Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Second Intersessional Consultation

Panel: International Cooperation

Chris Gibson
CEO/Executive Director

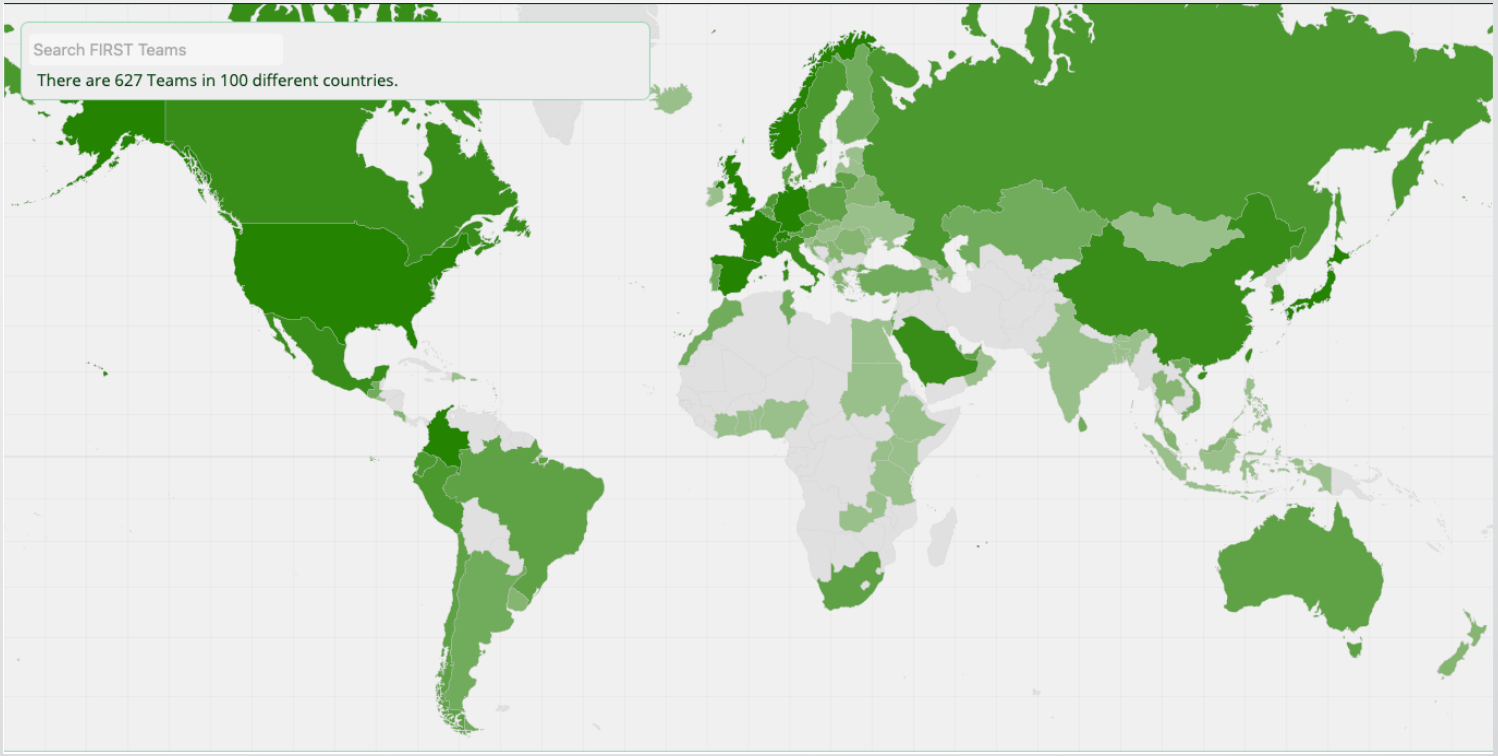
Monday, 13th June 2022

FIRST?

- FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents.
- FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

- FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all.
  - Global Coordination - You can always find the team and information you need.
  - Global Language - Incident responders around the world speak the same language and understand each other's intents and methods.
  - Policy and Governance - Make sure others understand what we do and enable us rather than limit us.

Global Membership



Context

- FIRST is a global, inclusive and, primarily, technical organisation
- FIRST believes that malicious activities should be resolved through an appropriate law enforcement process
  - Improving this, through activities such as this Ad Hoc Committee, is enormously important
- FIRST, as mentioned already, is fueled by trust
  - Trust both with constituents and partners
- Incident Responders are likened to firefighters or medical staff
  - Cyber norms
    - “Norm 11 (UNGGE 2015 report, paragraph 13k) – States should not conduct or knowingly support activity to harm the information systems of another State’s authorized emergency response teams (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity”

Incident Response / Cybercrime

- IR are often the first people to recognize that a cybercrime affecting ICT systems and ICT enabled infrastructure has been committed
  - Discovery is also often a decision point
    - Recover system/process?
    - Pursue LE process?
- IR resources limited
- International cooperation is vital

FIRST Position

- We seek to establish clarity on roles & responsibilities
- We believe:
  - CSIRTS should neither be merged nor confused with Law Enforcement
  - CSIRTS should not be responsible for attribution or prosecution
- Should either of these occur it will significantly affect the trust between teams and their constituents.

FIRST Activities

- Policy and Governance - Make sure others understand what we do and enable us rather than limit us.
- Law Enforcement Special Interest Group
  - To bring together CSIRTs and Law Enforcement
    - Understand each other's roles & responsibilities
    - Develop training
- Information sharing and other standards
  - CVSS
  - EPSS
  - TLP