

# Collaborative Security

Reflections about Security and the Open Internet

27th Annual First Conference  
June 18, 2015

**Internet  
Society**



independent source of  
leadership for Internet  
policy, technology  
standards, and future  
development

**Mission:**  
To promote the open  
development, evolution,  
and use of the Internet  
for the benefit of all  
people throughout the  
world.

Founded in 1992  
by Internet  
pioneers

Global and  
Inclusive

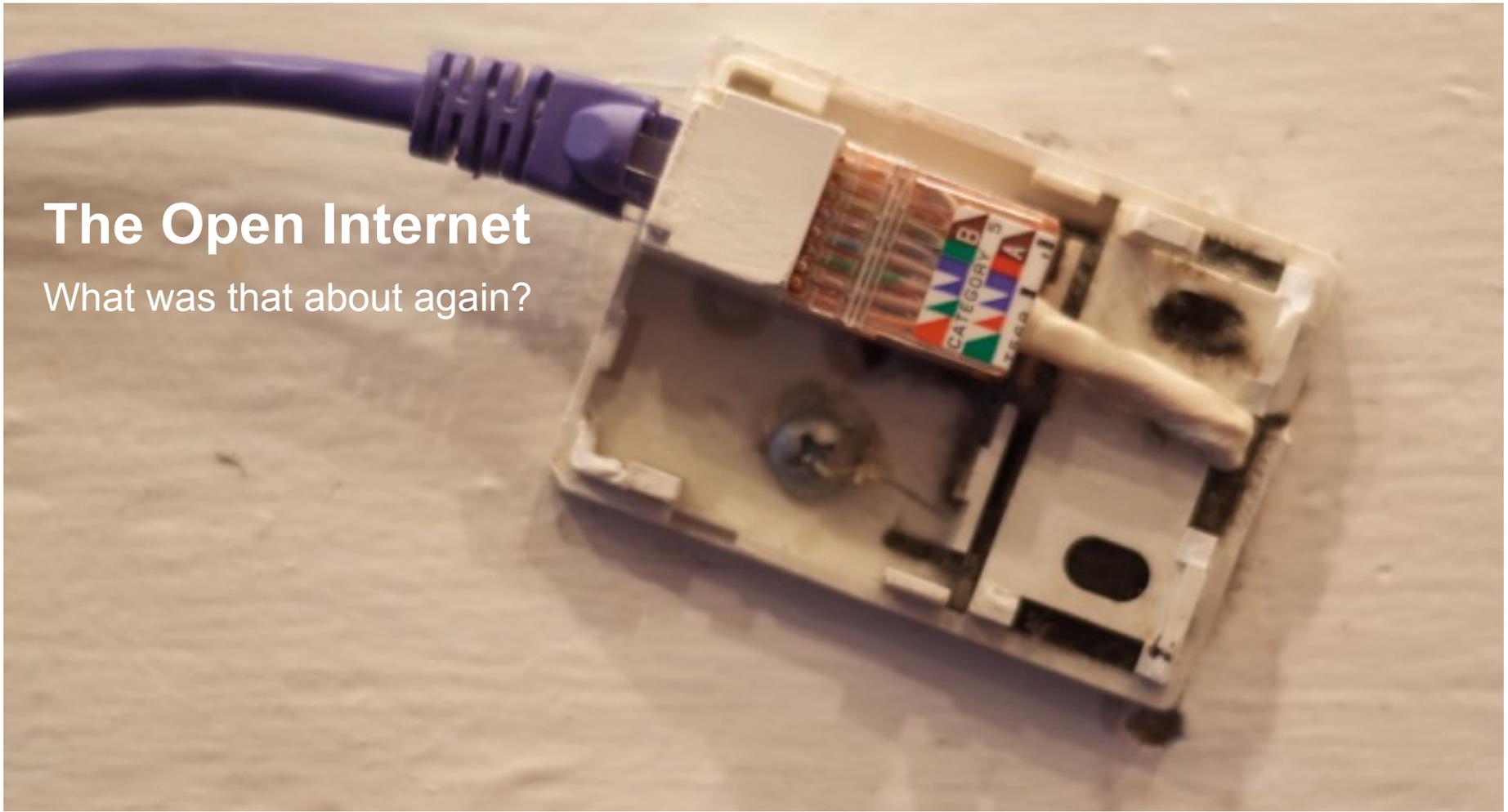
Independent and  
Not-for-Profit

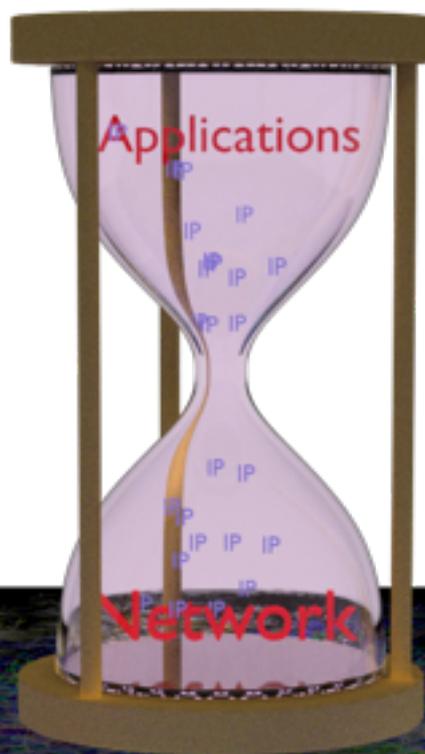
Organizational  
home for the  
IETF

<http://www.internetsociety.org/get-involved/individuals>

# The Open Internet

What was that about again?









# Security, stupid

The background of the slide features two blue spheres with a yin-yang symbol on them, set against a green, textured background. The spheres are positioned in the center, with one in the foreground and one slightly behind it. The text is arranged around these spheres on light blue, tilted rectangular cards.

**Open  
Platform**

**Open for  
attack and  
intrusion**

**Permission  
less  
innovation**

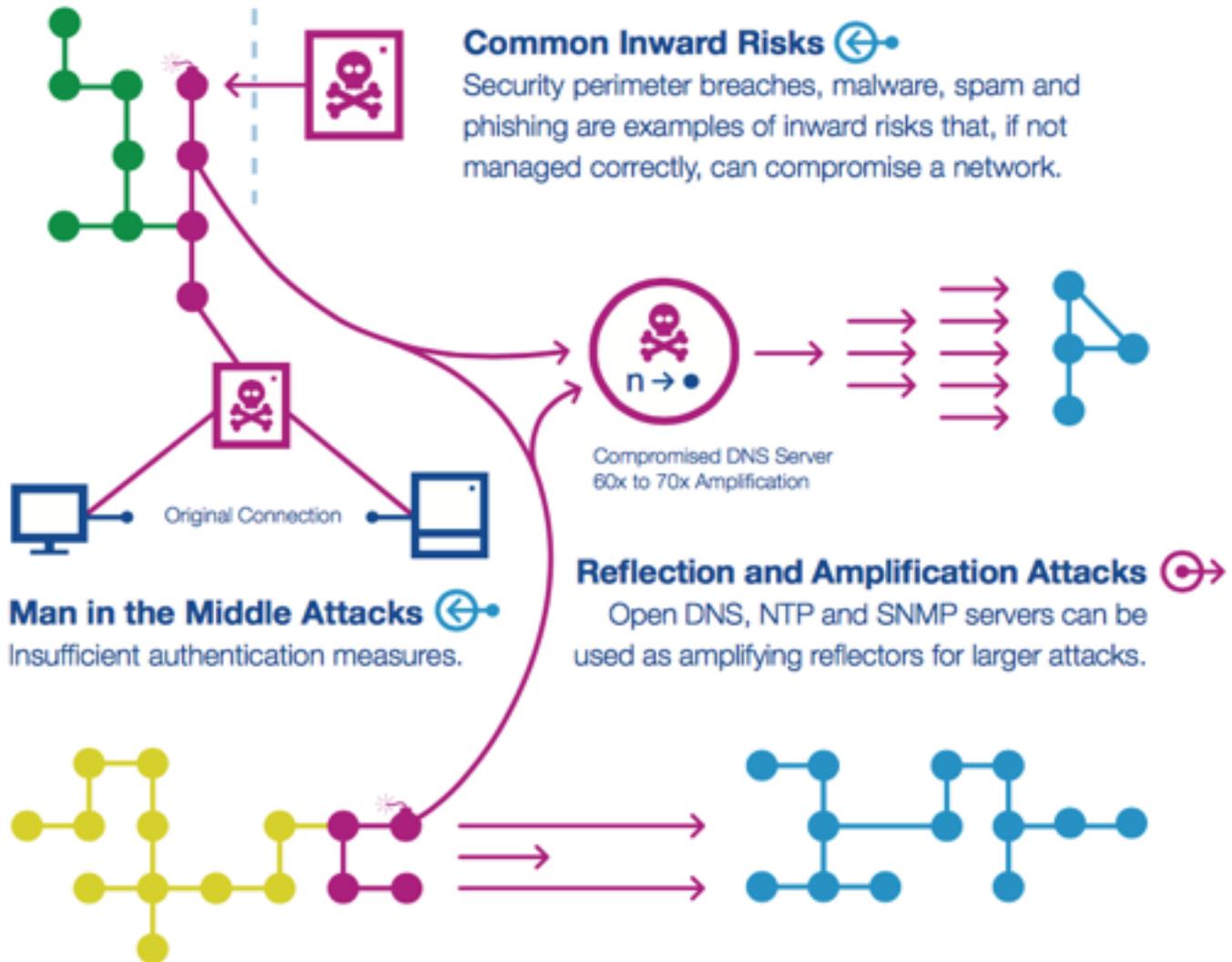
**Malware  
development  
& deployment**

**Global Reach**

**Attacks and  
crime are  
cross-border**

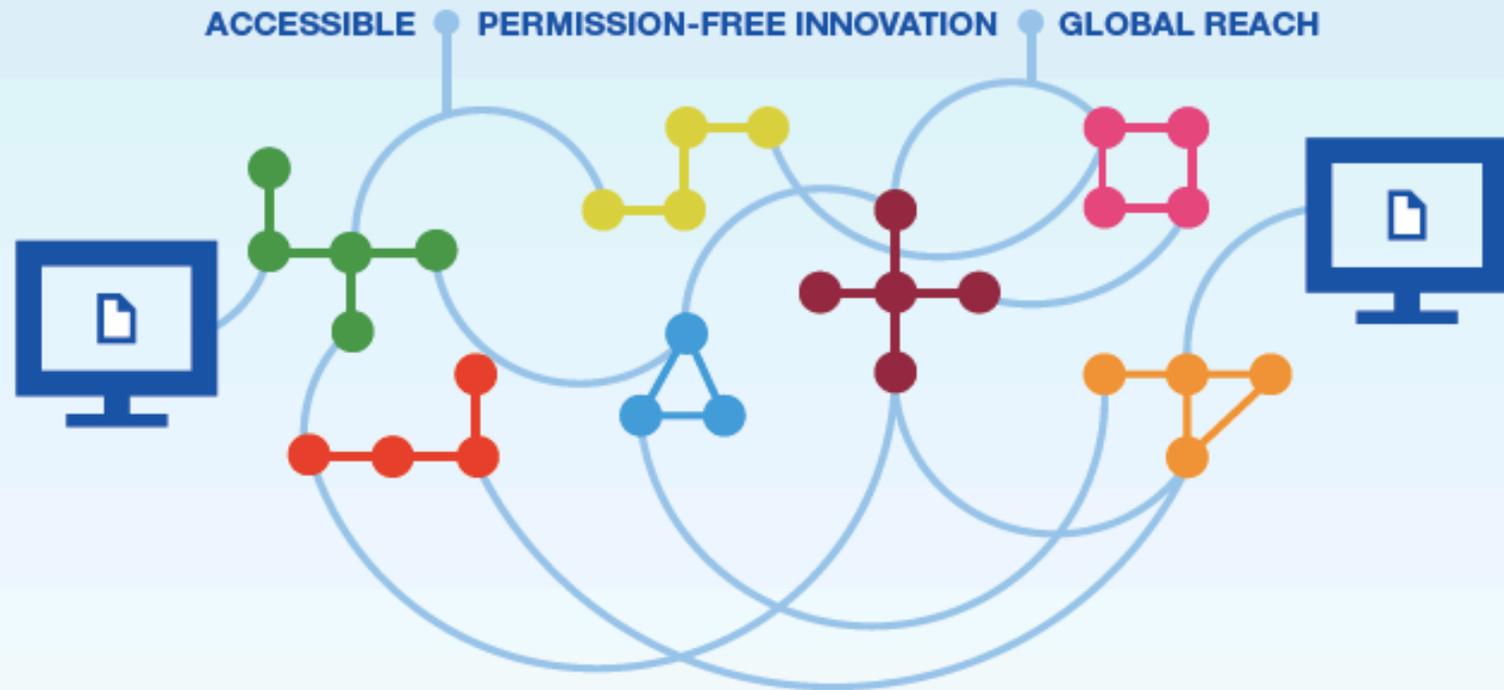
**Voluntary  
collaboration**

**Hard to  
mandate**



# The Internet is open, interconnected and interdependent

It's an ecosystem based on collaboration and shared responsibility



Each network is responsible not only for its own security, but also contributes to the overall security of the medium. The challenge is to create a culture of collective responsibility to make the Internet more secure and resilient.

**Fostering  
Confidence and  
Protecting  
Opportunities**

**Fundamental  
Properties and  
Values**

# **Collaborative Security**

An approach to tackling Internet Security issues

**APRIL 2015**

**Collective  
Responsibility**

**Think Globally  
Act Locally**

**Evolution and  
Consensus**



**Where the rubber meets the road.**

Orgs

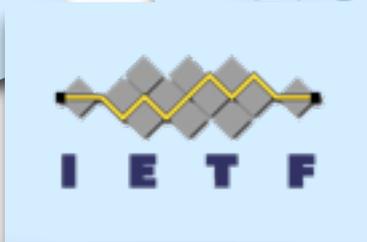
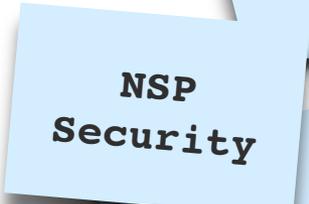
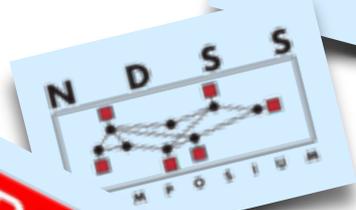
Development

Devops

Researchers

OPS

SDOs



# Examples of Standardization



**STIX**

**DOTS**

**IPfix**

**CARIS Workshop**

**Telemetry**

**Taxii**

**MILE**

**IODEFv2**

**Rolie**

**RID**

**SACM**

**XMPPgrid**

One goal of the workshop is to improve mutual awareness of the participating organizations, to understand their roles, and improve communication between them. A key outcome of the workshop is to provide greater awareness of existing efforts to mitigate specific types of attacks and greater understanding of the options others have to collaborate and engage with these efforts. Another goal is to improve end user experience through stronger coordination between the security, operations, and research communities.



**RDAP**

**Query and Response  
are standardized,  
structured and  
parseable**

**Restful Queries  
JSON responses**

**RFC  
7480-7485**

**"Registry Operator shall implement a new standard supporting access to domain name registration data (SAC 051) no later than one hundred thirty--five (135) days after it is requested by ICANN if: 1) the IETF produces a standard (i.e., it is published, at least, as a Proposed Standard RFC as specified in RFC 2026); and 2) its implementation is commercially reasonable in the context of the overall operation of the registry."**



```
{
  "handle": "APNIC-AP-V6-BNE",
  "start": "2001:dc0:2000::",
  "endAddress": "2001:dc0:3fff:ffff:ffff:ffff:ffff:ffff",
  "ipVersion": "v6",
  "name": "APNIC-AP-V6-BNE",
  "type": "ASSIGNED PORTABLE",
  "country": "AU",
  "parentHandle": "2001:0DC0::/32",
  "objectClassName": "ip network",
  "entities": [ {
    "handle": "DNS3-AP",
    "vcardArray": [ "vcard", [ [ "version", { }, "text", "Administration" ], [ "kind", { }, "text", "group" ], [
"adr", {
  "label": "6 Cordelia Street\\nSouth Brisbane\\nQLD",
  "text", [ "", "", "", "", "", "", "" ] ], [ "tel",
"voice",
"fax",
"email",
"roles": [ "administrative" ],
"objectClassName": "entity",
"remarks": [ {
  "title": "remarks",
  "description": [ "DNS in-addr.arpa zone files maintai
} ],
"links": [ {
  "value": "http://rdap.apnic.net/ip/2001:dc0:2000::/35",
  "rel": "self",
  "href": "http://rdap.apnic.net/ip/2001:dc0:2000::/35/entity/DNS3-AP",
  "type": "application"
} ]
}, {
  "handle": "IRT-2",
  "vcardArray": [
"email", {
  "pref": "1"
}, "text", "security",
"label": "Brisbane",
"roles": [ "abuse" ],
"objectClassName": "entity",
"remarks": [ {
  "title": "remarks",
  "description": [ "APNIC is a Regional Internet Registry.", "We do not operate",
complaints of network abuse.", "For more information, see www.apnic.net/irt" ]
} ]
}, {
  "value": "http://rdap.apnic.net/ip/2001:dc0:2000::/35",
  "rel": "self",
  "href": "http://rdap.apnic.net/ip/2001:dc0:2000::/35",
  "type": "application"
} ]
} ]
}
```



RDAP

How to find these services?

```

"hand
"star
"endAc
ff:ffff:ffff:ffff",
"ipVer
"name"
"type"
"country" : "AU",
"parentHandle" : "2001:0DC0::/32",
"objectClassName" : "ip network",
"entities" : [ {
  "handle" : "DNS3-AP",
  "vcardArray" : [ "vcard", [ [ "version", { }, "te
"adr", {
  "label" : "6 Cordelia Street\nSouth Brisbane\nQLD 4101"
}, "text", [ "", "", "", "", "", "", "" ] ], [ "tel", {
  "type" : "voice"
}, "text", "+61 7 3367 0490" ], [ "tel", {
  "type" : "fax"
}, "text", "+61 7 3367 0482" ], [ "email", { }, "text", "dns-ad
"roles" : [ "administrative" ],
"objectClassName" : "entity",
"remarks" : [ {
  "title" : "remarks",
  "description" : [ "DNS
} ],
"links" :

```

Top-Level Domains (TLDs), Autonomous System (AS) numbers, and network blocks are delegated by IANA to Internet registries such as TLD registries and Regional Internet Registries (RIRs) that then issue further delegations and maintain information about them. Thus, the bootstrap information needed by RDAP clients is best generated from data and processes already maintained by IANA; the relevant registries already exist at [\[ipv4req\]](#), [\[ipv6req\]](#), [\[asreq\]](#), and [\[domainreg\]](#).

```

"rel" : "self",
"href" : "http://rdap.apnic.net/entity/IRT-APNIC-AP",
"type" : "application/rdap+json"

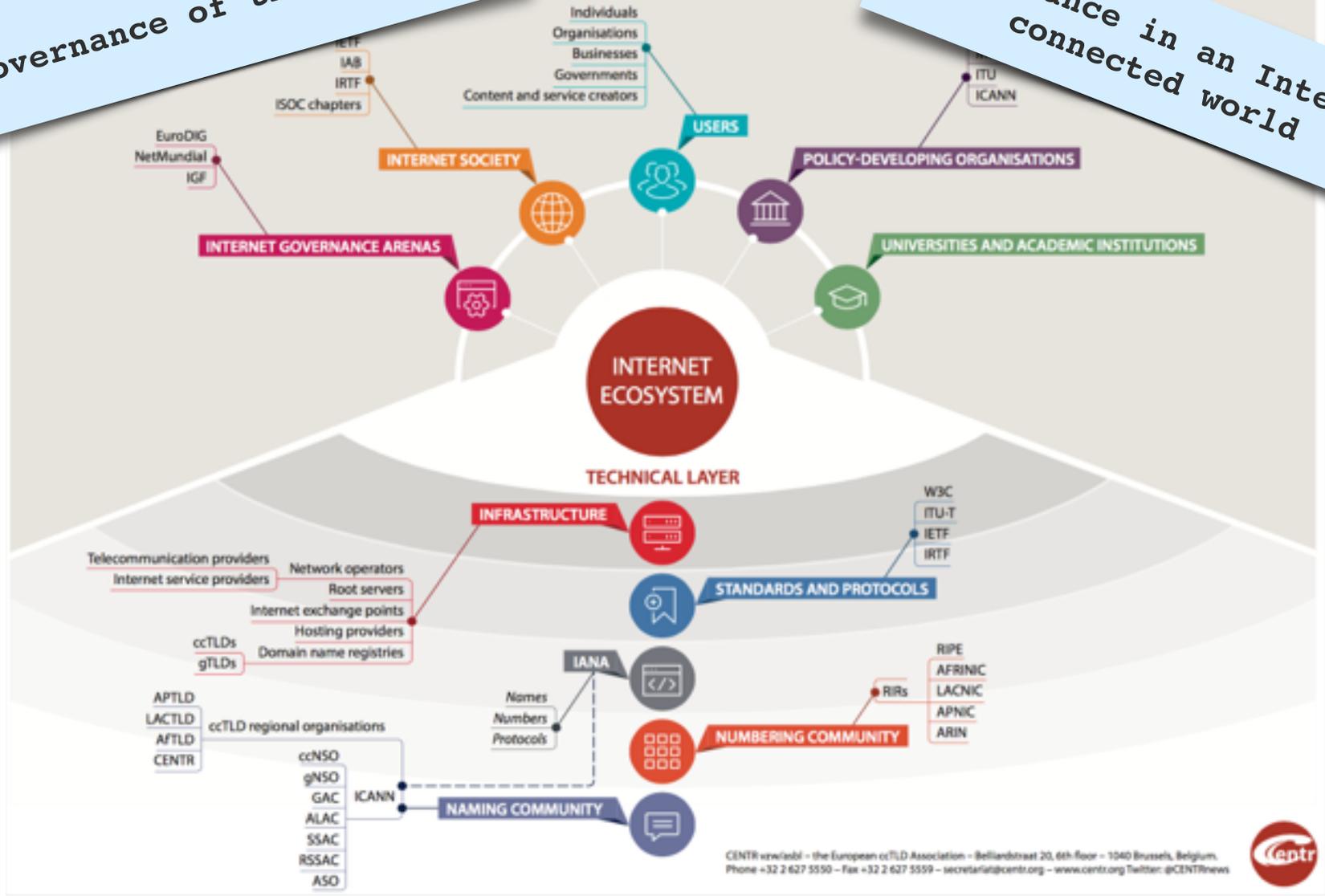
"remarks" : "Regional Internet Registry.", "We do not operate the referring network and", "is unable to investigate
for more information, see www.apnic.net/irt" ]
"rel" : "self",
"href" : "http://rdap.apnic.net/ip/2001:dc0:2000::/35",
"rel" : "self",
"href" : "http://rdap.apnic.net/entity/IRT-APNIC-AP",
"type" : "application/rdap+json"

```



# Governance of the Internet

# Governance in an Internet connected world





## Internet Assigned Numbers Authority

The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. [Learn more.](#)

### Domain Names

IANA manages the DNS Root Zone (assignments of ccTLDs and gTLDs) along with other functions such as the .int and .arpa zones.

- Root Zone Management
- Database of Top Level Domains
- .int Registry
- .arpa Registry
- IDN Practices Repository

### Number Resources

IANA coordinates allocations from the global IP and AS number spaces, such as those made to Regional Internet Registries.

- IP Addresses & AS Numbers
- Network abuse information

### Protocol Assignments

IANA is the central repository for protocol name and number registries used in many Internet protocols.

- Protocol Registries
- Apply for an assignment
- Time Zone Database

# Shared Internet Resources

Smooth operation of the Internet depends upon a **global, coordinated, community-driven** approach to managing key shared resources

## ROLES

### Policy >

Policies are the agreed upon rules developed through community-based processes by which shared Internet resources are managed.

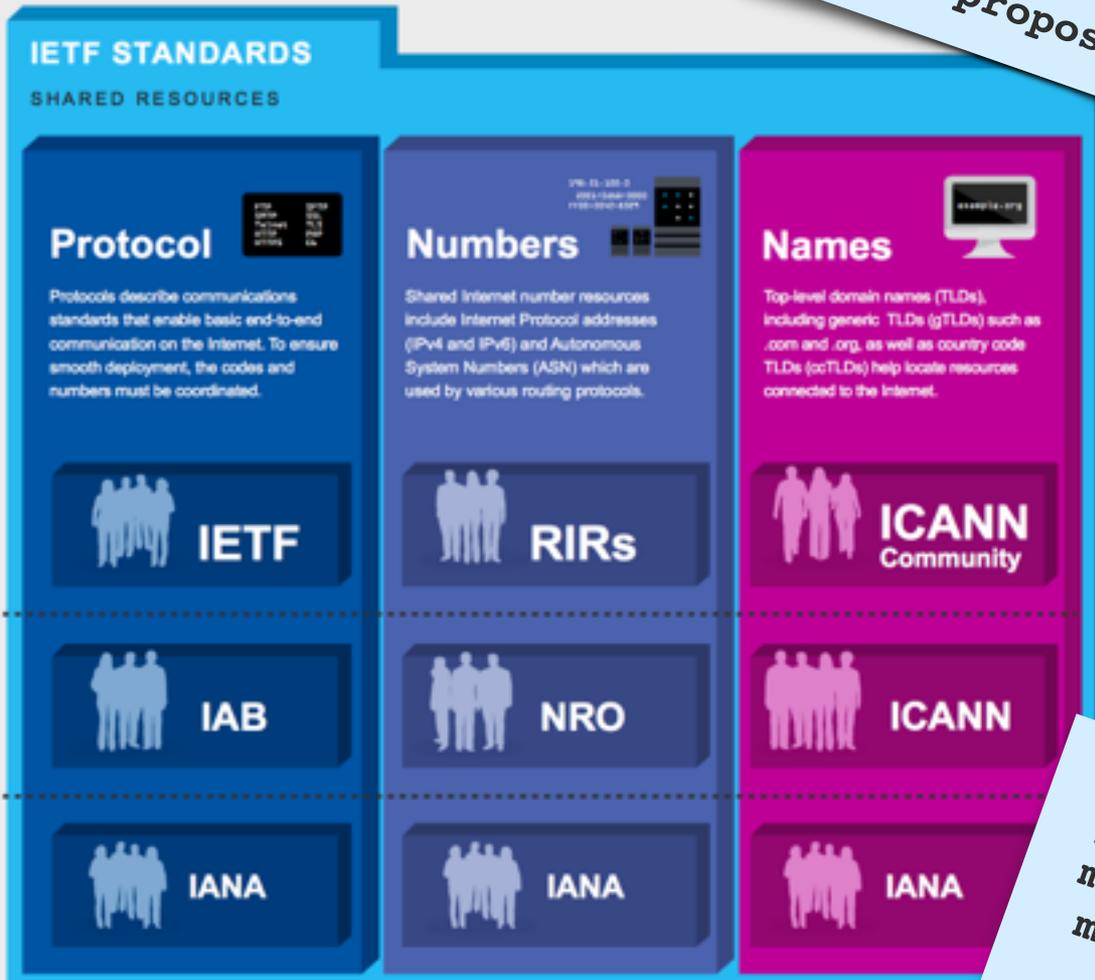
### Oversight >

Oversight to ensure policies and implementation are aligned promotes the coherent long-term development and use of shared Internet resources.

### Implementation >

Implementation of shared Internet resources in a neutral and responsible manner guided by the relevant policy and oversight processes.

Learn more at: [www.internetsociety.org](http://www.internetsociety.org)



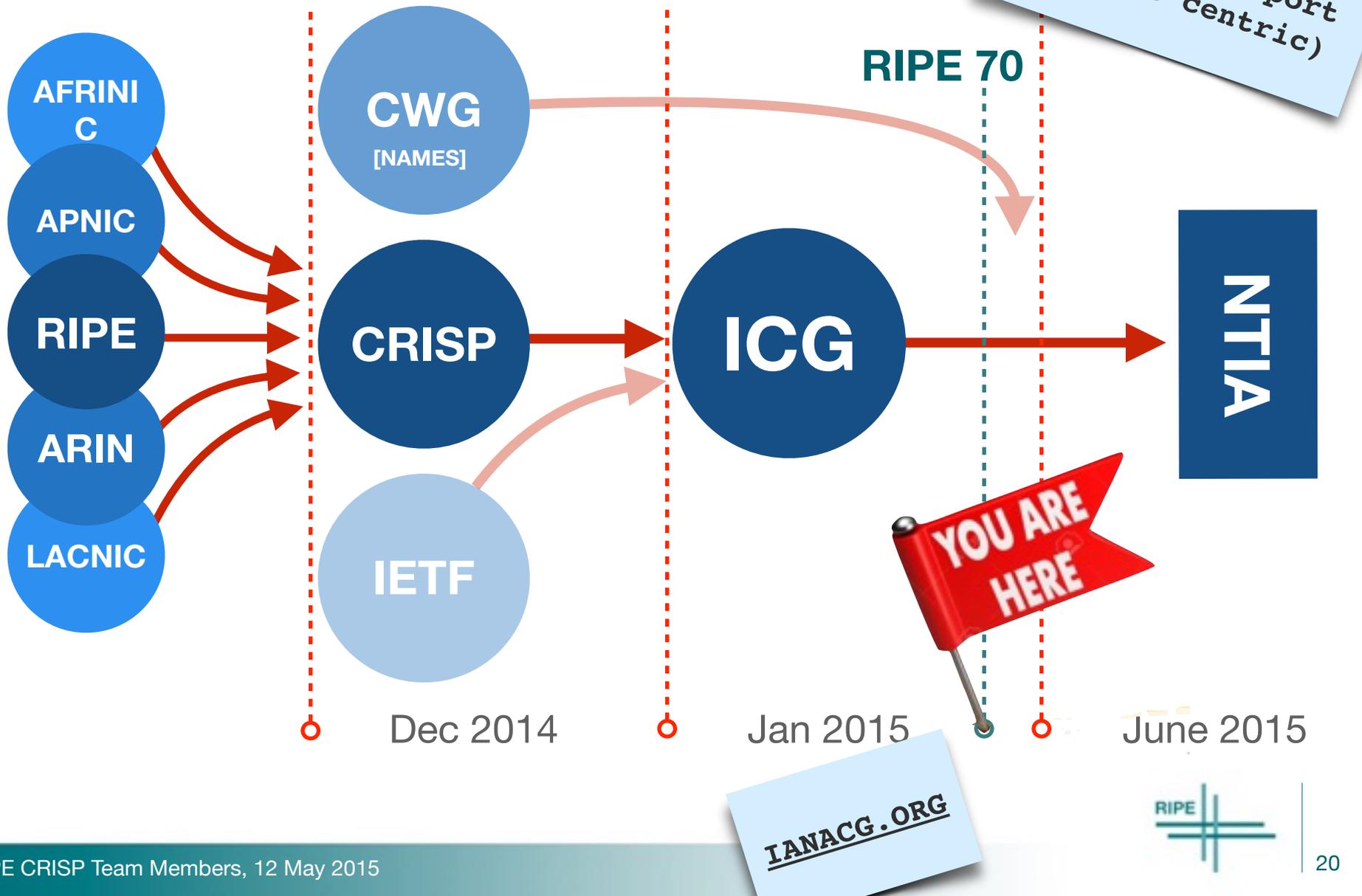
This is not a representation of the proposal

just a mental model

<http://www.internetsociety.org/who-makes-internet-work-internet-ecosystem>



# Overview of the process





# Mutually Agreed Norms for Routing Security (MANRS)

Stimulate visible improvements in security and resilience of Internet Routing by changing towards a culture of collective responsibility



common problems to be addressed

incorrect routing  
information

traffic with spoofed  
source IP addresses

coordination and  
collaboration  
between network  
operators

## Principles

- 1 The organization (ISP/network operator) recognizes the interdependent nature of the global routing system and its own role in contributing to a secure and resilient Internet.
- 2 The organization integrates best current practices related to routing security and resilience in its network management processes in line with the Actions.
- 3 The organization is committed to preventing, detecting and mitigating routing incidents through collaboration and coordination with peers and other ISPs in line with the Actions.
- 4 The organization encourages its customers and peers to adopt these Principles and Actions.

Action 1

**Prevent propagation of incorrect routing information.**

Action 2

**Prevent traffic with spoofed source IP addresses.**

Action 3

**Facilitate global operational communication and coordination between network operators.**

Advanced  
Action 4

**Facilitate validation of routing information on a global scale.**

Please have this  
conversation with  
your stakeholders



<http://www.routingmanifesto.org/>

or

<http://manrs.org/>

Contact  
[routingmanifesto@ISOC.org](mailto:routingmanifesto@ISOC.org)



# Olaf M. Kolkman

Chief Internet Technology  
Officer

[Kolkman@isoc.org](mailto:Kolkman@isoc.org)  
twitter: @kolkman