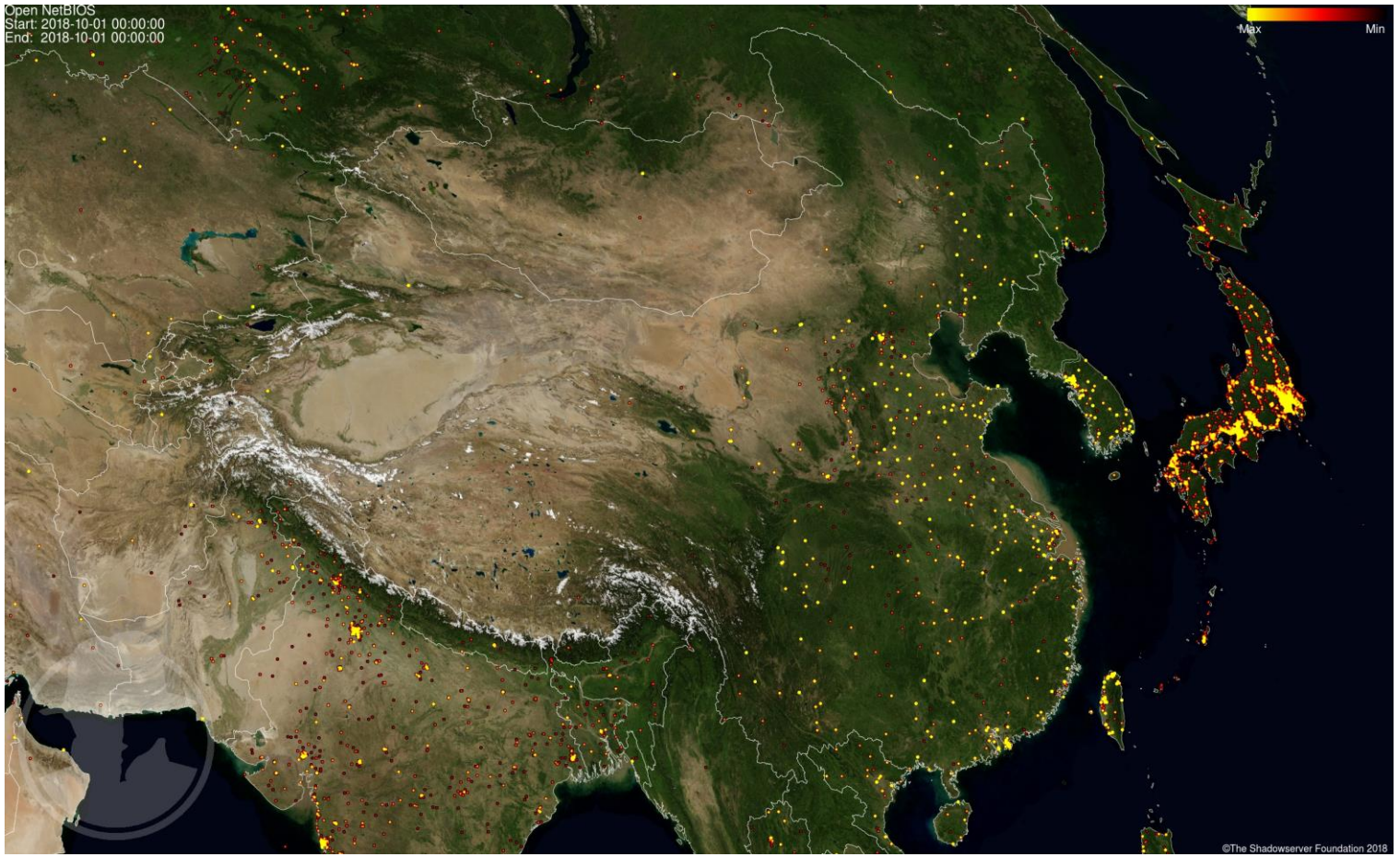


Shadowserver.org - https://dnsscan.shadowserver.org/open/openresolver_china_current.jpg

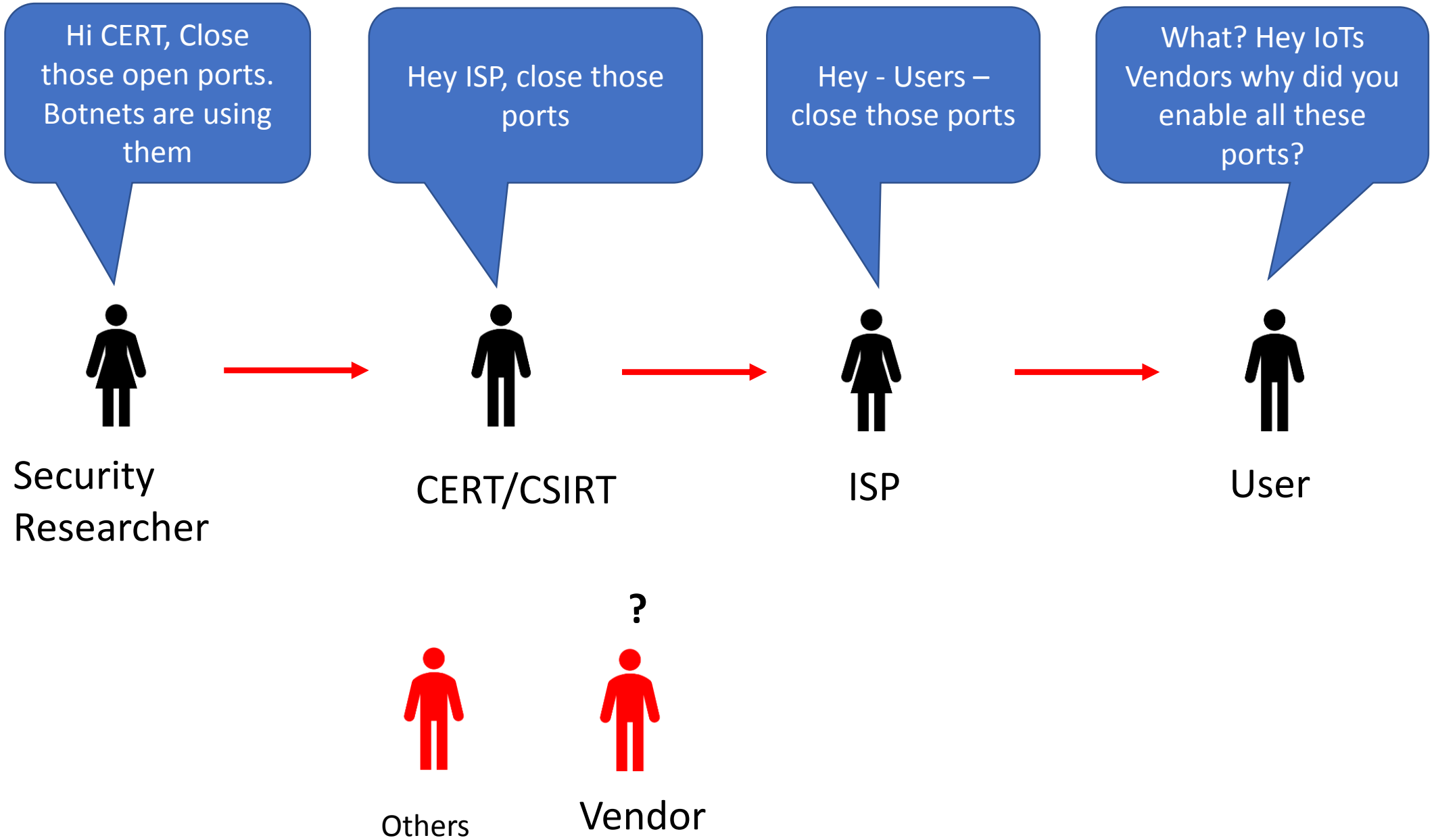
Open Netbios ports (UDP 137)

Top 20 Countries With Open NetBIOS

Country	Total
United States	128,220
China	73,115
Italy	58,383
Argentina	39,353
Brazil	37,046
France	34,738
Taiwan	33,809
Russian Federation	32,515
Korea, Republic of	31,368
Japan	23,999
Germany	22,950
United Kingdom	19,086
Hong Kong	18,749
Australia	17,917
Poland	17,844
Canada	13,903
Netherlands	13,050
Spain	11,228
Vietnam	9,581
Philippines	9,256



https://netbiosscan.shadowserver.org/all/netbios_china_current.jpg


Hi CERT, Close those open ports. Botnets are using them
Hey ISP, close those ports
Hey - Users – close those ports
What? Hey IoTs Vendors why did you enable all these ports?
Security Researcher
CERT/CSIRT
ISP
User
?
Others
Vendor

We Need to Fix This

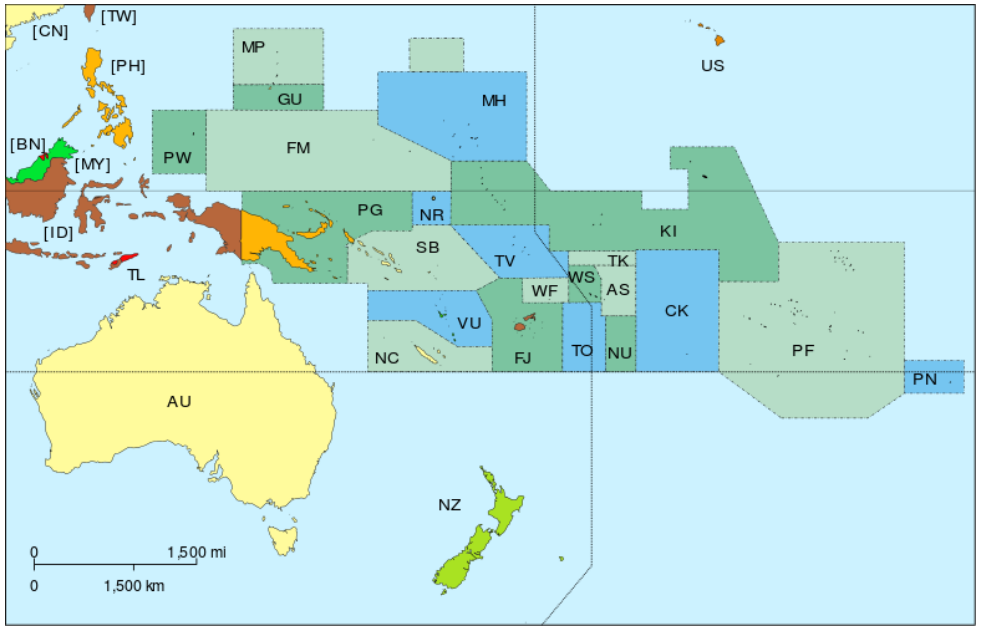
- We work well within our traditional “borders”
- What about
  - Inter-Communities
  - Inter-Sector
  - Inter-Governments
  - International
- Beyond Information Sharing
- Includes Problem Solving

Stories

CERT/CSIRT Establishment Project in the Pacific

Background

- PacCERT was established 2012 & ended in 2014
  - Constituents: 22 Pacific Island Economies
  - Based in Fiji (USP) – 2 staff
- Cyber Security activities were relatively low, not institutionalized, no coordination, no governance
- Good initiatives were not linked
- Lack of resources , many challenges
- Security threats becoming reality
- Opportunity to provide assistance



Opportunity for Collaboration & Assistance

- Capacity Development
  - 2016 – workshop in Tonga
  - 2016 - Tonga CERT Established
  - 2018 – PNG CERT, Vanuatu CERT
- Collaboration with APCERT, CERT Australia, DFAT, FIRST & others
  - 3 Regional CERT/CSIRT Workshops (2018 – 2019)
  - Site visits to CERT Australia, ThaiCERT
  - APCERT & FIRST Fellowship
  - PacSON established 2018
  - FIRST Fellowship for TongaCERT
  - ShadowSever Foundation & Team Cymru providing feeds
  - FIRST TC Event Noumea
  - Open source software

CSIRT Workshop Tonga

1st Regional CSIRT Training (Tonga)

Lessons Learned

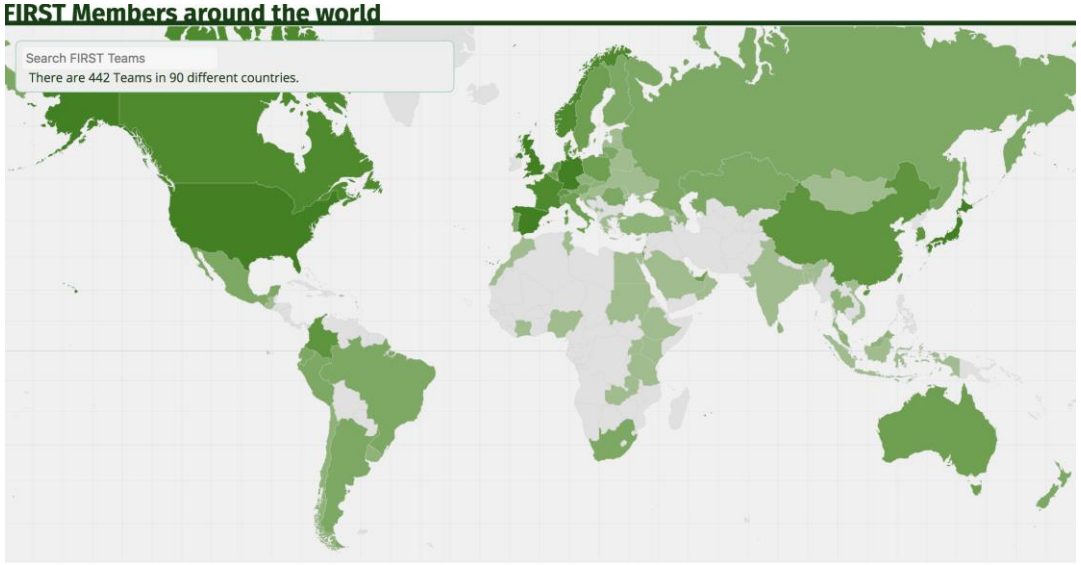
- Multi-stakeholder approach
  - Clarify
  - Complement vs Compete
- Big Picture
  - Set goals clearly & clarify
  - Start small and grow slowly
- There's no one right model
  - Context
  - Know options & adapt
  - CSIRT of the "Last Resort"
- Capacity Development
  - Learn from others
  - Support one another
  - Get Plugged-in-to the community
- Create a community

CERT Vanuatu Launch – 2018

2nd Regional CSIRT Workshop, New Caledonia

FIRST Fellowship Program

- Outreach to CERTs/CSIRTs in regions economies that are not (well) represented in the community
- Started in 2014
  - Renamed to Suguru Yamaguchi Fellowship Program
  - 13 Teams from Developing Economies
- Support newer teams
  - Participate in FIRST events
  - Support to become FIRST Member



CSIRT Training with AfricaCERT – 2017

Incident Handling for Policy Makers (and other stakeholder communities)

- To better understand
  - Issues and Challenges (i.e. GPDR, Trust)
  - What works and what doesn't work
  - Existing initiatives and efforts
- Hopefully
  - More frequent conversations
  - Policies that will improve & mature security practices
  - More resources for security related efforts
- Outcomes
  - Incident Handling for Policy Makers
  - Engagements at Internet Governance Forum, INTERPOL, GFCE, may other Forums

New York - 2018

Geneva - 2017

Conclusion

- Questions
  - Why is it difficult to do security?
  - What should we prioritize on?
  - What problems should be tackle first?
- Going beyond the “traditional border”
  - Strengthening everyone
  - Improving overall security
  - Solving problems
- Volunteering & Helping others
  - Mentoring
  - Open sourcing tools
  - Sharing your work & experience

Thank You!

Adli Wahid

adli@apnic.net

Twitter: @adliwahid