Council of European National Top-Level Domain Registries

Report on RIPE74

Budapest
8-12 May 2017

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Contents

Highlights

In the making: RIPE Working Group on IoT

The work of the RIPE address policy working group seems to be pretty much done, with minor housekeeping still to be done before the final depletion of IPv4 addresses. There is now room and interest in addressing new issues and the Internet of Things (IoT) has attracted increased interest. A new RIPE working group on IoT is now in the making. The main question posed during a Birds of a Feather (BoF) meeting on IoT in Budapest was what the community of network operators can do to improve the security of IoT traffic on the networks, and, even more simply, what their role is. The interested group led by Marco Hogewoning will have a full working group slot to discuss the way forward during the next RIPE meeting in Dubai. A draft text to develop a charter can be found on the dedicated mailing list.

A first IoT session had been held during RIPE73 last year. According to Hogewoning, the purpose of the RIPE74 BoF session was to move from a mere finger-pointing to "clueless" manufacturers and IoT service offerings. Questions to the operator community included: what role do service providers want to play; what role can they play; what do we need from manufacturers; and what is the role of government?

What devices, what services, what companies?

Elliot Lear, who is working on IoT for Cisco, triggered the discussion by listing the problems the technical community faces.

Lear said that operators like Google or Apple wouldn't have any problem controlling a million devices on the net, yet the issue was that "we do not even know what kind of devices they are". The diversity of devices – from light bulbs to door locks or network-enables pacemakers – made it difficult to conceive how to offer "secure" IoT services. Consumers, manufacturers, network vendors, services providers and governments were all parties to the game, with some of the latter up in arms after the Mirai attacks.

Lear asked what the RIPE community needed from hardware manufacturers like Cisco (and its competitors, such as Huawei).

Some ideas on what to do

A shortlist of ideas on steps that could be taken were offered during the BoF. Merike Keao (Farsight Security CTO) suggested that a certification of minimum standard security would be a possible first step. The minimum standard that all could agree upon could include things like "no default passwords", "use of cryptographically secure protocols" and obligatory "firmware/software updates". Tricky issues that had to be considered included the prevention of lock-ins of devices to services providers, as the devices might fail when the providers go out of service.

The technical community should share the "network security culture" developed over the last decade with the newcomers (IoT device makers or service providers), said a Czech participant. Very much like router vendors a decade ago, IoT vendors today allowed for easy-to-use password systems, from pre-installed to even "any password works"-concepts. "The mission is to share our culture, not because we are smart, but because we did it before", he recommended.

Remco van Mook, member of the RIPE Executive Board, appealed to the RIPE community to consider the fact that traffic from IoT devices would at some point flow through the networks of RIPE members. They could consider filtering traffic as it is done for other things (including spam or DDoS traffic). Providers selling network services, according to Mohsen Souissi, (AFNIC), also have an obligation to inform and educate their users.

However, there were certainly concerns raised against network providers guarding/monitoring the net. Leslie Daigle (former ISOC CTO) warned that the effects of Mirai traffic and ISP filtering getting in the way could result in similar effects. Gordon Lennox, former European Commission official, warned against the potential of regulation shrinking the space for innovative experiments.

Government regulation?

Beside the role of network operators, several BoF participants described where they saw a role for governments. One issue brought up was the lack

of legal responsibility for damages. Looking at the example of the Mirai attack, nobody tried to go back to the root cause for the attack, i.e. the cameras with the insecure Mirai software. Yet the interlinking of all sorts of devices, some with high and some with no security standard, made it unavoidable to consider liability issues.

Jeff Osborn (ISC CEO), pointed to two aspects in need of regulation. One was the need to prevent lock-ins that stopped users from moving their devices from a failing or insecure provider to a better one, making better security a competitive advantage. The other was that cross-border liability claims needed some international agreement amongst governments. It was up to the technical community to consider what minimum standards could be made part of international agreements, in a way politicians could understand.

"IoT and RIPE: We need to jump in"

Paul Rendeck (Director External Relation at RIPE NCC) appealed to the RIPE members not to leave the discussion to other technical bodies such as the IETF, the IEEE or the ITU, especially the latter, which is still seen as a form of competitor to self-regulatory bodies. Rendek said conferences with IoT device vendors and governments, in the Middle East for example, had shown that the IoT companies did not know RIPE, for example. Governments pleaded for RIPE NCC to show up and give visibility to RIPE, as "right now their eyes are on the ITU". Rendek said that the RIPE community needed to "jump in", explaining the efforts RIPE NCC staff has made over the last two meetings to promote the topic. RIPE NCC is a member of the European Alliance for IoT Innovation (AIOTI) and has recently asked members to contribute to a survey prepared by the organization.

Efforts to set standards for addressing and security IoT are underway at the ITU, reported Hogewoning during the Cooperation WG. There are now three WGs struggling to make their mark on IoT developments.

Working Party 1 of Study Group 20 covers four questions:

Q1: End-to-end connectivity, networks, interoperability, infrastructures and Big Data aspects related to IoT and SC&C
Q2: Requirements, capabilities and use cases across verticals
Q3: Architectures, management, protocols and Quality of Service
Q4: e/Smart services, applications and supporting platforms

Working Party 2 of Study Group 20 covers three questions:

Q5: Research and emerging technologies, terminology and definitions
Q6: Security, privacy, trust and identification
Q7: Evaluation and assessment of Smart Sustainable Cities and

Finally, IPv6 related IoT work is ongoing, aimed at establishing a recommendation and one supplement:

Y.IPv6RefModel "Reference Model of IPv6 Addressing Plan for Internet of Things Deployment"
Y.IPv6-suite "Reference Model of Protocol Suite for IPv6 Interoperable IoT Deployments
Y. IPv6-IoT Supp."IPv6 Potential for the Internet of Things and Smart Cities

Discussion on the Reference model has been postponed until the end of the year. Hogewoning said that RIPE NCC would further observe the work in its role as ITU sector member and would promote keeping any recommendations open to other standards, while underlining that with regards to IPv6, ITU was not the appropriate forum.

Huston: Widespread digital pollution has to be stopped

A much bleaker picture on IoT, or as he called it, the "internet of stupid things", was given before the BoF by Geoff Huston. Huston reported that an average household nowadays has about 40 network-enabled devices, citing a security expert. Yet only a third had an operating system that allowed the informed user to manipulate them. The devices were mostly embedded, running some proprietary software, which did not allow easy control of who "telephoned home". You could log the traffic of your router, said Huston, but who would take the time to check these logs? Privacy, even for the savvy, was a historical concept.

Given the mass of new, mostly insecure connected devices, digital pollution was only getting worse, increasing the risks for exploits and attacks. A main commercial driver, according to Huston, was the saturation with personal computers, handheld devices. The chip industry that could produce chips

ever more cheaply had changed their business model and was looking for large numbers of cheap chips.

Europol wish list: More WHOIS accuracy and no Carrier Grade NATs, please

Europol is talking to EU legislators about the potential of regulatory measures to avoid Carrier Grade NATs that complicate identification of users of an IP address at a given time. This was reported by Gregory Mounier, Europol Head of Outreach of the European Cybercrime Center (E3C), frequent guest at the development and operator community meetings in recent years. While the "hiding" resulting from address scarcity has a side effect of being privacy-friendly, agents would prefer a one-user-one-IP-address policy (or at least less users per IP). Migration to IPv6 has therefore a new fan in Europol (alas, Europol itself still has to migrate). Beside the call in the Cooperation Working Group against CGNs, Mounier called on the Database WG to change the RIPE registration policy to ensure better accuracy of the WHOIS database.

CGN and the Belgian Example

Chances to combat online crime are hampered by the use of carrier grade NATs, according to Mounier, who gave several examples from investigations. With 50 different users behind one IP address, some investigations could not be pursued or, at times, investigators went on to check every single user, leading to delay and investigation of many innocent citizens. Around 50 percent of fixed net connections and about 90 percent of mobile connections were behind CGNs, according to studies. Those interested in being anonymous could simply use their smartphones, Mounier said.

To change the situation, European law enforcement authorities (LEAs) earlier this year founded the European Network of Law Enforcement Experts for CGN. A quick fix the LEAs have in mind points to a voluntary code of conduct model between the Belgian Police and Belgian Providers. The Code sets the number to 16 users behind one Ipv4 address as a compromise. Providers further pledge to migrate to IPv6 as soon as possible.

Mounier hailed the model as having a positive effect on IPv6 adoption in Belgium which, according to Europol, is up to 49 percent, compared to what Mounier listed as much lower figures in France, the UK or Italy. The stats used seem to come from Google; recent figures by Akamai show more levelled adoption rates. Nevertheless, the expert Group and Europol are currently lobbying for some kind of mechanism (a code or guideline) with European legislators, Mounier confirmed. Members at the RIPE meeting were not fully convinced, pointing out that IP addresses would in fact become less and less important for identification. Mounier also did not figure in the ECJ ruling against data retention, which might in fact question measures to store identifiable personal information of users not necessarily operationally by default.

Another option, the storing of IP addresses at the connectivity providers and port numbers at the content providers, is harder to achieve and might run into the same data protection concerns.

Accuracy down the chain

While data protection officials have just taken aim at the ongoing WHOIS work at ICANN to question the increasing data sets ICANN obliges its registries/registrars to store, Europol is stepping up its effort to improve WHOIS accuracy at the IP registries.

In Budapest, Mounier bemoaned the problems law enforcement had in investigations in Europe due to the lack of WHOIS information for downstream providers and resellers, which are not held to the same policies and standards as RIPE members. He called on for changes in the registration policy that would make complete WHOIS entrances obligatory, all the way down the chain to the provider who serves end-customers with the IP addresses. He also said that law enforcement agents needed better information on geographic location of providers.

Changes to the RIPE registration policy to apply this would be significant, including a repurposing of the data, said Peter Koch, DENIC. Randy Bush, IIJ, argued that the purpose was operations and while law enforcement was certainly invited to use the database, "it is our database".

Shutdown policy proposal in AFRINIC called dangerous by RIPE community members

The proposal to sanction internet shutdowns by declining to allocate new IP address resources in the AFRINIC region gave rise to a fierce discussion at

RIPE74. The policy will be discussed during AFRINIC this week and the African RIR has never seen as many registrations from governments as for this meeting. Several governments have reacted harshly when the policy was proposed, for example Kenya, while AFRINIC felt compelled to underline the proposal was just "a proposal still to be discussed in the upcoming AFRINIC open policy meeting".

The core of the proposal is that AFRINIC should decline to allocate resources for 12 months to all state entities after a shutdown or partial shutdown. The ban shall include all state-owned entities (over 50 percent state ownership), but not academic institutions. The decision for a ban shall be made after a consultation of the AFRINIC community by the AFRINIC governance committee. During the 12-month suspension time, AFRINIC will also stop assisting in any transfers. All sub-assignments of space within the individual country for the state entities shall also cease. If a government has three or more shutdowns during 10 years, all resources shall be revoked.

Andrew Alston, from connectivity provider Liquid Communications, who co-authored the proposal with Liquid Communications CTO, Ben Roberts, and Fiona Asonga, CEO of the Kenyan Telecommunications Service Provider Association (TESPOK), explained the motivation behind the policy during the RIPE meeting.

Shutdowns have become more numerous, even a regular political tool, and were often (if not always) used to silence the political opposition or minority groups. The viciousness of the tool was highlighted recently when the English-speaking minority of Cameroon was deprived of network access for months. Cutting networks could result in people dying at the hands of autocratic governments, he said. A regularly updated list of shutdowns all over the world is provided by NGO Access Now here.

The shutdowns were also costly for African economies, as illustrated by the recent exodus of registrants form the Cameroon TLD. Before the extended shutdown, there have been 63,000 domains registered in Cameroon's ccTLD. Three months into the shutdown, registration has gone down to 31,000.

With international talks over internet as a fundamental right for every person, sanctioning the prevention of access, expression and informational rights was well within AFRINIC 's mandate, Alston said.

RIPE74 participants vocally disagreed, arguing that such sanctions were contrary to the role of the RIRs as neutral IP resource administrators and risked setting them up against governments. Daniel Karrenberg, RIPE NCC Chief Technologist on leave, called the policy proposal dangerous. Malcolm Hutty (LINX), while acknowledging the problem said, "your proposal stinks".

Beside the potential clash with governments, some of whom already were sceptical of the self-governance models in resource administration, issues addressed were that denying governments and public institutions (including academia or social institutions, as planned in the first draft) allocation of new resources or even taking away allocated resources resulted in similar effects as the ones the policy wanted to address. At the same time, a withdrawal of resources or de-allocation did not automatically mean that those resources would not be routed any more. This very fact had been upheld by the RIRs against law enforcements' call to block IP addresses of suspects. Asking for such a measure could now suggest to governments and law enforcement that IP address blocking was possible via the IP registries.

Alston reacted by pointing to changes already included in the second draft, for example the academia exception. However, one main goal of the proposal had already been reached: there was a worldwide discussion on the shutdowns. A number of alternative proposals for sanctions had also been put forward: ICANN could be asked to withdraw the ccTLD delegation from a perpetrator country or no-service and revocations daily fines (for each shutdown day) could be collected, with the help of the ITU.

At AFRINIC 26 (29 May – 2 June), the draft proposal did not find support from most participants. After a fierce discussion at the Open Policy Discussion session, the authors announced they would reconsider, look for further feedback and bring the idea to another forum, such as the Geneva IGF.

Address Policy, Address Markets

RIPE's Address Policy Working Group looks like it's running out of business, apart from some housekeeping. A mere two policy proposals are currently under discussion, less than any other RIR at this moment. However, there is one topic that could receive a lot of attention, if it was filed as an

active policy proposal: how should the last remaining reserves of IPv4 space be distributed?

According to the RIPE last /8 policy, each LIR can currently receive a /22 block once. Given the actual burn rate, RIPE NCC will run out on 5 February 2020 (according to Geoff Huston's statistics). There could be a need for further stretching the last resources, some of the experts at RIPE think. Randy Bush (Internet Initiative Japan) said that he considered it wasn't possible to start a business in four years without having a v4 addresses. RIPE should therefore consider making the future "minimum allocation size" a /24 instead of the current /22 block.

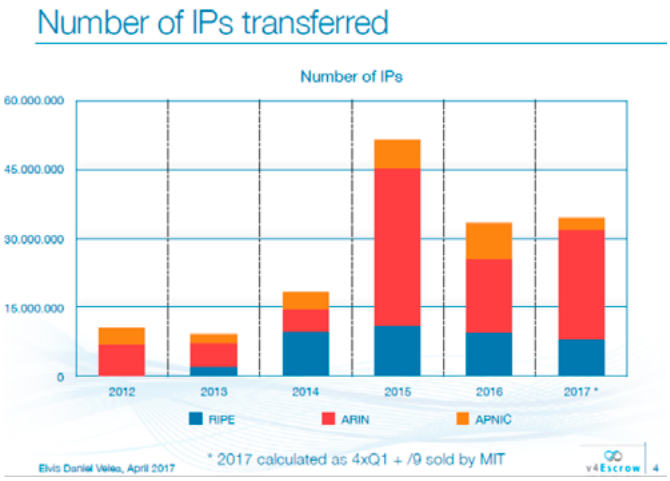
Talks about such a stretch-out policy has already been made in the LACNIC region, which is down to its last /10 block of IPv4. A majority of requests on the ARIN waiting list (resource requests outside special processes to receive small slots for transition) in recent months was also for /24 blocks.

Earlier concerns over a possible explosion of routing tables is not seen as a problem any more by exerts, but some of the opposition to the extension strategies comes from those who would prefer a faster migration to IPv6.

	Available /32s	Reserved /32s	Current Run Out
APNIC	6,840,832	4,071,680	Last /8: early 2020
RIPE NCC	12,497,304	1,050,176	Last /8: early 2021
ARIN	0	6,163,968	
LACNIC	16,128	4,930,560	
AFRINIC	18,076,672	1,840,384	Pool: May2018
	37,412,936	**18,056,768**	

Transfers Markets

With IPv4 more difficult to get, transfers markets have been the new source for resources. Elvis Velea, CEO of the domain broker Service V4Escrow, gave stats showing a decrease of transfers from 50,000,000 in 2015 to 35,000,000 in 2016. For 2017, a slight upturn could be expected, also due to the sale of an MIT /9 block.



Velea underlined that he believes the statistics were not complete, as legacy address transfers are not tracked in the same way as transfers of RIR allocated space. Prices started from $5 USD per single IP-address in 2012 and have risen to up to $20 USD per single IP address nowadays. The prices could rise even more, and Velea expects a solid transfers market at least until 2025. At some point, large legacy holders would bring their assets in IPv4 resources to the market (like MIT this year).

All RIRs will have intra-RIR transfers policies soon, with AFRINIC about to join the club. Differences between the RIRs still exist when it comes to inter-RIR transfers. AFRINIC and LACNIC are both currently considering to allow transfers into their regions, while still holding up against "address-exports".

According to its policy proposal, in addition to publishing statistics on inter-RIR IPv4 and ASN transfers (including legacy resources) and statistics for IPv4, IPv6 and ASN transfers within its service region, RIPE NCC should also "publish updates regarding who holds a legacy resource". The policy change would also protect legacy holders from potential hijacks, Velea argues.

For buyers of second-hand IPv4 addresses, he had several recommendations: be sure to talk to the person that has the authority to sell, ask for blacklist reports beforehand, start routing immediately, but do not use the resources immediately, as a customer could easily receive traffic from the wrong (geo) location.

IPv6 Address Policy

The second policy on the agenda of the RIPE address policy WG is related to IPv6. It aims to change the registration policy for IPv6 provider independent address space to allow the allocation of subnets smaller than a /64. The founders of the Freifunk Hochstift / Freifunk Rheinland e.V. (AS201701), an NGO setting up free WIFIs in Nordrhine-Westfalia, were declined IP space because they wanted to use prefixes to set-up WIFIs in public places. Sub-assignments of IP space had been prevented to stop routing tables to grow due to everybody getting their own independent provider space. The policy is still under discussion.

DNS Working Groups, Plenary Bits

DNS Working Group

Two ongoing software projects and a community project to list and address DNS violations in the wild got the most attention during the DNS WG in Budapest.

The DNS violations project, initiated by cz.nic, has been working on a platform that allows everybody to send DNS protocol violations encountered on the net, from violations of IETF DNS standards to sloppy implementation or just misconfiguration. Starting from an internal listing of the developers of the Knot DNS Resolver, cz.nic has established an open list and allows everybody to send in issues.

Ondrej Sury, cz.nic, presented examples in Budapest, saying the purpose was not "to shame operators or the writers of DNS software", but instead to share knowledge about the problems and help vendors, operators and developers not to fall in the same traps over and over again. The proposal received much applause, and Sury said cz.nic was looking for people to use the platform and for additional support to enhance it (for example by adding a website to the existing github repository). The list of problems is already impressively long (see here). A mailing list can be found here.

Much interest was also expressed in an extension of a tool to better understand incoming DDoS traffic and DNSDIST. Originally only a load balancer, the new edition allowed live traffic inspection (buffering the last 10,000 requests) and according to DNSDIST developer Pieter Lexis from PowerDNS, providing an "swiss army knive" against DDoS protection. Possible selectors and actions:

Selectors	Actions
SourceAddress	Drop
Destinationaddress	RouttoPool
QNAME	Truncate
QTYPE	ReturnSERVEFAIL, NO-TIM, REFUSED
Flags	Returncustomeranswer
OPCODE	Delayeresponsebynmilli-seconds
TCPquery	Removeflagbeforepass-ingtobackend
Numberofentriesina-packetsection	AddoriginatingIPaddres-sinanEDNSooption
Numberoflabelsinth-ename	Logqueryto TCP/IPhost-viaProtobuf
RegularExpression	Increasestatisticscounter
Combineselectorswith-And, OrandNot	StripEDNSClientSubnet SendSNMPtrap

The DNS WG also received updates on the ongoing implementation of DNS privacy RFCs standardized by the IETF, namely the getDNS library and Stubby resolver implementation. Test servers for DNS Privacy enhancing resolvers are available for Unbound (NLnet Labs, OARC, YeN), Knot (Daniel Kahn Gillmore, ACLU) and BIND plus TLS Proxy (SURFnet, Sinodun). More information here.

In his regular update, Anand Buddhdev gave figures on the further roll-out of K root server out of the box instances (now 47 globally, in addition to 5 core sites) plus the updates to CentOS 7 and 10G connections on the core sites. He also announced that the change from DNScheck to Zonemaster for pre-delegation checks is about to be completed, with Zonemaster becoming productive in the weeks after the RIPE meeting. Finally, he reported that 17 of the larger TLDs (over 10,000 domains) that RIPE NCC served for secondary services had been decommissioned, with 8 still to go. A larger group of 41 now are examined through a survey that has been sent out.

Cooperation WG

Besides the Europol presentation, the most noteworthy item in the Cooperation WG was a comprehensive overview of the Digital Object Architecture or Handle System by ICANN researcher Alain Durand. The Office of the ICANN CTO (OCTO) puts its techie staff to work on a number of study issues, including the DOA. OCTO has been looking into DOA since 2015, has a prefix and operates a handle server.

DOA has been created by internet co-founder Bob Kahn as an alternative to DNS, but according to Durand, is closer to the DNS than to X500 or LDAP. It allows storing and retrieving of data about digital

objects, and does not control communications with physical devices. It is used by the publication industry (to catalogue books & articles), the TV industry (to catalogue assets) and by academic institutions (MPI cataloguing results of experiments).

The DOA is the major architectural project of the Cooperation for National Research Initiatives (CNRI), founded in 1986 by Bob Kahn. CNRI worked on software such as GnuMailman, Python and in the early days gave funding to the ISOC and served as the IETF secretariat. Today, DOA is the main project of CNRI, which nevertheless has established the DONA foundation as governance, standards body for DOA and Global Handle Registry Operator (comparable to the DNS central root).

DONA is based in Geneva and has an MoU with the ITU which according to Durand acts as secretariat. Information about Dona Statutes, minutes from Annual Board meetings and a new "Non proprietary Status of the DOA Architecture" are available on the website.

DONA is working on propagating a system of Multi-Primary Administrators (MPAs). According to the 2016 Board meeting minutes, two new MPA operators joined in 2016, the DOI Foundation and the Communications and Information Technology Commission (CITC) of Saudi Arabia, bringing the number to five, together with CNRI, "GWD G" and "the Coalition".

Durand described the features with persistence and flat hierarchies being the most important, said that so far, there was a lack of client implementations: beside the CNRI Java client, there was a plugin for Firefox, not supported in all Firefox versions.

Durand also said it was not too clear how one could participate or how exactly the process of becoming an MPA looked like.

Comparison of DOA and DNS

	DOA	DNS
Syntax	Dot-separated UTF-8 No length limitation	DNS-on-wire format DNS name format
Bits on Wire	UDP/TCP 2641, HTTP/HTTPS 8000	UDP/TCP port 53, DNS/TLS
Resolution	GHR LHR Replication Caching server Slicing	Root servers Authoritative servers Secondary servers Caching Resolvers Anycast
Data Administration	Per object	Per DNS zone
Data Management	In-band	Out-of-band
Data Objects	Extensible indexed types, predefined or opaque	Defined RR types TBD DOA RR type

Comparison of DOA and DNS: Security and Privacy

	DOA	DNS
Security/ Authentication	DOA clients can force servers to use MD5-based challenge-response authentication	
Automatic Key Rollover Mechanism	Not supported	RFC 5011 ICANN KSK rollover
Privacy	Relying on proxies creates a privacy concern. Deploying DOA clients is difficult. There are no native operating system or browser implementations. Deployment of clients is further hindered by the key rollover issues mentioned above.	Recursive resolvers share the same privacy issues as proxies. However, privacy-conscious users may opt to run their own resolvers.

Comparison of DOA and DNS: Governance

	DOA	DNS
Registration	MPAs	Registries and registrars
Protocol Extensions	DONA	IETF
Policy Development	DONA	ICANN
Operation	DONA/CNRI/MPAs	Root, TLD, and resolver operators

Anti-abuse – Implementation of the EU Network and Information Security (NIS) Directive

Nathalie Falot, legal counsel at Considerati and advisor for the Dutch national cyber security centre on legislation, shared some insight about the choices EU governments currently have to make with regard to the implementation of the NIS Directive. The directive entered into force in August 2016 and has to be implemented within 21 months from that date. Governments in the EU have to establish CSIRTs (if they have not done so already) that will work within the Cooperation Working Group on EU level. Governments need to adopt a national network security strategy and put into place security requirements and breach notification in legislation and supervision. With regard to operators, governments have to provide rule sets for two different kind of operators: operators of essential services (minimum list) and digital service providers (maximum list).

Given the instrument – a directive – governments have some flexibility on how to implement the it and Falot gave two examples of how governments could diverge in implementation. One was on the question of how to organize cybersecurity authorities. The Netherlands has chosen, at least for supervision, a decentralized approach "so the supervisor of the banking sector will also have to supervise on cyber security in that sector. The reason we do this is that we feel that cyber security is not something that should be looked as different from the rest of your working: it's part of your work, it's part of your sector, every sector will have some dependency on cyber security, so the supervisor in that sector should take it into account in its supervisory tasks." But there were other countries going for a centralized cybersecurity oversight.

Secondly, countries vary in how to decide on who is an essential operator. For the Netherlands, this is decided by the legislator. For Germany, for example, operators like the ccTLD registry have to self-identify.

Plenary Bits: Accountability and Diversity

After completing the IANA transition, the RIPE Community started considering its own accountability framework. The main goal was to look for potential "gaps" in accountability mechanisms. Members of the Task Force are Corinne Cath, Hans Petter Holen, Malcolm Hutty, Alexander Isavnin, Peter Koch, Joanna Kulesza, Francesca Merletti, Gregory Mounier, Steve Nash, Nurani Nimpuno, Wim Rullens, Carsten Schiefner and William Sylvester.

The Task Force Members met for their second f2f meeting during RIPE74. So far, discussions on the dedicated mailing list has been quiet. During the Budapest plenary slot on the issue, there was a brief clash of views that illustrated the concern of a potential "bureaucratization" of the so far rather light-weight and informal RIPE processes. Long-time RIPE NCC Research Officer Daniel Karrenberg has criticized the absence of timelines for the work of the Accountability Task Force.

In a related discussion about the future mechanism to select a RIPE Chair, the Chair of the Accountability Task Force, Filiz Yilmaz (Akamai), stepped down after some fierce exchanges on the "RIPE Chair" mailing list.

A mechanism for the future chair selection process is an effort started by current Chair Hans Petter Holen. Holen had been selected by the late Chair Rob Blokzijl who was the first and only Chair since the inception of the RIR. RIPE has obviously not been eager to create formal processes, which is certainly illustrated by the rather awkward WG Chair elections.

In another plenary debate, the Community discussed how RIPE could nurture diversity in the Community. Mirjam Kühne, organizing the session for the RIPE NCC, requested proposals on additional next steps.

The next RIPE meeting will take place in Dubai on 22-26 October 2017

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 54 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn