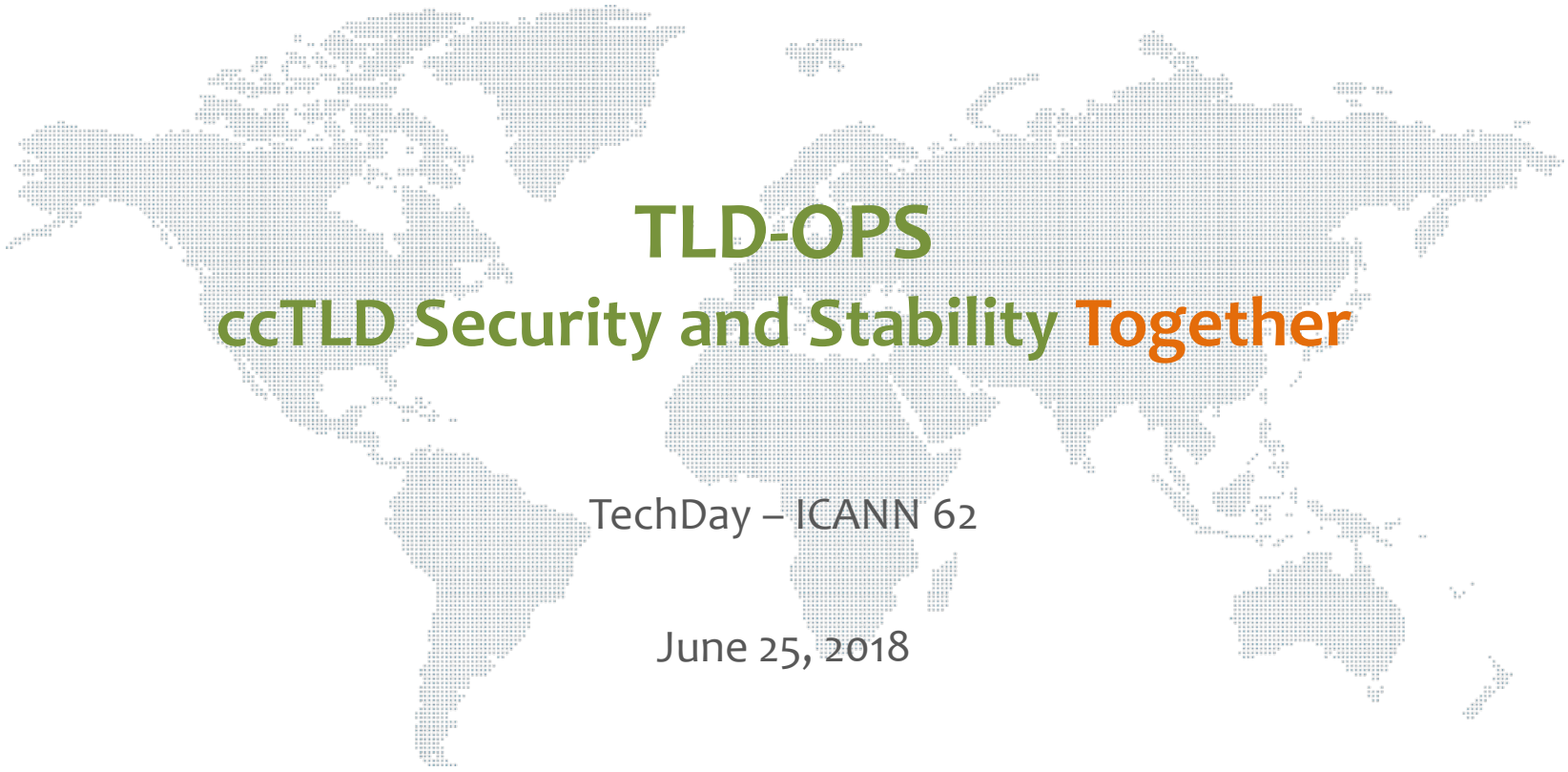


TLD-OPS
ccTLD Security and Stability Together

TechDay – ICANN 62

June 25, 2018

ICANN 62 POLICY FORUM
PANAMA CITY
25–28 June 2018

ccNSO

ICANN

TLD-OPS, what is it ?

- Global technical incident response community *for and by ccTLDs*, open to *all* ccTLDs.
- Brings together 345+ people who are responsible for the operational security and stability of 193 different ccTLDs.
- Goal: enable ccTLD operators to collaboratively detect and mitigate incidents that may affect the operational security and stability of ccTLD services and of the wider Internet.
- Further *extends* members' existing incident response structures, processes, and tools and *does not* replace them.
- Guidance by TLD-OPS Standing Committee
  - ccTLD reps and Liaisons (SSAC, IANA, ICANN's security team)

Together, we are stronger

- Open and global incident response community for and by ccTLDs
- Builds on standard mailing list (192 ccTLDs, 345+ subscribers, 99 ccTLDs missing)
- Enhances local incident response facilities, not a replacement
- Increases everyone's reachability and security awareness
  - Everyone has everyone else's contact info in their inbox, even offline
  - Exchange security alerts and queries (DDoS attacks, phishing, etc.)
  - Learn from each other
- Easy to join (through IANA Admin Contact)

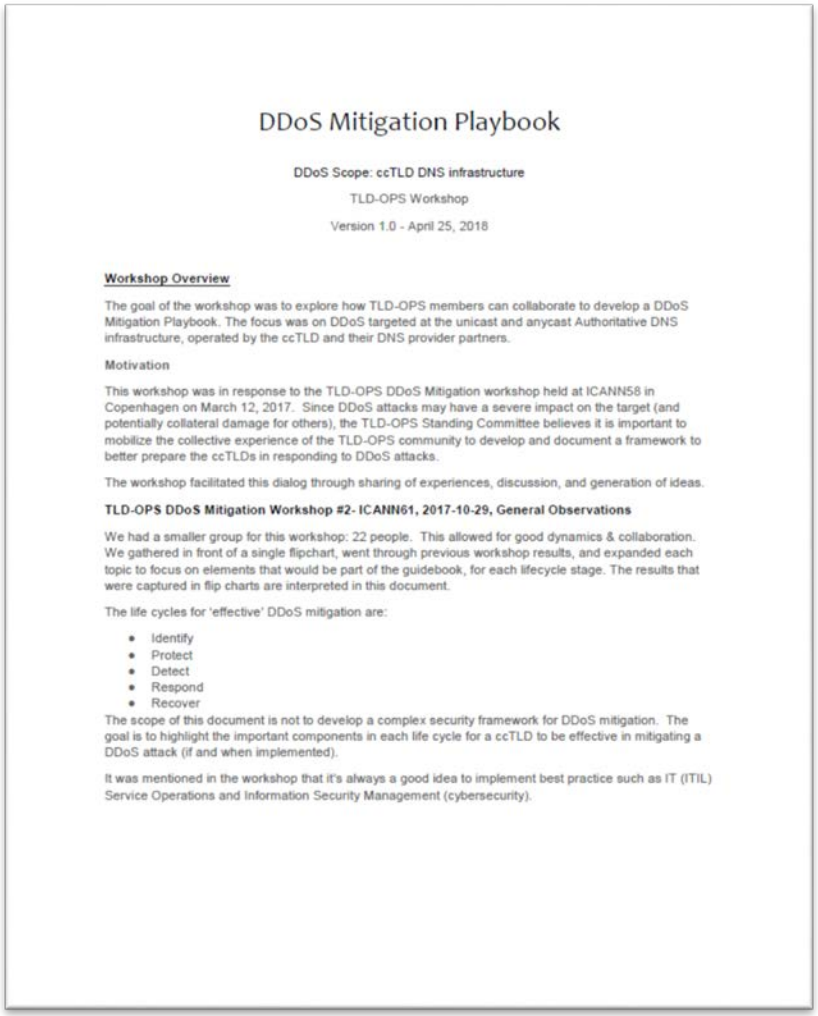
Together, we create value for the community

New tools for
the community

ccNSO ICANN

A first delivery : the DDOS Mitigation Playbook

- The goal of the first workshop was to explore how TLD-OPS members can collaborate to detect and mitigate DDOS attack
- Two sessions took place during ICANN Mettings 58 and 60 to share experiences, discussions and generation of ideas.
- The topic has approched from multiple persepctives, such as technical, operational, compliance and strategic.



DDoS Mitigation Playbook

DDoS Scope: ccTLD DNS infrastructure

TLD-OPS Workshop

Version 1.0 - April 25, 2018

Workshop Overview

The goal of the workshop was to explore how TLD-OPS members can collaborate to develop a DDoS Mitigation Playbook. The focus was on DDoS targeted at the unicast and anycast Authoritative DNS infrastructure, operated by the ccTLD and their DNS provider partners.

Motivation

This workshop was in response to the TLD-OPS DDoS Mitigation workshop held at ICANN58 in Copenhagen on March 12, 2017. Since DDoS attacks may have a severe impact on the target (and potentially collateral damage for others), the TLD-OPS Standing Committee believes it is important to mobilize the collective experience of the TLD-OPS community to develop and document a framework to better prepare the ccTLDs in responding to DDoS attacks.

The workshop facilitated this dialog through sharing of experiences, discussion, and generation of ideas.

TLD-OPS DDoS Mitigation Workshop #2- ICANN61, 2017-10-29, General Observations

We had a smaller group for this workshop: 22 people. This allowed for good dynamics & collaboration. We gathered in front of a single flipchart, went through previous workshop results, and expanded each topic to focus on elements that would be part of the guidebook, for each lifecycle stage. The results that were captured in flip charts are interpreted in this document.

The life cycles for 'effective' DDoS mitigation are:

- Identify
- Protect
- Detect
- Respond
- Recover

The scope of this document is not to develop a complex security framework for DDoS mitigation. The goal is to highlight the important components in each life cycle for a ccTLD to be effective in mitigating a DDoS attack (if and when implemented).

It was mentioned in the workshop that it's always a good idea to implement best practice such as IT (ITIL) Service Operations and Information Security Management (cybersecurity).

ccNSO ICANN

What's next?
Natural Disasters – DR/BCP Readiness

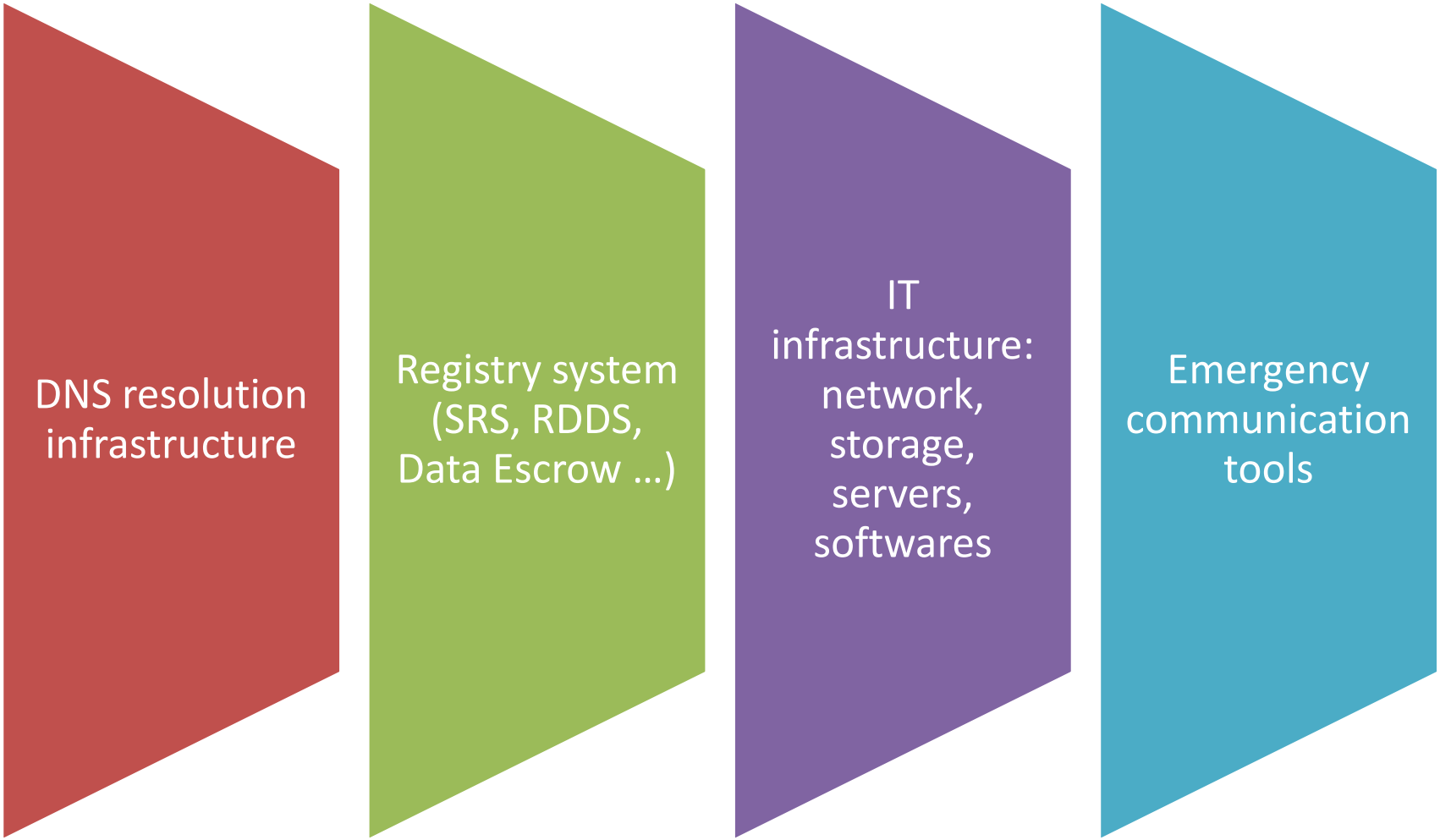
- Expand to general Disaster Recovery and Business Continuity Planning
  - Request from community following natural disasters
  - BCP is many things to many people
  - Where to start?
  - Where to focus?
  - Past Experience?

- Technical continuity plans for the DNS, Registry and corporate systems

- The Business part focuses on plans, initiation, testing, critical even, communications, simulation

ccNSO ICANN

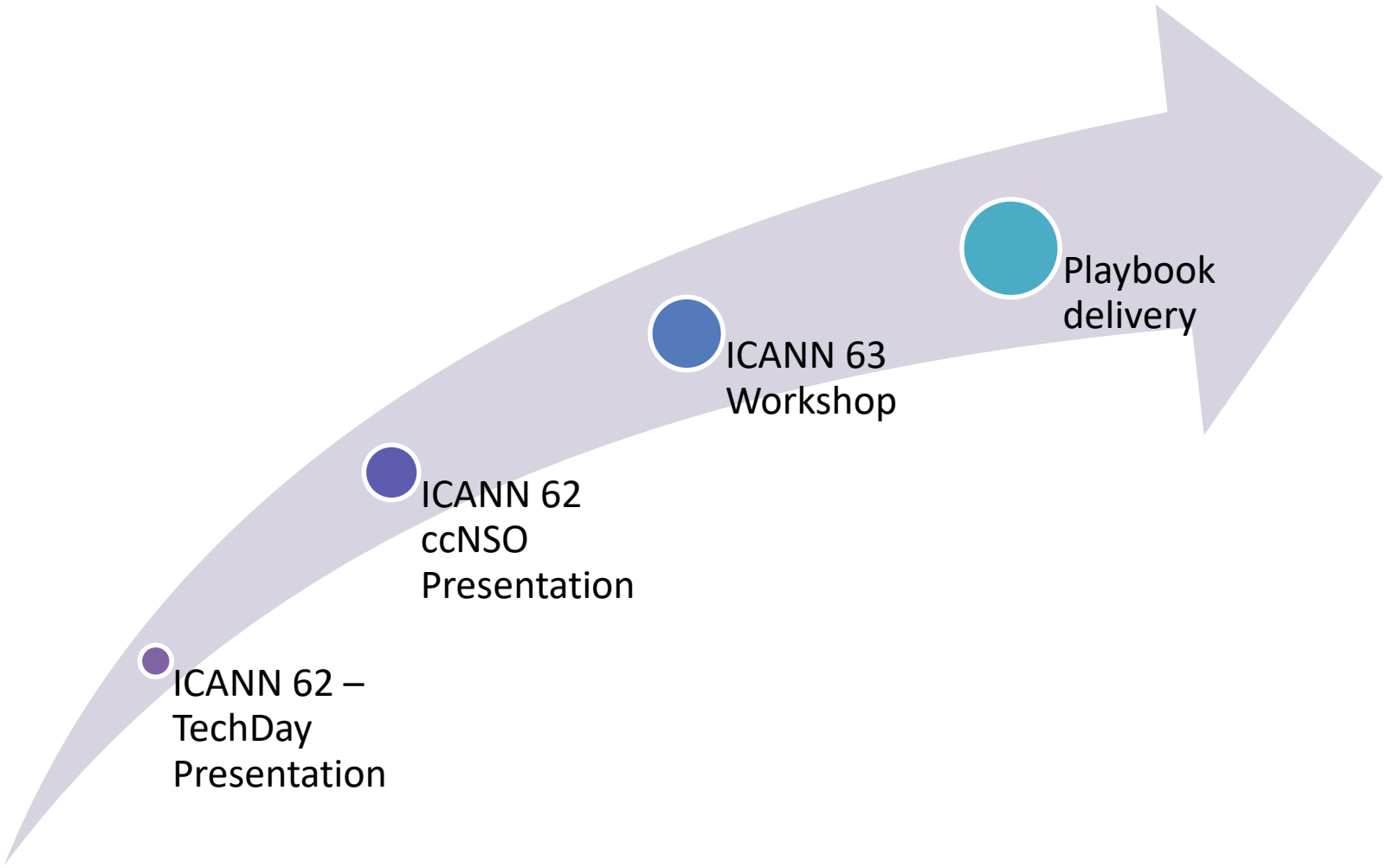
Focus for the TLD-OPS community



Feedback from the communauty

- What does the community needs ? A playbook with advises, a synthesis of feedbacks …
- Past experience from the ccTLDs
- Different type of actions depending on the geographical area
- Presentation of different types of technical continuity plans

Tentative action plan



Q&A

TLD-OPS Standing Committee
Frederico Neves, .br
Jacques Latour, .ca (chair)
Erwin Lansing, .dk
Régis Massé, .fr
Ali Hadji Mmadi, .km
Abibu Ntahigiye, .tz
Brett Carr, .uk
Warren Kumari (SSAC contact)
John Crain (ICANN's security team contact)
Kim Davies (IANA contact)

ICANN Staff
Kim Carlson

TLD-OPS Home
http://ccnso.icann.org/resources/tld-ops-secure-communication.htm

TLD-OPS Leaflet
https://ccnso.icann.org/en/workinggroups/tld-ops-enhanced-incident-response-capabilities-cctlds-27nov17-en.pdf
Arabic, Chinese, French, Russian, Spanish

Contact
Jacques Latour
Standing Committee Chair
+1.613.291.1619
jacques.latour@cira.ca