Pushing Coordinated Vulnerability Disclosure forward in Asia Pacific

JPCERT Coordination Center
Global CVD Project Lead
Tomo Ito

Today's presentation

- APCERT Coordinated Vulnerability Disclosure WG recently established
  - Introduction of the WG
    - Members, objectives, motivation..
  - Asia Pacific CVD challenges
  - Idea for the WG's future structure
- Ask your opinions on the WG's future structure & activities

On CVD

CVD and its situation today

- Coordinated Vulnerability Disclosure (CVD)
  - Gathering, coordinating, and disclosing of vulnerability information
  - It is a global good practice
  - Often many different stakeholders are involved in CVD cases (MPCVD)
  - Vulnerability information flows through global product supply chain
  - MPCVD complexity = Supply chain complexity
- The importance of CVD increasing

CVD and its situation today

- Coordinated Vulnerability Disclosure (CVD)
  - Gathering, coordinating, and disclosing of vulnerability information
  - It is a **global** good practice
  - Often many different stakeholders are involved in CVD cases (MPCVD)
  - Vulnerability information flows through **global** product supply chain
  - MPCVD complexity = Supply chain complexity
- The importance of CVD increasing

For JPCERT/CC…

- Important factors of CVD
  - Information is reached to appropriate stakeholders
  - Mitigation is created before vulnerability is disclosed
  - Vul information is disclosed at an appropriate timing
  - Fix is applied
- The purpose of CVD is to reduce risks to the users, developers and the society

CVD Global Situation

In the US…

- CERT/CC the very first CVD Coordinator organization
- CISA actively tackling supply chain issues, including CVD & CVE
- Vendors high CVD maturity overall
- …many more

In the EU…

- NCSC-NL, NCSC-FI, etc. experienced in CVD
- ENISA & regional CSIRTs setting up CVD structure
- High maturity vendors
- Cyber Resilience act
  - VDP requirement for PDE manufactures..

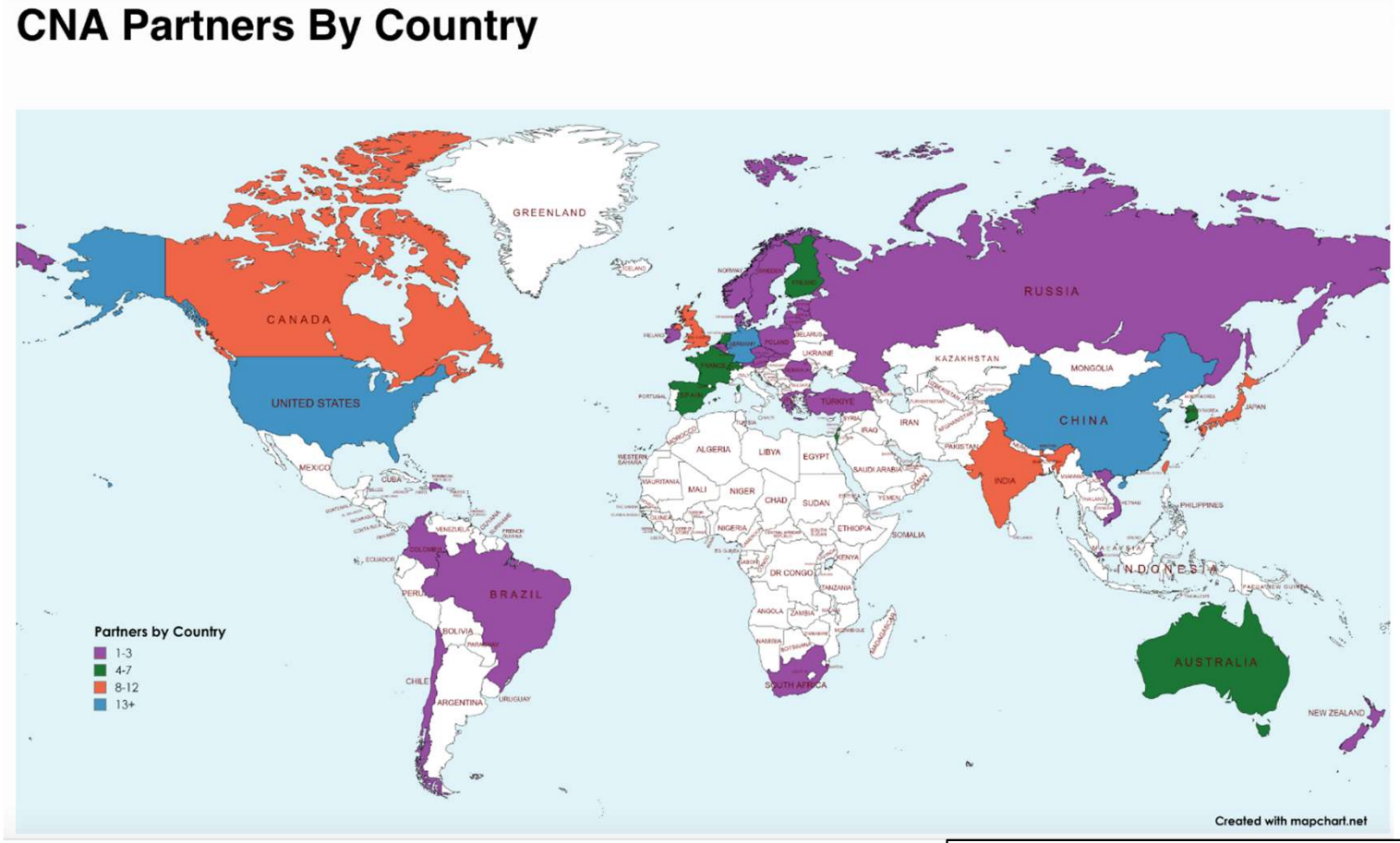
Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities. A coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Given the fact that information

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

In Asia-Pacific…

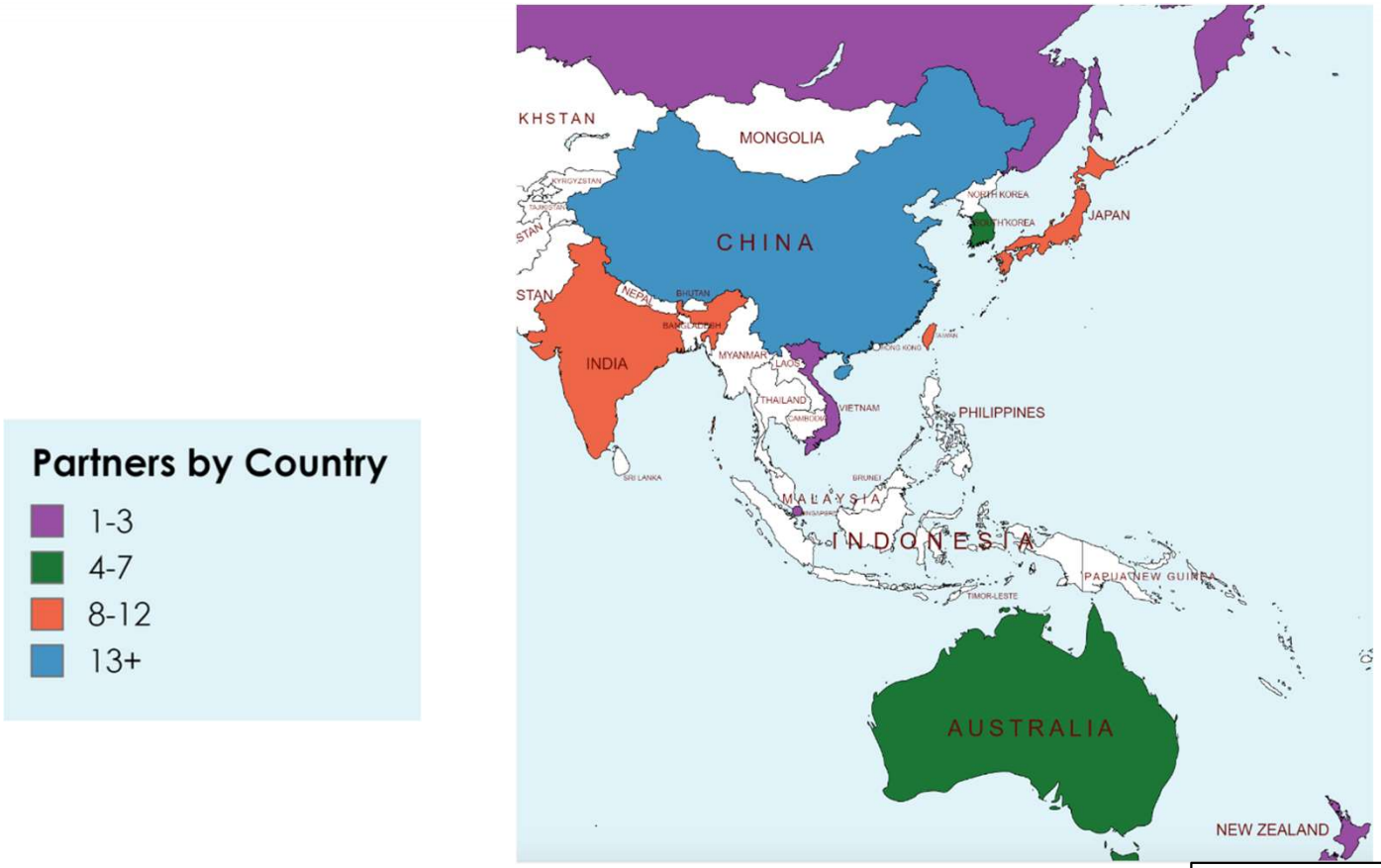
- Many product/component suppliers exist
- CVD readiness level is low overall
- CNA adoption spaces left
- There has not been any ongoing CVD collaborative framework in Asia Pacific region

CNA partners around the world



CVE - CNA Partners By Country
https://www.cve.org/ProgramOrganization/CNAs

CNA partners situation in Asia Pacific



CVE - CNA Partners By Country
https://www.cve.org/ProgramOrganization/CNAs

Since CVD is global…

- Global cooperation is a must
- Recently a Coordinator organization in Asia Pacific helped JPCERT/CC find a product supplier in their area
  - It was found that the company was closed
  - Very helpful - Hard to confirm things from different part of the world
- Have seen many cases where the CVD cases fail due to cultural/language gaps between different regions or stakeholders

APCERT CVD WG

Motivation for CVD WG creation

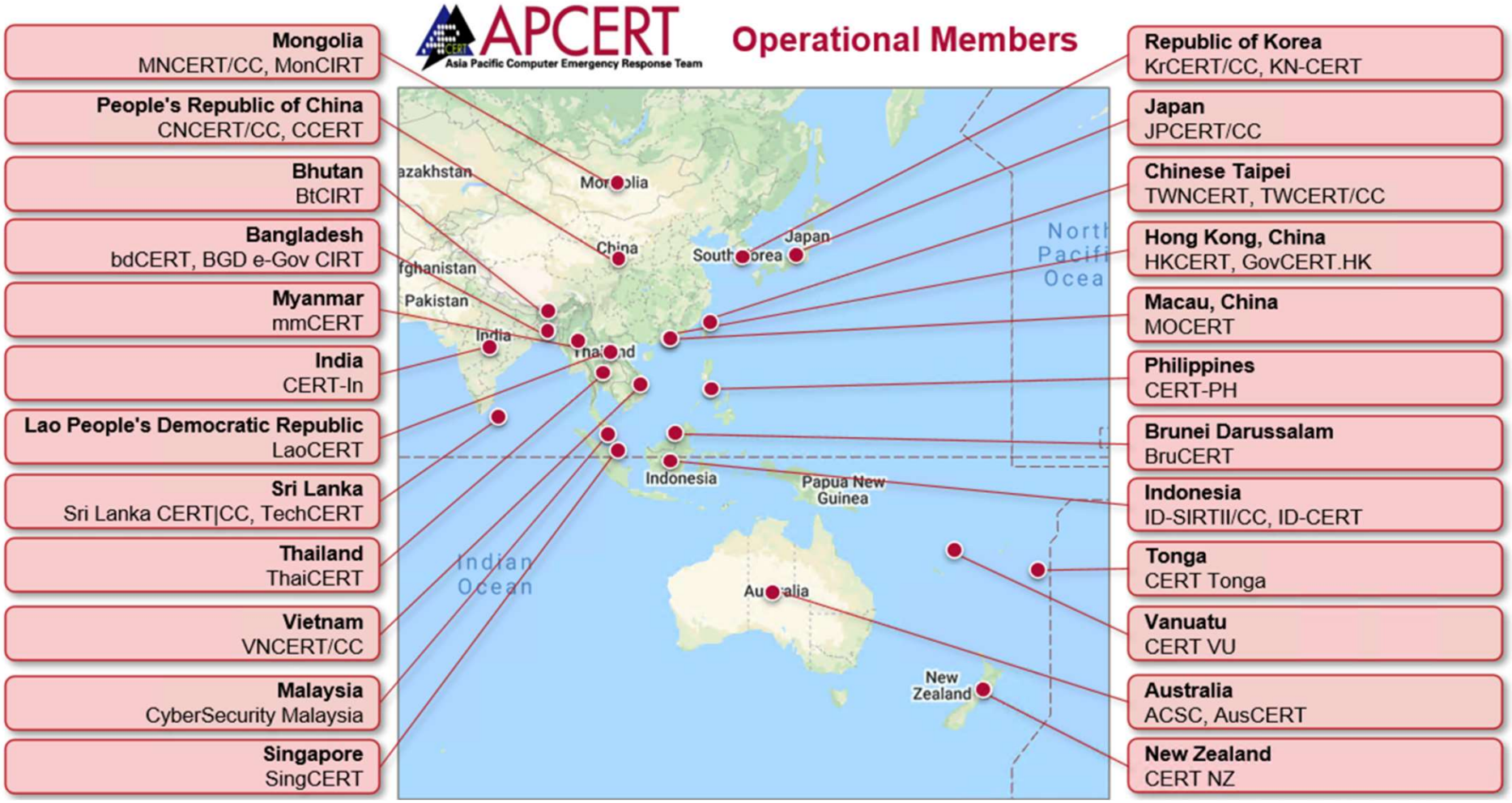
- JPCERT/CC is CVD coordinator, CVE Numbering Authority (CNA) and Root
  - Multi-party coordination (MPCVD) occurs frequently and collaboration among different stakeholders is a must
  - There has not been any ongoing CVD collaborative framework in the Asia Pacific
  - Interdependent world – many products/Components come from the region
  - CVD/CVE adoption spaces left
  - Need for CVE discussions/cooperation/adoption as Asia Pacific

CVD WG in APCERT

APCERT

APCERT
https://www.apcert.org/

APCERT Operational Members list



APCERT CVD WG Starting members

- 6 Asia Pacific CSIRT/Coordinator organizations:
  - CERT-In
  - KrCERT/CC
  - TWCERT/CC
  - Cybersecurity Malaysia
  - AusCERT
  - JPCERT/CC

APCERT CVD WG objectives

- Enhance AP regional and international cooperation
- Jointly develop capacity to deal with global CVD challenges
- Facilitate knowledge and experience sharing/exchange within the WG participants and APCERT members as a whole
- Assist other CERTs in AP region and around the world
- Find solutions to overcome challenges encountered while carrying out CVD/CVE activities
- Develop a cooperative framework for CVD activities, including vulnerability reporting, mitigation and disclosure

Planned activities

- Quarterly meetings
- Presentations of each member's CVD activities/interests
  - Document outputs
- Find Asia Pacific CVD challenges
- Create Asia Pacific cooperative CVD framework

WG situation

- We are starting to
  - Get to know each other
  - Share knowledge and learn from each other
- Then Later, plans to
  - Create a cooperative CVD framework as Asia Pacific
  - …and contribute to the global CVD ecosystem

Asia Pacific Challenges

Asia Pacific CVD Challenges spotted thus far

1. Being “Latecomers”
2. CVD weighs more on “government”
3. Low maturity level

1. Being “Latecomers”

- As a regional movement, we are latecomers
  - Some experienced, some just starting
- Early adaptors move ahead of laws/regulations
  - The latecomers reference the trials of the early adaptors
- Often laws & regulations are created by latecomers without enough experiences

2. CVD weighs more on government

- CVD = Good practice
  - More “cultural” than “regulations”
- Government agency leading CVD - CVD more treated as “the government work”
  - Can affect the motivation and maturity level of private companies in both positive and negative way
  - Government-set CVD framework in Japan - Close relationships with the vendors but risks of stakeholders being framework-dependent exist (less “spontaneous”)

2. CVD weighs more on government

- Often unclear of multiple things
  - Who is doing what on CVD?
  - How will the information be treated?
  - Who will the information be shared with?
  - Detachment from the expecting common CVD practice?
  - Laws/regulations – is it safe to contact them?
  - Will these change all of a sudden?
- Such uncleanses/doubts cause motivational loss of external parties

3. Low maturity level

- Matured PSIRTs/security teams/CNAs exist in the region, but in general the level is low
- Lacking CVD readiness (VDP…)
- CVE/CNA adoption spaces left
- Wide gaps between matured and unmatured
  - Wide gap between government/CERT and private organizations in some regions

Things can be connected and complicated

- Latecomers creating “matured” framework referencing the early adaptors works without much experience

  → May result in widening of the gap between matured and unmatured (even more)

- No simple/perfect answer for existing issues

If we can contribute to these…

- Important factors of CVD
  - Information is reached to appropriate stakeholders
  - Mitigation is created before vulnerability is disclosed
  - Vul information is disclosed at an appropriate timing
  - Fix is applied
- The purpose of CVD is [illegible]educe risks to the users, developers and the soc[illegible]

How can we contribute?

The WG works and the future

- Different organizations, different reasons
- Discussions, consensus building of what a good CVD is a must
- Take necessary actions
  - CVD/CVE Development
    - Raise CVD maturity level
    - Create CNAs
  - Create a cooperative framework
    - Coordinate MPCVD

How could the WG function in the future to contribute to the ecosystem?

Key elements to consider

- CVD as good practice
  - In Asia pacific, CVD tends to be more government-led
- “Clearness”
  - Who is doing what on CVD?
  - How will the information be treated?
  - Who will the information be shared with?
  - Detachment from the expecting common CVD practice?
  - Laws/regulations – is it safe to contact them?
- Stability
  - Will these change all of a sudden?

In other words

- More-region-specific CVD
  - Just make things harder
  - …and such circumstances do not matter to them
- Unclearness
  - Causes confusions
  - blocks communication/information flow
- Instability
  - Takes away the predictability and motivations

No one wants troubles

To secure.. Asia Pacific CVD supporting team

- If necessary, act as..
  - Translator
    - Overcoming cultural/language barriers
  - Balancer/mediator
  - Safe harbor
  - Point-of-Contact of the Asia Pacific
- Risk & trouble absorber
  - beyond regional circumstances
- Harmonized with the global ecosystem
- Often CERT's job, but not everyone/every time

Your input is appreciated

On Asia Pacific CVD Supporting Team

- WG Becoming the the region's CVD supporter is a big possibility
- Absorbing risks/problems & balancing: our strong motivation
- WG just started – more inputs at this point is very valuable
- Action item idea to make this happen is truly appreciated

Awareness raising

- To tackle different challenges, getting people involved/motivated is a must
- One good way is to conduct awareness-raising activities
  - Different image of CVD between stakeholders
  - Efficient and balanced messaging is essential
- Any awareness raising activities that worked?
  - Success story or important factors
    - Government or CERT to the public?
    - Inside your organization?
    - CVE Program to CNA prospects?

Summary

Summary

- APCERT CVD WG activities started
  - Discussions, consensus building of “good CVD”
  - Cooperative framework building
  - Idea of Asia Pacific CVD Supporting Team
- Your opinions are always welcome (especially at this early stage)

tomotaka.itou@jpcert.or.jp

Thank you!