The Forum of Incident Response and Security Teams (FIRST)

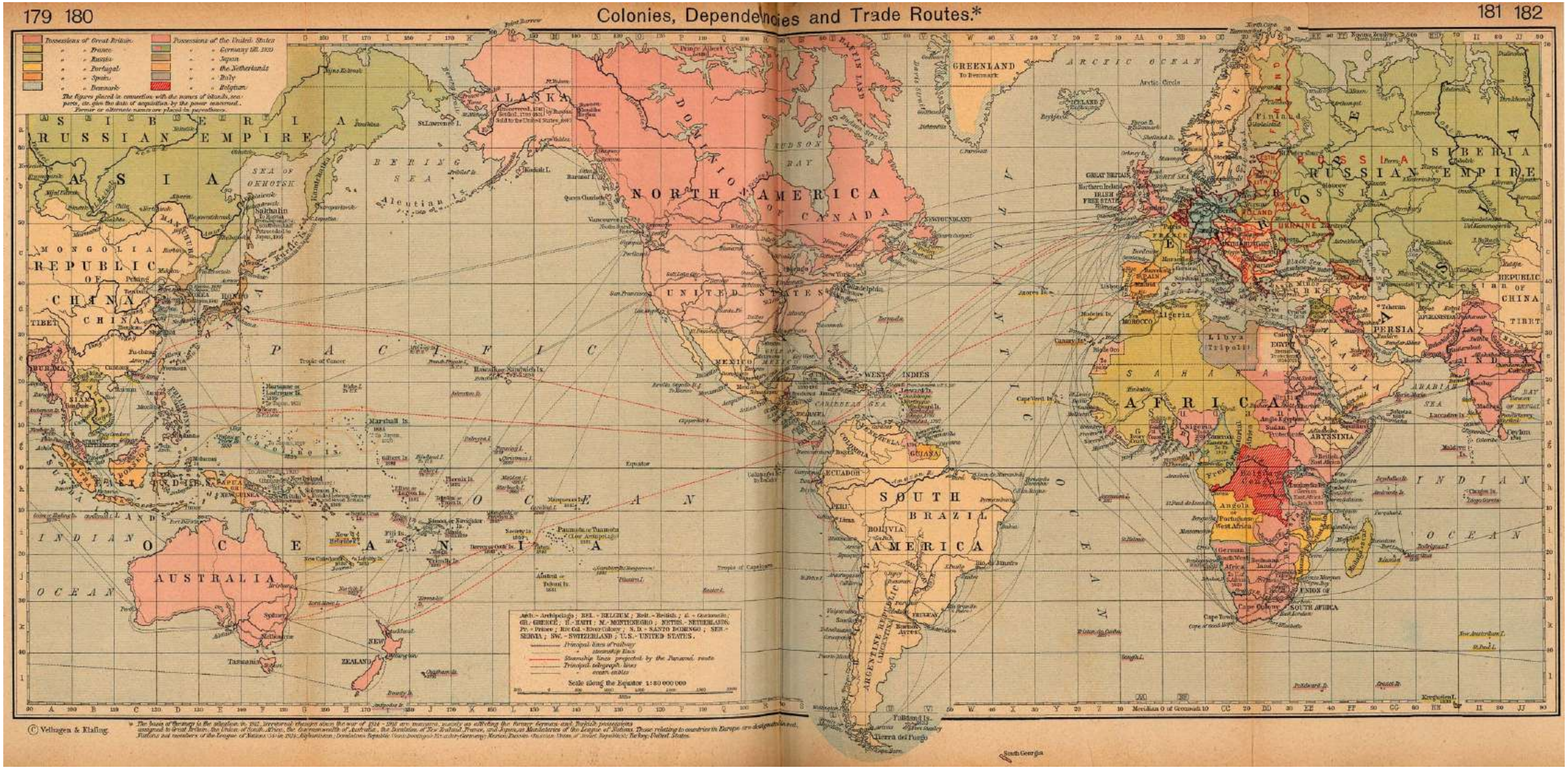
Dr. Serge Droz
Chair, Board of Directors
serge.droz@first.org

Agenda

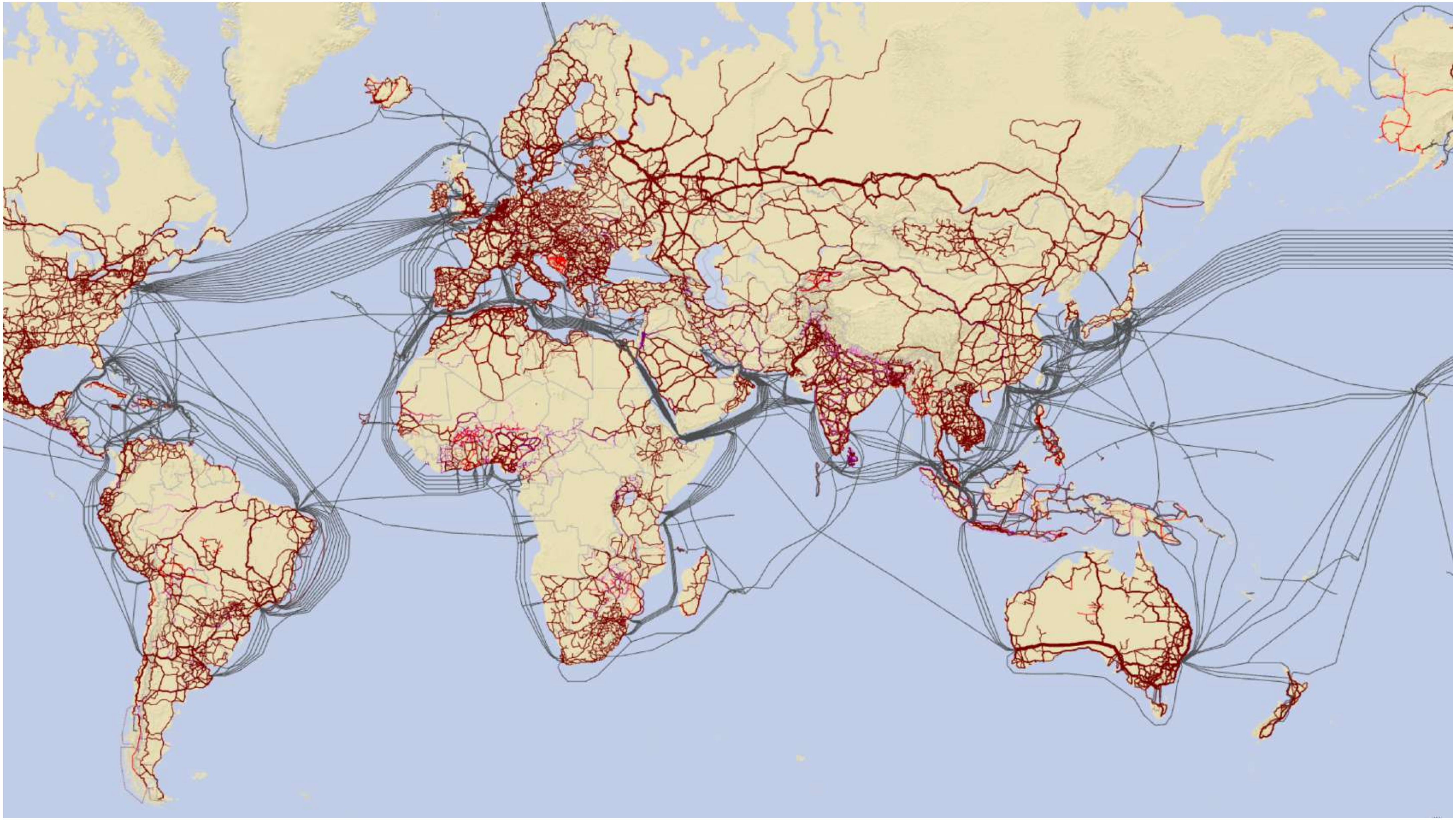
- What we want
- Introduction to FIRST
- Overview of projects and initiatives
- FIRST in 2020
- Questions and Answers

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK



Historical map of trade routes, Library of the University of Texas at Austin



State of Cyberspace

Access to knowledge

Collaboration

Prosperity

State of Cyberspace

Threats

Criminals

States

Disinformation

Hate

Surveillance

Remedies

Norms

Education

Incident Response

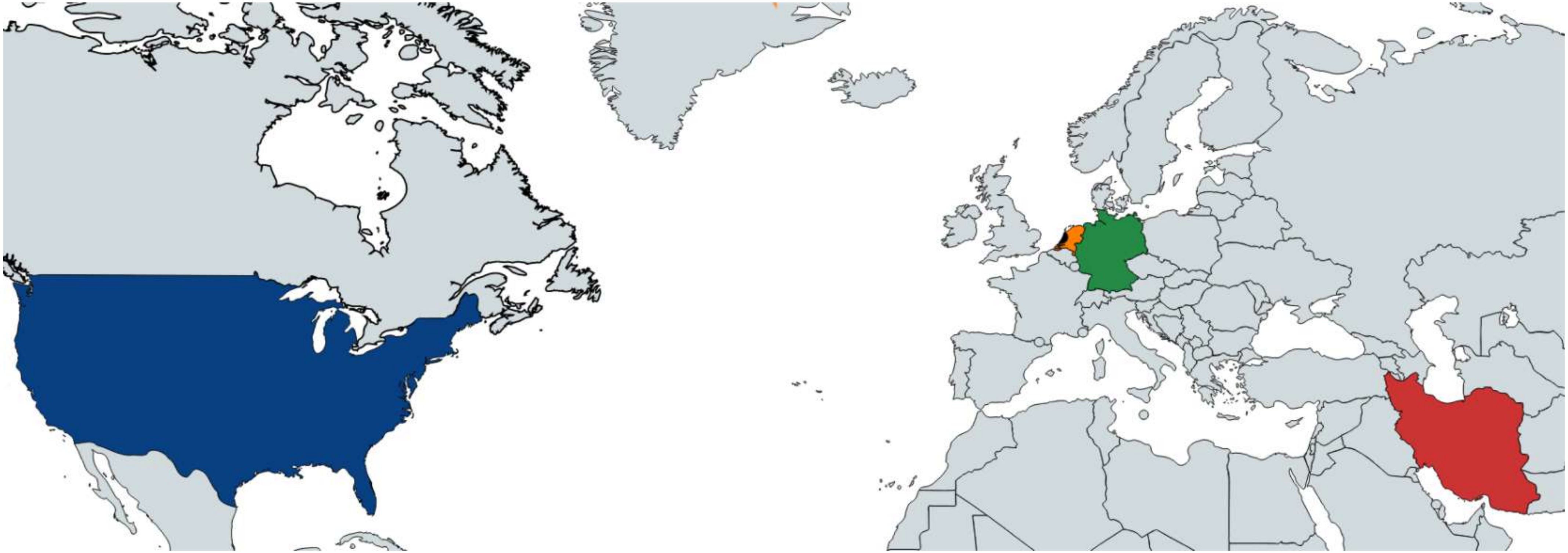
Remedies

Norms

GGE 2015

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized **emergency response teams** (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Incidents are global



Diginotar: National Crisis in NL, Discovered by Iranian User, Reported by Germany, dependance on US, Victims in Iran

Trust inhibitors

- **Hidden Agendas**
- **Placing the CERT in the wrong spot**
- **Sanctions**

Trust inhibitors: Wrong spot

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. **A State should not use authorized emergency response teams to engage in malicious international activity**.

Trust inhibitors: Sanctions

FIRST

Who are we?

- Association of Incident Response and Security Teams
- Founded in 1989

- We enable incident responders
    - To **engage with their peers**
    - To have a **shared understanding** of security problems
    - By developing **technologies and standards**
    - By foster an **environment conductive to their work**

FIRST’s Mission

Global Coordination: In an emergency you can always find the teams you need to support you in our global community.

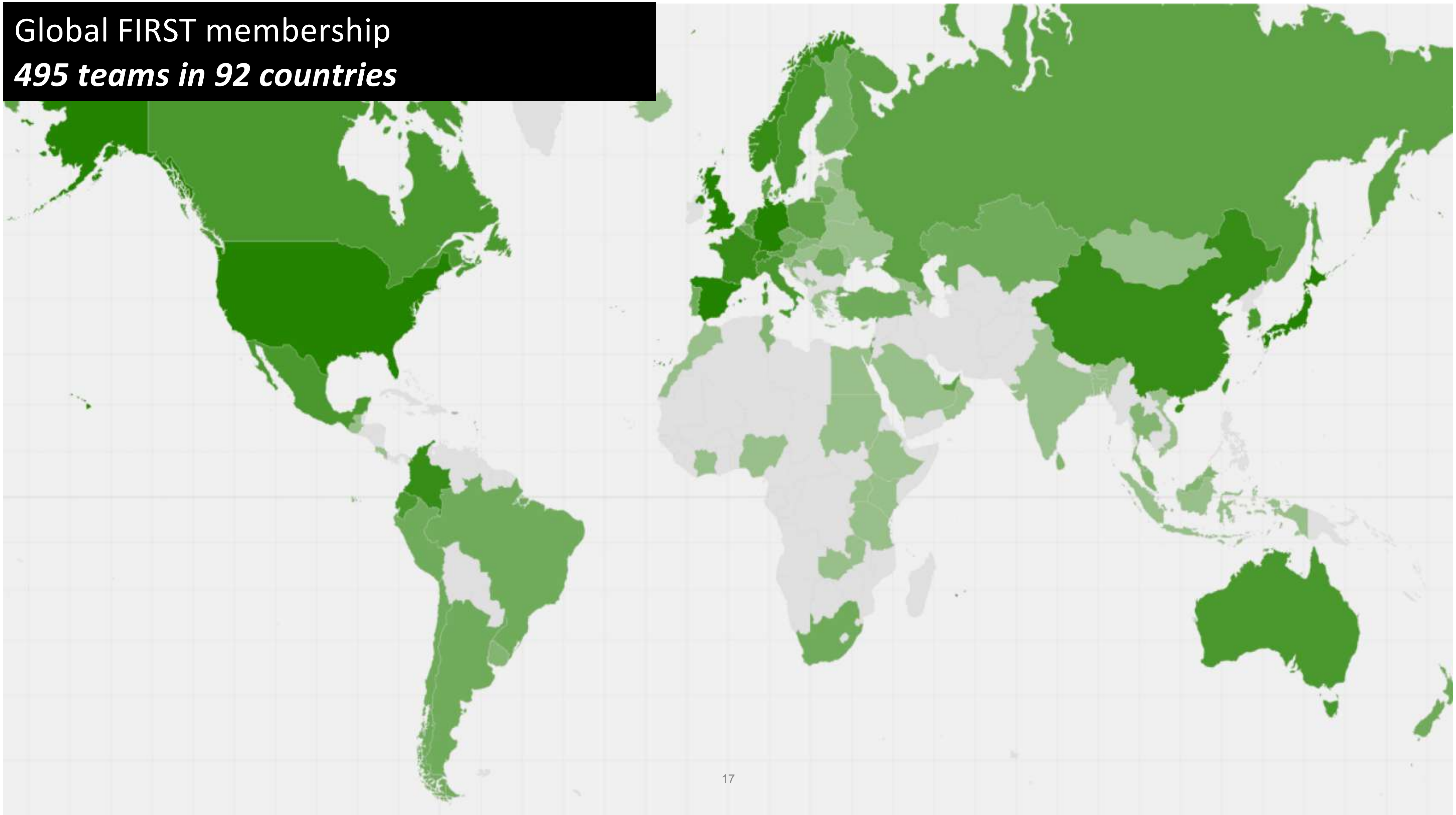
Global Language: Incident responders around the world speak the same language and understand each other’s intents and methods.

Automation: Let machines do the boring calculations, so humans can focus on the hard questions.

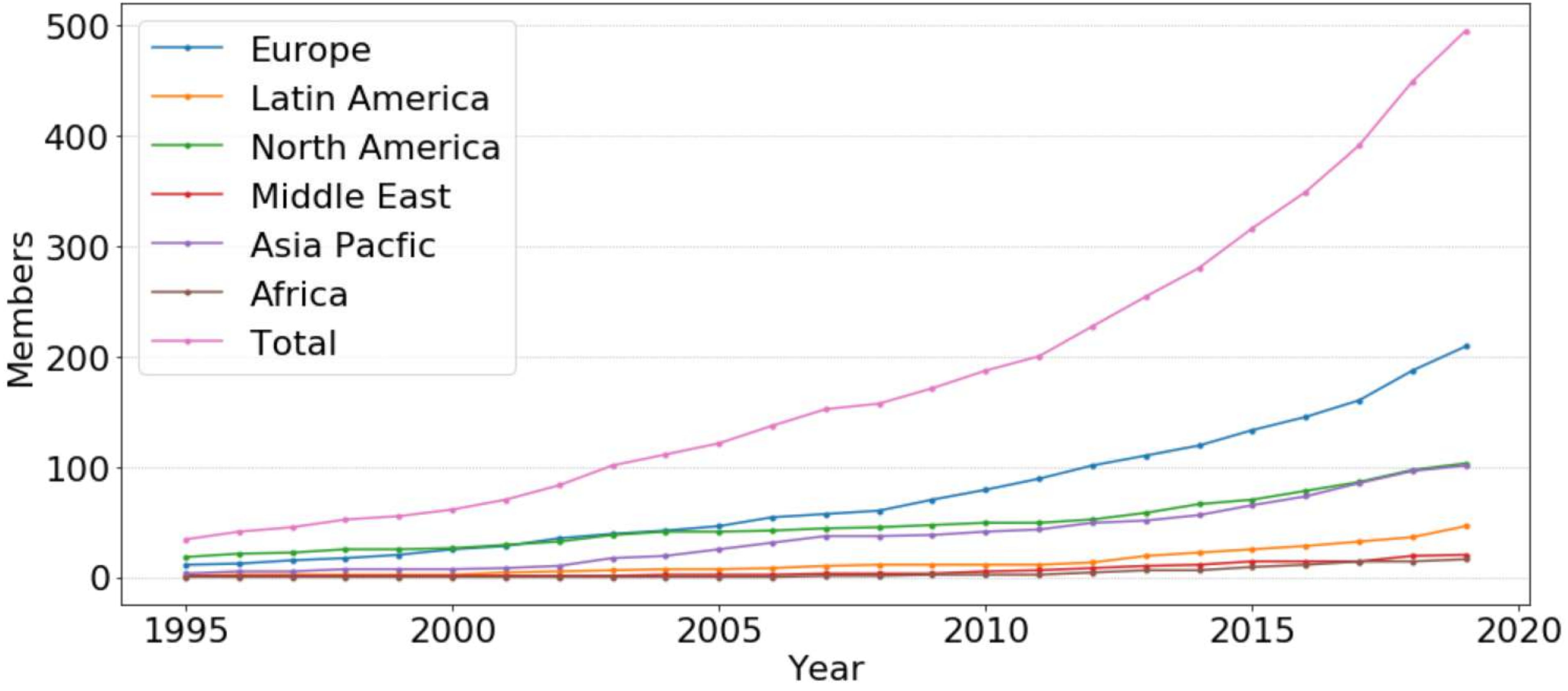
Policy and Governance: Make sure others understand what we do, and enable us rather than limit us.

Global FIRST membership

495 teams in 92 countries

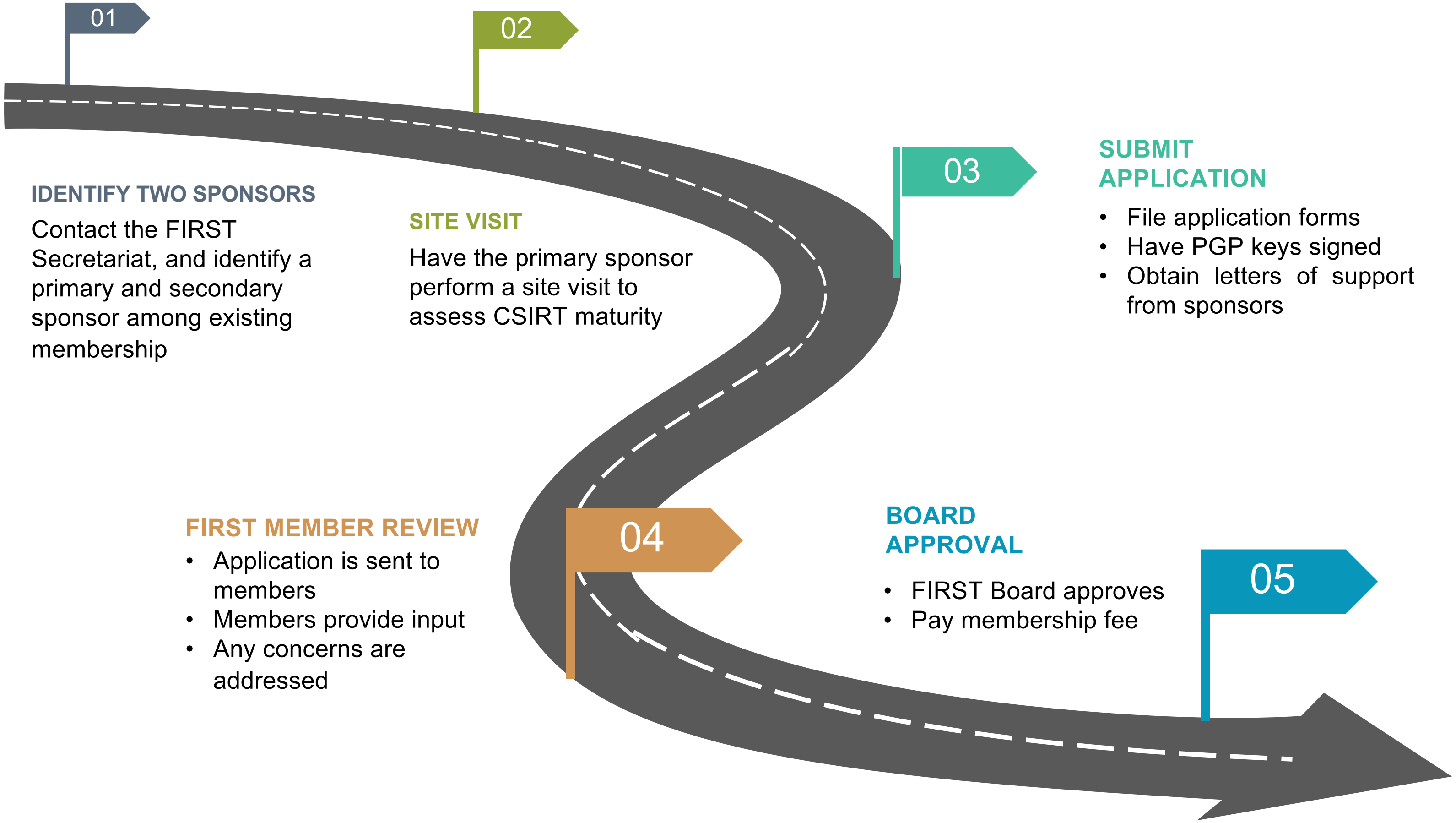


Membership



Europe
Latin America
North America
Middle East
Asia Pacfic
Africa
Total
Members
500
400
300
200
100
0
1995
2000
2005
2010
2015
2020
Year

Membership application process



IDENTIFY TWO SPONSORS

Contact the FIRST Secretariat, and identify a primary and secondary sponsor among existing membership

SITE VISIT

Have the primary sponsor perform a site visit to assess CSIRT maturity

SUBMIT APPLICATION

- File application forms
- Have PGP keys signed
- Obtain letters of support from sponsors

FIRST MEMBER REVIEW

- Application is sent to members
- Members provide input
- Any concerns are addressed

BOARD APPROVAL

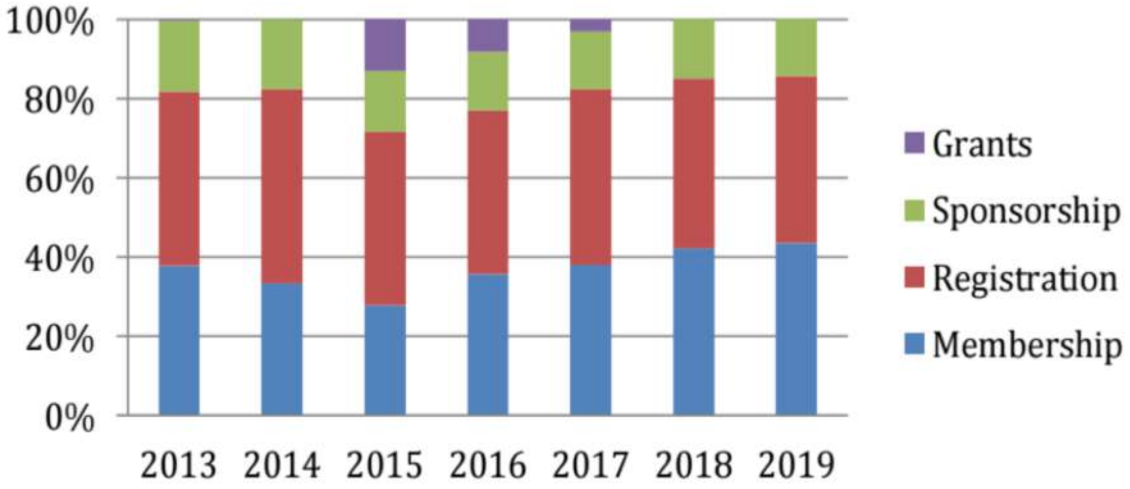
- FIRST Board approves
- Pay membership fee

Fellowship Program

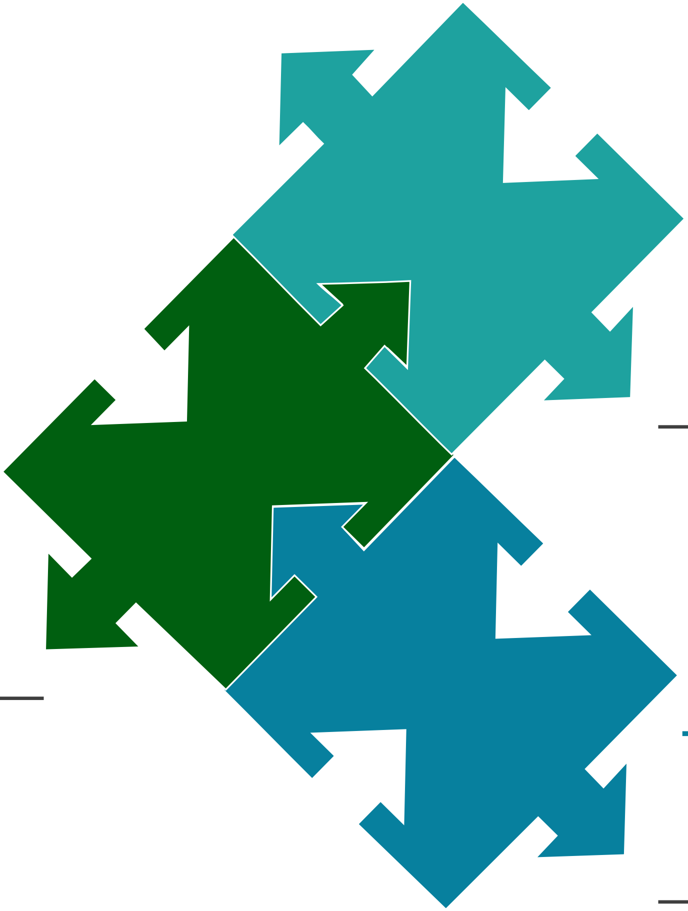
- FIRST **funds participation** for up to four new teams each year
- Open to CSIRTs with some **level of national responsibility**

FIRST as an organisation

- Lead by a 10-person **Board of Directors**, elected by Members
- No headquarters, but **secretariat** in Chicago
- **501c3 non-profit** incorporated in the United States
- Funded primarily through membership and conference fees



Events



Symposia

- Four per year
- In each major region (Africa, Europe, Latin America, Asia)
- Hosted by FIRST and often a partner

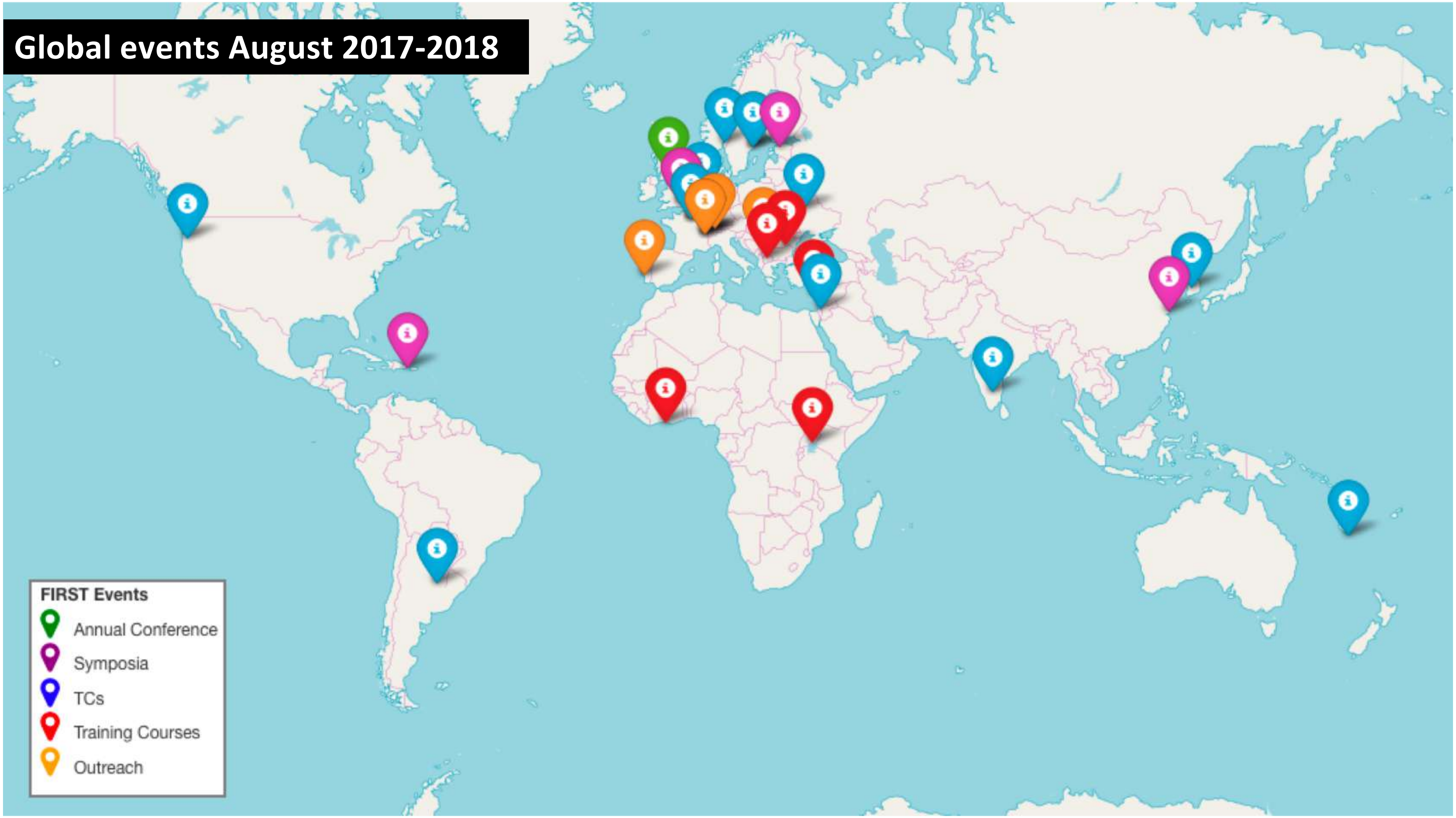
Conference

- Flagship event
- Once per year, travels between regions
- ~500-800 attendees

Technical Colloquium

- Organized by individual members
- National or regional event
- Typically 10-15 events per year

Global events August 2017-2018



Training and Education

- FIRST maintains a **CSIRT and PSIRT Services Framework**
  - Details all services typically offered by CSIRT
  - Offers a roadmap and guide for CSIRT as they expand capability
- FIRST **develops training materials** for individual services
  - CSIRT Fundamentals, Incident Coordination, Information Sources
  - All materials are Creative Commons licensed and available for free
- FIRST **delivers training** with partners and at events
  - Roster of trainer-practitioners

Special Interest Groups

- Convene members around topics of common interest
- Often have a formal charter, timeline and deliverables

- Types of SIGs:
  - **Working groups:** Big Data, Ethics, Red Team
  - **Standards groups:** CVSS, IEP, TLP, Passive DNS exchange
  - **Discussion groups:** Vendors, Metrics, Industrial Control Systems
  - **Bird of a Feather session:** legal issues, specific temporary topics

Standards

Common Vulnerability Scoring System

- Scoring system for software vulnerabilities
- Allows integration of environmental factors
- Interactive training

Traffic Light Protocol

- Allows data senders to encode how information may be distributed
- Focused on human sharing, simple to use

TLP

IEP

Information Exchange Protocol

- More fine grained specification of **Handling**, **Action**, **Sharing** and **Licensing** policies
- Focused on machine sharing (JSON)

Passive DNS

- Enable easier sharing of passive DNS information
- Standard contributed to the IETF

Passive DNS

Technical resources

Membership database

A FIRST member database with contact information for incident responders at other members. **Including PGP keys.**

FIRST Incident Response Team API

Poll information on other members using a **public API**.

Malware Information Sharing Platform

Share machine-parseable incident descriptions with members using the **MISP platform**.

Mailing lists and IRC

Immediate communications channels with other FIRST members.

Internet Governance and Policy

- Be a **trusted security expert** to the policy community
- FIRST regularly participates in policy forums, such as the Internet Governance Forum, Global Conference on Cyberspace to educate policy makers on incident response
- Lead experts to the **IGF Best Practices Forum on Cybersecurity**
- Help **develop technology expertise** and capability

Partners

Partners share our vision of a strong incident response community

OIC-CERT
Computer Emergency Response Team
ITU
ORGANIZATION OF AMERICAN STATES
OAS
More rights for more people
GÉANT
GFCE
Global Forum on Cyber Expertise
lacnic
ICT for peace foundation
APNIC

Marc-Olivier Jodoin

FIRST Annual Conference 2020

Program this morning

Time	Talk	Presenter
9:00	Welcome	Serge Droz
9:30	Remediation Ballet: Choreographing your team to victory	Simon Freiberg and Jason Solomon (Google)
10:30	Integrating red teaming and CSIRT	Jordi Aguilà (e-la Caixa CSIRT, ES)
11:00	Coffee break	
11:15	A Field Guide to communicating a security incident	Izzi Lithgow (CERT NZ)
12:00	DFIR Acquisition presentation	Sam Bonanno (ACSC)
12:30	Lunch	

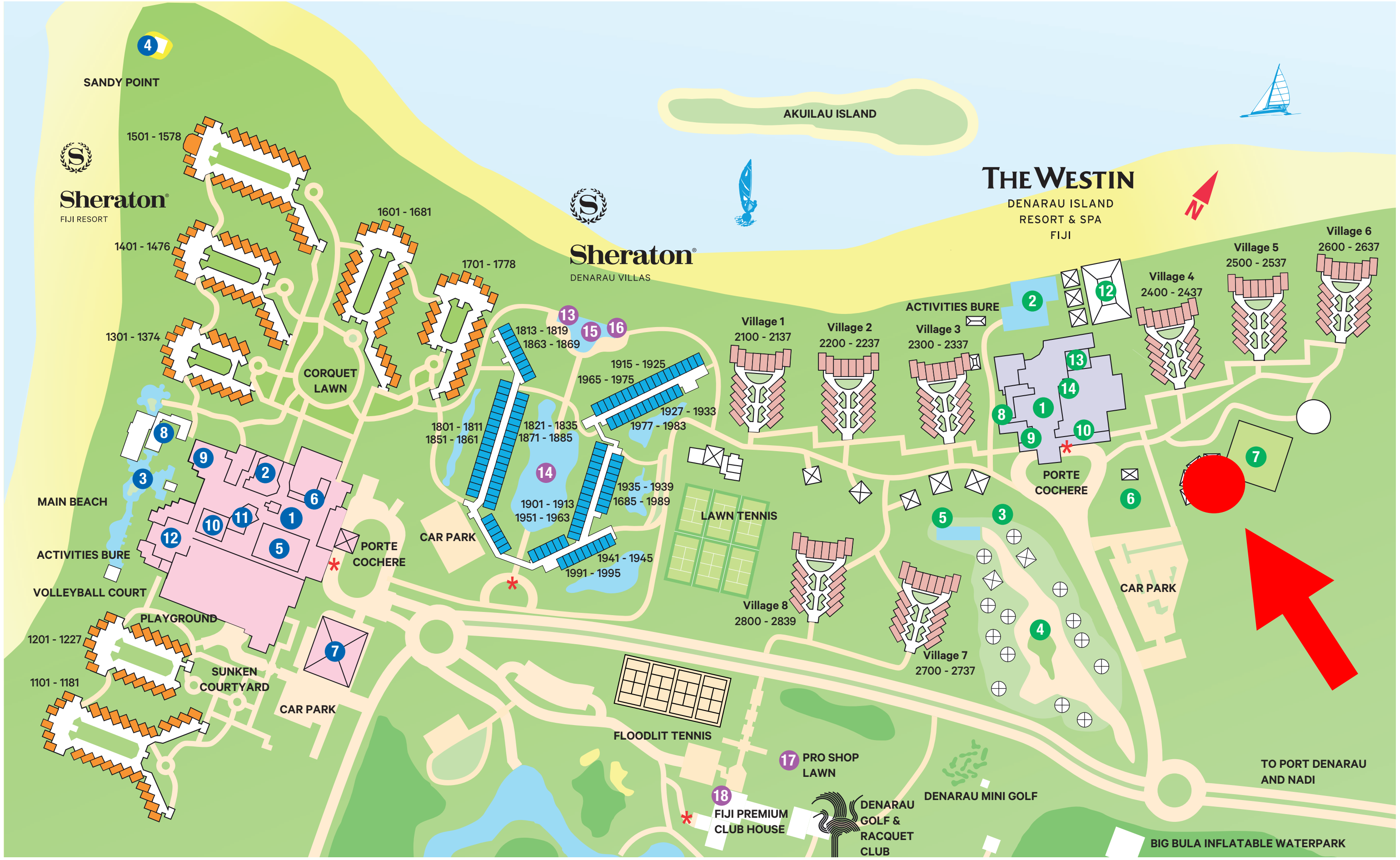
Program this afternoon

Time	Talk	Presenter
13:45	The Policy Implications of Incident Response	Maarten Van Horenbeeck (Zendesk), Serge Droz (OS-CERT)
14:45	IR using Jupyter Notebooks	Serge Droz (OS-CERT)
15:15	Coffee Break	
15:30	Measuring CSIRT Maturity using SIM3	Maarten Van Horenbeeck (Zendesk)
16:00	Responding to Incidents in Industrial Environments	Hinne Hettema (Port of Auckland, NZ)
17:00	Closing remarks	Serge Droz (OS-CERT)
19:00	Networking reception - Sandy Court @ Westin Denarau Fiji Resort	

And our training days

Wednesday, November 6th 2019	Thursday, November 7th 2019
Breach workshop 1: Cyber Extortion Adli Abdul Wahid (APCERT) Frangipani (Ballroom B)	CSIRT Basic Training - Part 1 Maarten Van Horenbeeck (Zendesk) Frangipani (Ballroom B)
Breach workshop 2: Critical Infrastructure Attack Serge Droz (OS-CERT) Gardenia (Ballroom C)	CSIRT Advanced Training - Part 2 Serge Droz (OS-CERT) Adli Wahid (APNIC) Gardenia (Ballroom C)
Malware Analysis When You’re in A Hurry Hinne Hettema (Port of Auckland) Frangipani (Ballroom B)	CSIRT Basic Training - Part 1 Maarten Van Horenbeeck (Zendesk) Frangipani (Ballroom B)
CSIRT Advanced Training - Part 1 Serge Droz (OS-CERT) Adli Wahid (APNIC) Gardenia (Ballroom C)	CSIRT Advanced Training - Part 3 Serge Droz (OS-CERT) Adli Wahid (APNIC) Gardenia (Ballroom C)

Reception



Coco

Palms

7-9pm

This could be the beginning …

FIRST™

Improving Security Together

PaCSON

PACIFIC CYBER SECURITY OPERATIONAL NETWORK

Questions?

first-sec@first.org
https://www.first.org