TLD-OPS
ccTLD Security and Stability Together

ccNSO – ICANN 62

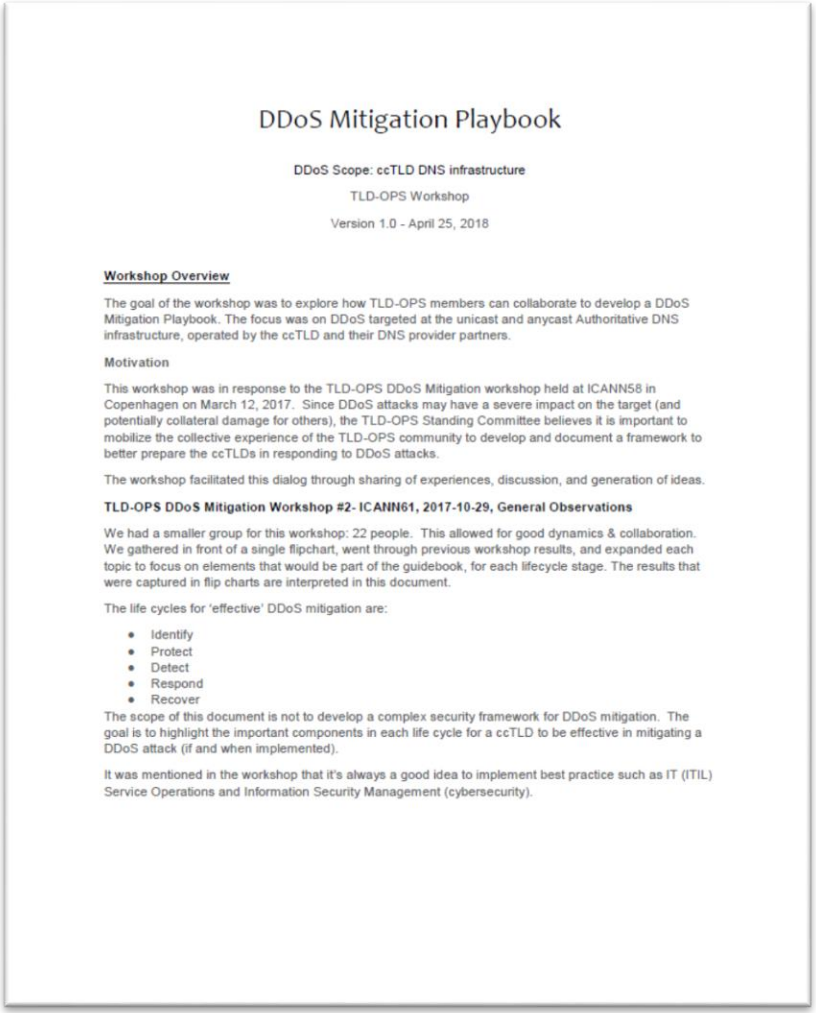
June 27, 2018

ICANN 62 POLICY FORUM
PANAMA CITY
25–28 June 2018

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 Meetings 58 and 60 to share experiences, discussions and generation of ideas.
- The topic has approached from multiple perspectives, 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

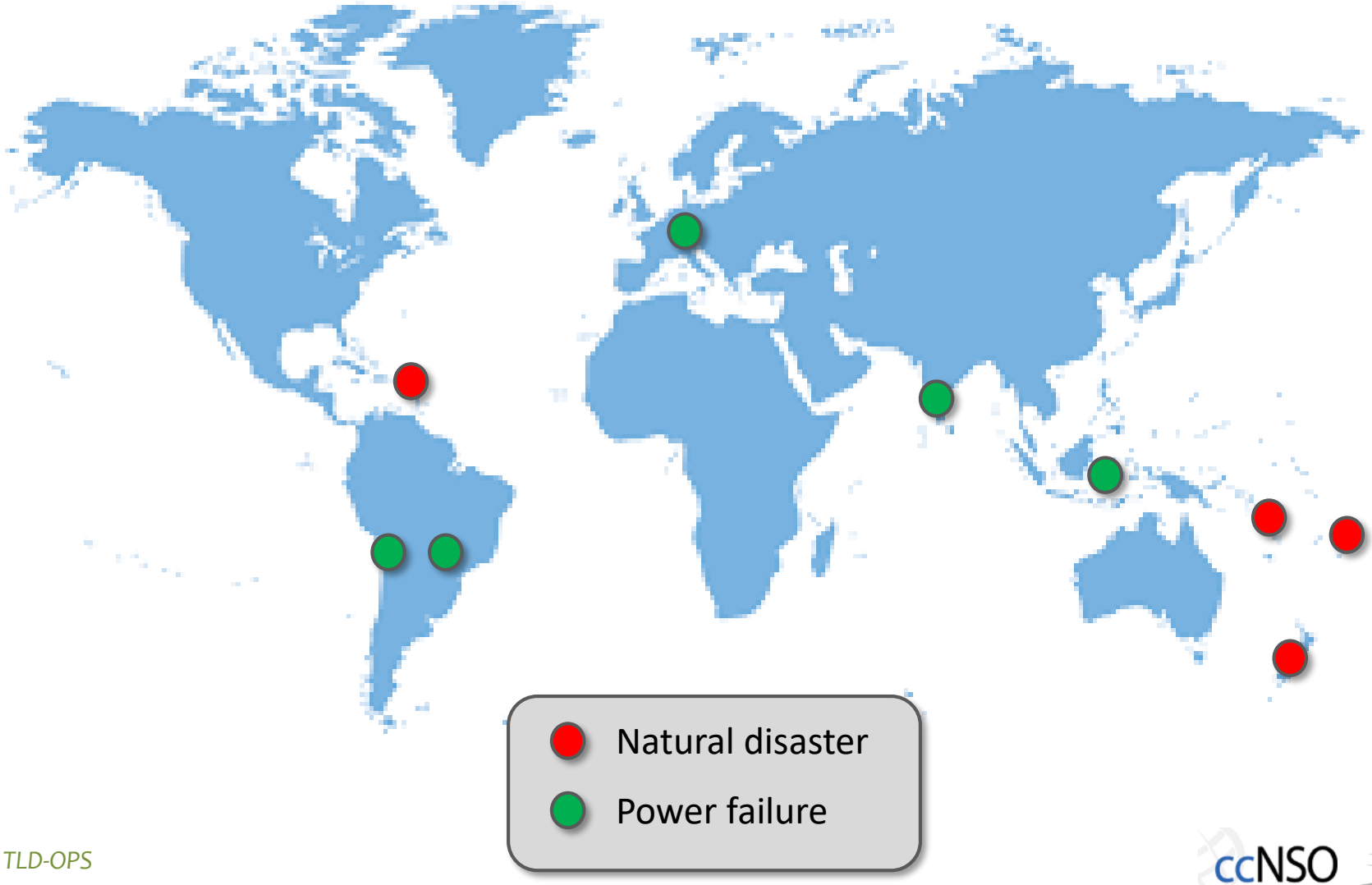
Natural disaster – What impact for ccTLDs ?

- Puerto Rico was recently hit by one of the strongest hurricanes in recent history, resulting in significant problems for the .PR registry which didn't have any impact because of the recovery plan in place.

- A survey was conducted at the beginning of the year to collect information on the type of disasters and emergencies ccTLDs have faced

- Some highlights :
  - 4 TLDs reported a recent natural disaster
  - 50% of respondents who experienced disaster in their organization estimated that the time taken to recover operations was under 6 hours
  - Organizations with large domain counts (> 50 000) are generally set-up to perform remote disaster recovery if needed
  - 78% of ccTLDs (globally) consider their organization either prepared or very prepared for a disaster/emergency

Last natural disasters



ccNSO ICANN

Major root causes

Earthquakes

Hurricanes, cyclones, tornadoes

Volcanic eruptions

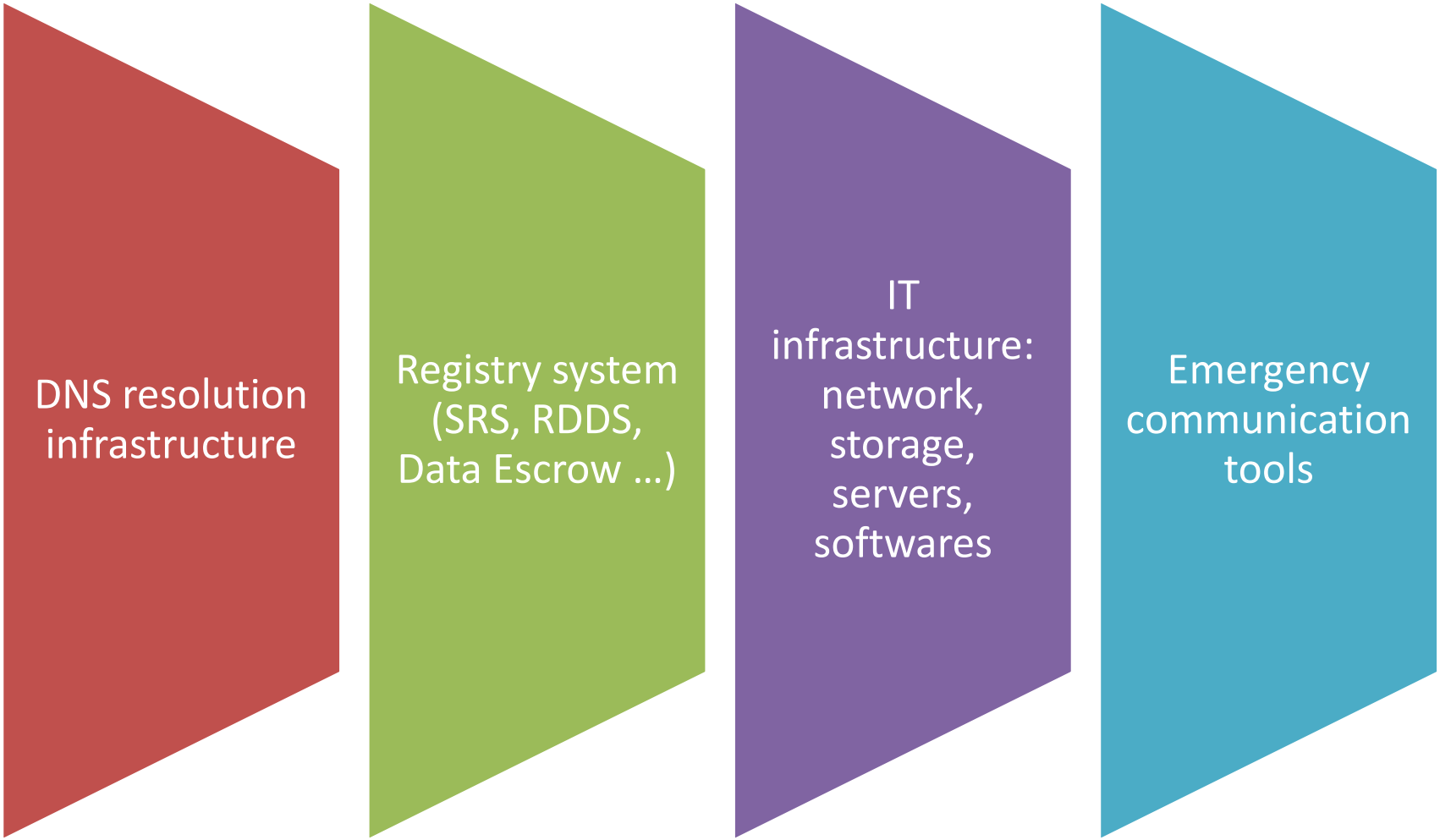
What's next?
Natural Disasters – DR/BCP Readiness

- 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

Focus for the TLD-OPS community

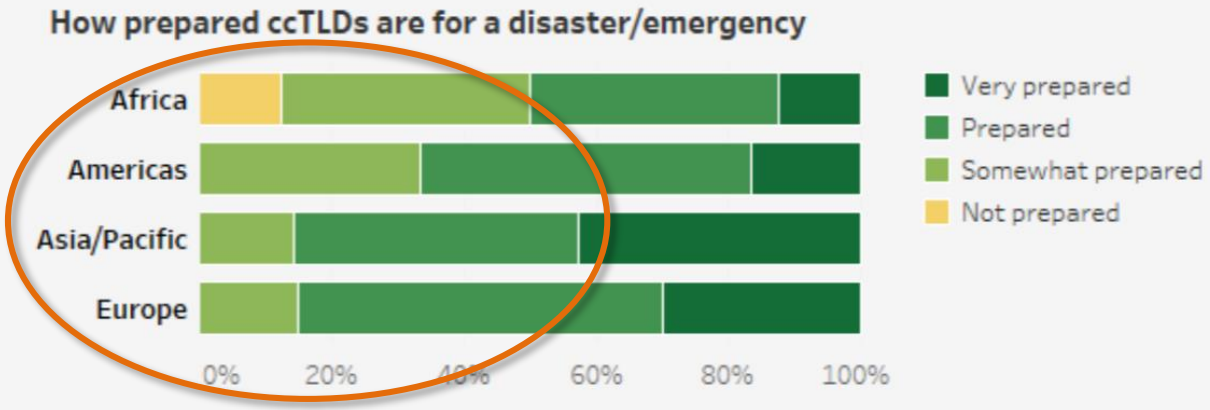


ccNSO ICANN

Disaster and emergency preparedness in ccTLD Registries Joint Survey Results (ICANN61)

Overall preparedness for a disaster/emergency

78% of ccTLDs (globally) consider their organisation either *prepared* or *very prepared* for a disaster/emergency

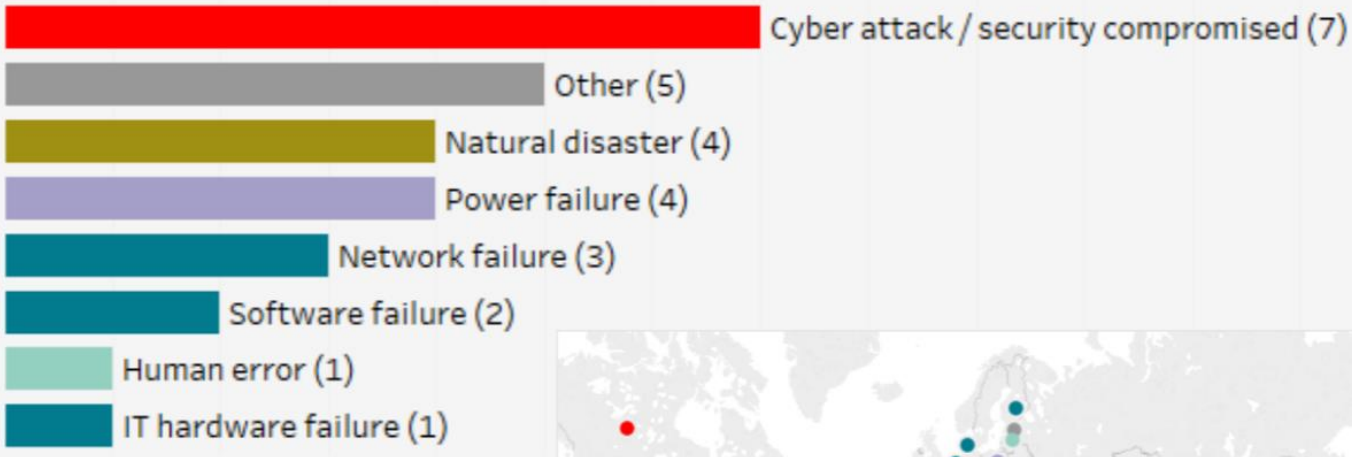


Want advice?
Considering talking to 'very prepared' registries in your region:
.au, .be, .ca, .de, .dk, .no, .nu, .nz, .om, .qa, .ru, .tn, .uk, .vu

https://lactld.info/sites/default/files/2018-04/Preparaci%C3%B3n%20de%20los%20ccTLD%20ante%20las%20emergencias%20y%20los%20desastres%20naturales.pdf

Disaster and emergency preparedness in ccTLD Registries Joint Survey Results (ICANN61)

Cyber attack/security compromise are most common cause of incidents (25%)

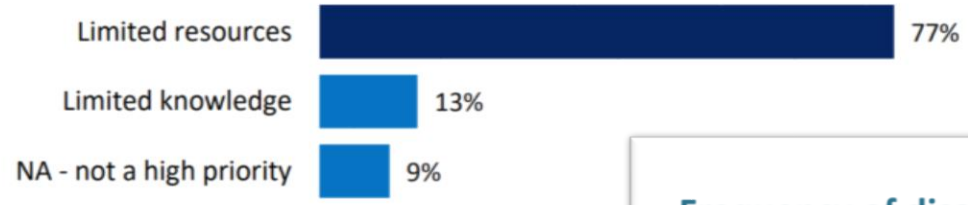


FOCUS NOT ONLY ON NATURAL DISASTERS

Disaster and emergency preparedness in ccTLD Registries Joint Survey Results (ICANN61)

Barriers to regular disaster testing and planning

'Limited resource' was the most common barrier to regular disaster testing and planning (77 % of respondents). See Annexe 1.11 for data.



Frequency of disaster testing

14 respondents (27%) of respondents reported that their organisations never perform disaster testing.

See Annexe 1.8 for data.*

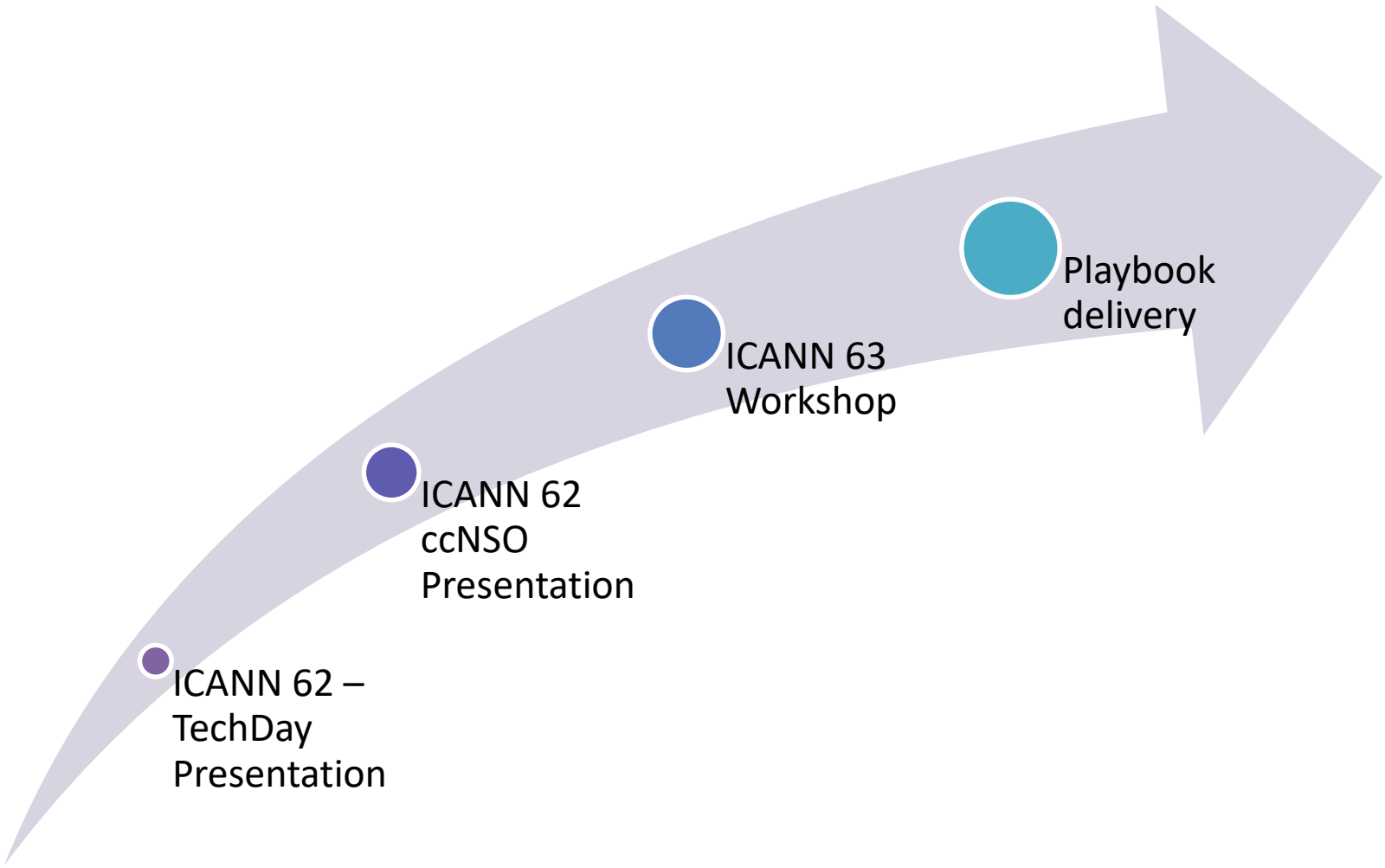
*4 respondents each had two respondents providing different responses to the above question. Both responses were counted in the above chart.

Workshop: Table top exercise valuable?

Feedback from the community

- What does the community needs ? A playbook with advices, 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 (co-chair)
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