Council of European National Top Level Domain Registries

Report on

RIPE71

Bucharest

16-20 November 2015

Table of Contents

RIPE71 from 10,000 feet

RIPE is experiencing phenomenal member growth due to the attempt by many parties to become eligible for a little piece of the last /8 IPv4 address block which any newcomer can receive once. While for 36 months the pool had benefited from returned address space, RIPE NCC now projects real runout of old address space in about 5 years from now – given that member growth will not accelerate further or no hidden IPv4 treasures can be found somewhere. The IANA pool will run out in 2019 according to Elise Gerich from IANA (see Address Policy).

The growth brings with it financial benefits, so the organization has been able to lower member fees to €1,400 annually for each member. At the same time the organisation faces change with regard to its composition. “We are no longer an organization of ISPs only,” said Axel Pawlik, Executive Director of the NCC (see Highlights: “Who is RIPE accountable to”). Tahar Schaa representing the German Government in the Cooperation Working Group, and giving the only presentation from the government side, called on the RIPE Community to better reflect that governments were also a “new type of users” of the RIPE system.

With more types of LIRs developing, including government local internet registries (LIRs), there was a need to acknowledge different needs. Pointing to recent changes in the policies of subsequent IPv6 allocations (proposed by the UK government), Schaa said that if RIPE was multistakeholder, the different needs had to be reflected.

The RIPE Community, contrary to the IETF, spent some time discussing the status quo of the IANA transition and while some participants asked for a plan B, there are also those characterizing a potential failure of the transition as a minor nuisance only. A plan B that could mean to take the IP address registry database elsewhere (away from ICANN) has been a topic in several RIPE discussions since the IANA transition started (see Highlights: “The RIPE Community’s take on IANA”).

An update report from the DNSSEC key roll-over design team triggered a heated debate over the shortcomings of current procedures for the KSK roll-over at the root zone. The debate which was continued beyond the DNS WG meeting raised some serious issues (see Highlights: “Roll to disaster”). Perhaps the most important factor influencing the final time plan for the roll could be the IANA transition, an ICANN source said.

The meeting was the first meeting of RIPE in Bucharest. It was attended by 526 participants and it was also the first RIPE meeting ever without former RIPE Chair Rob Blokzijl who passed away on 1 December 2015.

Roll to Disaster: DNSSEC specifications lack specifics for well-formed KSK roll in the root zone

An update report on work concerning the KSK roll in the root zone, presented by Jaap Akkerhuis (NLnet Labs), member of the Design Team, ended in a rant from Geoff Huston (APNIC) on the lack of sound procedures for the rollover. Huston warned that not only was there no well documented process for the planned rollover, but there was nothing in place for an emergency rollover of the KSK. Would the situation of a compromised KSK arise, the root zone managers (and DNS operators) would have to improvise.

RFC 5011 too sloppy?

One issue at stake according to Huston is a lack of specificity in RFC 5011 on "automated updates of DNSSEC trust anchors" which had been added to the suite of DNSSEC documents in 2007 when only a handful of TLDs were signed and preparations to sign the root zone was just under way. (Meanwhile the number of signed TLDs is 951, of which 942 TLDs have trust anchors published as DS records in the root zone; see http://stats.research.icann.org/dns/tld_report/).

Akkerhuis in his update report focussed on RFC 5011 which, according to recommendation #1 of the Design Group, is expected to be the procedure to follow for the roll. The biggest problem according to the experts, Akkerhuis acknowledged, is that 5011 does not include signalling that would allow the root zone managers to check the status quo before and during a roll. This makes it more difficult to measure the impact of the key roll and to, in case of major problems, roll back. It is unclear for example how long a roll-back might be possible given that different resolver implementations might schedule the dropping of the original key differently.

Huston was adamant in his rant: "I am appalled by the DNSSEC standards that came out of the IETF. The description of the way in which you maintain keys, you have a relationship with relying parties, the way you can change the key material at the root, is nonsensical, if it's there at all." There was no emergency key in place and even the planned roll was a "roll to disaster".

With more security mechanisms relying on the DNSSEC signed zone for trust – for example with DANE – the lack of sound procedures was even more serious. Huston was highly critical of the DNS Working Group at the IETF and also of the DNS WG gathered at RIPE (which had urged ICANN to sign the root). He warned that without immediate action "to design a process that minimizes the damage, this is mission impossible."

While the discussion was continued after the end of the official session, there were no conclusions on whether or when to put in signalling features into 5011 or a follow-up RFC.

Next steps for the roll?

The plan for the roll-over of the KSK is not yet completed, Akkerhuis reported. A consultation on the draft plan from the Design Team has been concluded by ICANN with several amendments proposed by just over a dozen commenters. Recommendations made during the consultations include special warnings with regard to the lack of a communication plan to make operators of validating resolvers outside of the inner circle of the DNS community at the RIPE and IETF meetings much more aware, given that failure to roll properly could resolve in failure of DNS resolution.

Experts like Warren Kumari, Chair of DPRIVE WG (Google, but speaking personally) criticized the Design Group for not basing their work on the earlier (2013) considerations for the roll, work seemed to not advance over earlier considerations. At the same time experts seem divided over the timing of the roll. Some of the comments in the ICANN consultation in fact question the need for the roll in the first place, given that there was no issue with the trust for the key.

An algorithm change is not seen as necessary for the time being by the Design Group itself (there have been comments questioning to stay with RSA 2048 instead of exploring the shorter elliptic curve algorithms getting much more en vogue due to their smaller size for the same security level). Postponing the roll once more would allow to prepare to avoid failure, provide measurement and potentially signalling capabilities, says one camp. The other camp warns against a delay and calls at least for a fixed time plan.

An issue for the slow pace to date certainly is the IANA transition which includes a potential change of roles of the root zone maintainer trio. The NTIA, one major force behind the original push to have the root zone signed, might "roll-out"

of its responsibility. With the transition talks in a desperate stretch run at the moment, acceleration of the KSA roll-over could perhaps only be brought about by compromise or by a much more determined fraction of the DNS community.

The RIPE Community's take on IANA

Should the RIPE and the RIR community make an attempt to proceed with the transition of the numbers part of the IANA transition on their own if the naming people cannot get their act together? The question has been raised in the RIR (and the technical community in general) many times starting as early as 2002. At the RIPE meeting the possibility of a "plan B" was again discussed briefly in a plenary section on the ongoing IANA transition work.

On 22 January, the completed accountability proposal (third draft, then passed by the different Supporting Organziations and Advisory Committees of ICANN in the first half of January) is expected to be placed before the ICANN Board of Directors, according to Athina Fragkouli, Legal Counsel of the RIPE NCC. While it has been difficult to ignore the many concerns voiced during the preparatory discussions, for the RIRs January is a hard deadline, she said.

The RIR representatives in the CCWG, according to Fragkouli, told their colleagues that "we cannot go further than that, later than January, because it would jeopardize the IANA transition and we cannot accept that." A further delay of the final proposal, as the RIR community is concerned, could shift the window necessary for the review by the NTIA too far into 2016 to make the September deadline.

It was this calculation that led to the once more raised question about a potential "nuclear option", i.e. a separation of the three IANA functions and a staged transition, with the numbers and the protocols running first. IETF Chair Jari Arkko said, if doing it once again, such a staged, "incremental" transition in his opinion would be a preferential choice - "as in all big IT projects". But the IETF agrees very much with the RIPE NCC officials that for the time being, the process should be completed as is.

Fragkoli reminded the RIPE community on the clear demands from NTIA: "NTIA did say they want nothing else than a complete proposal. If we push it further, if we do not complete, then we are all screwed and the transition will not happen." She also noted that there were "communities out there" that did not share the RIPE community's high interest in completing the transition.

Daniel Karrenberg, CTO of RIPE and member of the IANA transition Coordination Group (ICG) ventured that for the RIPE community there in fact were no big operational concerns in the current IANA oversight system. The RIRs did collaborate on the transition because of the call from the NTIA, but, "frankly I personally think whether it (the ICG proposal) goes through or not is not of life importance. It will not affect us operationally."

The IETF Endowment Fund appeal

IETF Chair Jari Arkko jointly with ISOC's CFO Greg Kapfer presented a plan to the RIPE community to set up an IETF endowment fund of 20 million US Dollar in an effort to get an additional pillar for long-term IETF funding. Currently the IETF budget of around $5.5 million USD annually come from members (40 percent), ISOC (35 percent) and meeting sponsors (25 percent). The endowment idea started 3 years ago with an appeal from former ISOC President Lynn St. Amour, but has not been pursued a lot since. With the big endowment money the standardization body hopes to be able to fund parts of its expenses from the interest. An endowment fund Board would be deciding on how to invest, Kapfer said, control of the money would lie with the IETF.

Many questions were raised during the NCC Services session on the idea. The major one was if ISOC wanted to pull out or decrease their contribution of around $2 million USD or if the IETF wanted to become more independent, also administratively? Arkko and Kapfer said "no" to both questions, the ISOC would remain the organisational home. But the diversification of income sources would give the IETF more "room to manoeuvre", Arkko said. Kapfer said the ISOC would continue funding and had good relationship with the organisation.

Several RIPE community members said the IETF would have to explain much more what was behind the idea of the endowment and also put down figures on paper to make the case.

Further outreach of the IETF to different communities, regions (for the first time the IETF will be hosted in Latin America in 2016, in Buenos Aires) was one of the issues on the IETF agenda for which more money could be needed.

The ongoing IANA transition, new work styles with more intersessionals, a lot of work over GIT, more remote presentations and also the trend of open source becoming mainstream were changing the face of the IETF, Arkko reported.

We just did not call it multistakeholderism – How accountable are the RIRs?

One of the many presentations brought to RIPE's Cooperation WG in Bucharest concerned an investigation into the accountability RIPE (and the RIRs in general) provide for in their policy making processes. Farzaneh Badii gave a quick brief on the questions she and her colleagues at the Humboldt Institute of Internet and Society want to work on.

One major question she said was if accountability mechanisms in the five RIRs had been converging because RIRs just had copied processes developed by one or the other or if it was a natural development towards the most effective model possible. She called the copy-and-paste variant an instance of "institutional isomorphism", but acknowledged that most of the work to even understand how accountability was realized in the different RIRs and whom they wanted to be accountable to and in fact were, was still ahead.

Some members of the RIPE community challenged the suggestion that there was a need for a closer look if accountability (transparency, consultation, evaluation and correction) and multistakeholderism was implemented in RIPE's processes. Nurani Nimpuno, elected as a new NRO Numbers Council member in Bucharest, underlined that RIPE had acted according to the multistakeholder idea before the word even existed. "We just didn't call it multistakeholderism because we weren't inventive enough in coming up with buzz words", she said. Contrary to ICANN, which put a lot of power at the top and then considered procedures allowing to kick those in power out, RIPE policy processes, while continuously shaped over the years, were based on "community empowerment".

RIPE was unique, said Shane Kerr, addressing the questions of differences and convergence of the RIRs as the community and community body preceded the registry and its administration (RIPE NCC).

On the other side, Peter Koch (Denic, but speaking personally) ventured that the study could check on the potential self-referential nature of accountability in the RIR processes. While Working Groups were open, he said, they were not attached to the RIPE NCC, where operational work is done.

Decisions on the RIPE NCC and the registry are in fact taken in closed meetings of the RIPE members. The question of "who is accountable to whom" and "what is the role of those affected by the policies outside of the community of RIPE members" deserves a look.

RIPE NCC CEO Axel Pawlik and Communications Director Paul Rendek welcomed the work. Rendek said he had expected the accountability question coming the RIR's way for some time. With regard to the convergence and similarities of the RIRs there was a lot of window-dressing going on to create the impression of homogeneity, yet that could at times cause some headaches. Pawlik said RIPE NCC would support the effort.

Tahar Schaa, representing the German Government in the Cooperation WG, called on the RIPE Community to acknowledge that governments were a "new type of user" of the RIPE system, and were in fact one of many such new types. Pointing to recent changes in the policies of subsequent IPv6 allocations (proposed by the UK government) Schaa said multistakeholderism, which was a buzz word for how RIPE had worked all along, meant that it had to reflect such needs.

Schaa's talk was the only one by a government representative in the Cooperation WG which seems to be worth noting as it indicates a trend for this WG. Instead of providing a space where governments and the rest of the community can meet up and discuss, it seems the Cooperation WG just looks into regulatory/legislative or Internet governance related developments, without much government participation.

Governments much prefer attending the RIPE NCC government roundtables, which are closed meetings, though. A similar development can be seen in the Anti-Abuse WG, where the Chair usually reports back from meet-ups with Lea outside of RIPE. Ways of intervention for those affected by RIPE policies outside of the narrower community of RIPE members are not very well spelled out or at least are not very well known.

Working Groups and Plenary Bits

DNS Working Group

Rolling, rolling, rolling – Algorithm roll for DNSSEC

RIPE NCC has prepared a roll of the algorithm for its DNSSEC signed zones in order to prevent potential collision attacks documented for the still used Sha1 algorithm (the new algorithm will be Sha 256). The roll also should allow to get some experience with such a roll, Anand Buddhdev from the DNS Team of RIPE NCC reported.

Buddhdev summarized the experiences made when preparing for the roll which has been performed in the meantime for several of the RIPE managed zones. Issues to address were an update of the DNSSEC signer software which did not support signing a zone with two different algorithms. Signer software often had poor or no support for algorithm roll-over according to research done by the RIPE NCC team (for details see RIPE labs article here).

Tests performed (in October) showed the following:

- for the algorithm roll both KSK and ZSK have to be rolled in parallel (contrary to when an algorithm is kept)
- all zone records have to be signed by both keys, the old ZSK, the new ZSK, using the old algorithm and the new one, making the zone and size of the responses larger (according to RFC 6840, "it is an old DS record issue", Buddhdev said)
- before keys can be introduced the signatures have to be introduced, otherwise validation can fail
- old keys and signatures have to be kept in the zone until DS record in parent zone is updated (only after the DS record is updated the old ZSK and its signatures and the old KSK and its associated signatures can be removed
- proceed very carefully (RIPE NCC chose a phased process, rolling the reverse-DNS zone of the RIPE meeting space first, then RIPE NCC internal zone and then the big reverse-DNS zones and forward zones, including e.164.arpa)

Buddhdev also updated the DNS WG on DNS developments in RIPE. The DNS team of RIPE NCC added 17 new anycast servers for K-Root in 2015 (the total number now is 34). Most instances are in Europe, but RIPE NCC also added some in the US and the Middle East. The team used the expansion to bring up software diversity for K-Root servers. Contrary to exclusive NSD version 3 software, Buddhdev and his colleagues added BIND 9 and Knot DNS in addition to NSD 4. To increase diversity for BGP software Bird and ExaBGP both are used, plus both Cisco and Juniper routers are used in parallel to "protect against vulnerabilities in one type of software" (RIPE Labs article on expansion).

RIPE NCC reacted to the start of inter-RIR IP address transfers by updating its provisioning software. The software (in Python) would take input from the RIPE database and input from the other RIRs and merge these into zones to publish them, Buddhdev explained.

With regard to the secondary DNS services for a number of ccTLDs and members of the RIPE NCC there is now a RIPE document on guidelines on how to operate these secondary services (and who is eligible to be served). The document had been reviewed by the DNS Working Group and the community.

Measurements and new DNS software tools

Joao Damas (Bond Internet Systems) looked into the potential "cost" and benefits of leaning more and more to TCP instead of UDP for DNS traffic. The big advantage of TCP was avoidance of spoofing. The research wanted to see if there was any penalty for TCP. Data examined came from two medium-size ISP recursive servers (200 and 400 queries per second throughout the whole period with peaks).

Highlighted issues were the potential of re-using open connections (be careful of the number to avoid using up all your ports!). Mail servers for example could be a service interested in the reuse of open connections, due to frequent que-

rying a permanent connection would be highly beneficial. But in general reuse was not much used.

A potential advantage of TCP could be its tolerance of larger messages (due to more data in DNS, keys and DNSSEC signatures. For NSEC3 instead of NSEC signing, Damas summarized, there was no big problem.

There was a need for more mechanisms of signalling points between end points in DNS.

An earlier study (two years ago) by Geoff Huston et al showed that about 7% of recursive resolvers will not use TCP and around 2% of all users will not get an answer at all.

Ondrej Sury of cz.nic presented a resolver testbed for the Knot resolver. The lab software test called "Deckard" allows simulating "everything on run time". The test scenarios were inspired by Unbound test cases. One test scenario developed allowed to check the functioning of the Jinja2 template for the Knot Resolver. It allows, for example, to try out minimization and the setting of trust anchors. Tests for the authoritative part were available, as well as more complicated examples.

Participation and more test cases for resolvers and even for DNS tools were highly welcome. Deckard would be useful to do more testing of DNS servers, Sury said. "If you have any questions Deckard will answer them", he said.

Marco Davids from SIDN Labs gave a short presentation of ENTRADA, a "small big data platform" that aggregates DNS query data received on the authoritative name server for .nl (roughly 300 gigabyte of data per day, with only 10 percent of all captured by now). Entrada is set-up with a Hadoop environment distributed file system, Parquet for storage and Impala for the interface for querying.

The basic idea was to do research on DNS, also enriching the database with additional sources (geolocation to IP addresses, AS numbers and other information). "We are hoping to build services and applications and disclose all that through user interfaces and APIs", said Davids.

An SIDN internal privacy board will check the applications and SIDN published a privacy framework position paper. "There are quite a few procedures and things like that that we take into account before playing with the data ourselves or even disclose it with other parties such as universities." IP address information will be taken out after 18 months, the rest of the data will stay there indefinitely for now.

Examples of possible research applications include information about the use of a domain for phishing: comparison with phishing alerts showed that ENTRADA could catch the respective malicious behaviour even beforehand. Another project is the "resolver reputation system", which allowed to discover Spambot networks. One could also think about information about who was doing TLSA or Dane, or IPv6.

Xavier Gorjon presented measurements for DNSSEC deployment and sources of DNSSEC failure in an effort to show different sources, where ISPs providing DNSSEC are currently blamed.

Willem Toorop (NLnet Labs) presented a project to replace the system stub resolver with GetDNS allowing to push DNSSEC validation closer to the edge, to the application layer. This would also allow signalling DNSSEC failure. The project emanated from work on a DNS library for application developers at the IETF. So far DNSSEC failure appears as a network failure. GetDNS also implemented parts of the IETF roadblock avoidance draft that lists sources for DNSSEC failure. Features include information about the lack of a DS record in the parent zone, which makes DNSSEC validation unnecessary. The NS switch module provides a DNSSEC-enabled alternative to the system-stub with no need to do anything within the application. DNSSEC roadblocks are avoided and there is DNSSEC failure signalling. Work is ongoing, so the switch module is still experimental.

Toorop also called on participants to comment on a US CERT advisory that premises firewalls should block out port 53.

Jan Vcelák (Cz.nic labs) presented work to implement geographic split-horizon for DNS to allow, for example content providers to match the physical location of his distributed servers to the physical location of the client. The purpose of the developed extension is that the resolver can send signalling the address of the client (or the network of the client) to the server. Cz.nic Labs looked into geolocation support from geoIP DNS, GeoDNS, PowerDNS, gdnsd and the one of its own KnotDNS software, calling GDN the most advanced. For Knot DNS there is a prototype, which supports EDNS-Client-Subnet and DNSSEC (online signing).

Address Policy Working Group – No roll-back of last-mile policy

The address policy WG engaged in a lengthy debate over a proposal to liberalize the last-mile policy of RIPE which currently grants members and newcomers alike one /22 allocation from the last /8 block.

Elvis Velea and Radu-Adrian Feurdean (French Mobile Virtual Operator Coriolis) tabled a proposal to allow allocations of /22 from the last /8 on a recurring basis, every 18th month. The rationale given was that the current policy was unfair to smaller companies who had only small address space portions reserved and no deep pockets to open up new companies/LIRs in order to fetch additional assignments. Velea also pointed to the fact that 36 months after the start of the last-mile policy (handing out one /22 from the last /8 to each member), RIPE still had 99 percent of the equivalent of a /8.

The proposal was rejected by many who argued either that burning the last IPv4 resources faster would be even more unfair to newcomers in the future or that for those begging for an additional /22 (1024 single addresses) no number of addresses would be enough.

RIPE NCC reported that it expected the final runout of IPv4 in about 5 years. Over the last 36 months it had benefitted from allocations of returned IP addresses from the IANA pool, but allocations from IANA will become smaller. Elise Gerich said the IANA pool will runout of IPv4 in 2019. RIPE also had recapped some resources through its clean-up process, which is now very much concluded.

Cooperation WG – Privacy, Export control, Cyberwar

The Cooperation WG this time brought in a number of researchers to discuss regulatory and policy issues of interest to the RIPE community. Participation of governments – the other end of "cooperation" – seems to be dwindling, possibly also due to the ever growing number of IG-related conferences and, perhaps even more, due to the government roundtables organized by the RIPE NCC as closed-door meetings.

Regulatory issues presented briefly in the packed programme included the ongoing privacy legislative efforts in the EU. Valentina Pavel gave an update on the status quo of the EU privacy regulation, the EU-US data protection umbrella agreement and talked quickly on the effects of the Safe Harbour Judgement of the European Court of Justice. The new EU data protection regulation (and the additional directive for data protection by public authorities and law enforcement agencies) were finalized in the trilogue consultations by EU Commission, Council and Parliament on 13 December and passed by the Committee for Civil Liberties (LIBE) on 17 December. The final vote in plenary will be in March 2016.

The umbrella agreement between the EU and the US is an attempt to forge a one-stop shop for all data transfers for criminal prosecution between the two regions. It was paradoxical that the text of the umbrella agreement was finalized (in closed negotiations between the EU Commission and the US) at the same time as the Court in Luxemburg ruled that the US had no adequate data protection level and the Safe Harbour Agreement therefore was invalid, Pavel acknowledged.

While data could currently still be transferred by business between the EU and the US, each transfer after the ruling was open for investigation by European data protection officials in the member states. It was also questionable if a new Safe Harbour Agreement could fulfil the safeguards called for by the ECJ as long as the US continued their mass surveillance programs.

Collin Anderson gave an overview over recent developments in IT export controls. The older 41-member Wassenaar Arrangement (from 1996) was originally focused on arms export controls, but did already include restrictions on exports of encryption and high computing devices. It allows for exports of sensitive (dual-use goods) only when licenses are granted. Items listed in the most recent edition include Computers (category 4 of the arrangement), telecommunications (category 5 part 1), and information security (category 5 part 2).

In 2012 a broader discussion set in about the need to consider surveillance technology for export controls – with the IMSI-catcher for mobile communication surveillance being one of the first technologies to be listed. Additional technology to be added during subsequent Wassenaar update meetings also include IP Network monitoring and intrusion control.

Due to a rapid growth of exports of surveillance technology after the Snowden revelations in 2013, several initiatives started in the EU. While the reform of the regulation EC 248/2009 is proceeding slowly, several European states moved ahead. Germany now lists monitoring centres for lawful interception systems and data retention systems for lawful interception information, when sold to a government), the Netherlands introduced a catch-all clause for exports of all items that will potentially be used to violate human rights and Switzerland bans exports of internet and mobile surveillance technologies "if there 'are reasonable grounds to believe' that the items could be used for repression in the country of destination." Discussion at the EU level are expected to result in the completion of a review of 248/2009 in 2016.

Cyberwar and good old international humanitarian law – A mismatch?

In a combined presentation a group of young researchers from the University of Leiden explored the applicability of international humanitarian law (IHL) to cyber arms conflicts. The threshold of warfare as described in IHL had not been reached so far. Problems with applicability stem from the fact that most attacks so far lack direct physical consequences and identification of attackers is difficult (and therefore it is difficult to distinguish between "international" and "internal" acts of war). So far the threshold set by IHL has not been reached – a minority of legal experts think that a meltdown of the New York Stock exchange resulting from a "cyberattack" could very well be considered an act of "force".

Distinguishability

Once accepted as applicable the problems are only starting. First, the principle that the combatants must distinguish between civilian and military targets contradicts the nature of the net as a connected, dual-use system (worms or viruses used against the "enemy" will spread, e.g. Stuxnet). Hackers also do not wear uniforms – so neither attackers nor targets can be clearly be distinguished as civilians or military.

Proportionality and Precaution

Attacks have to be proportional with regard to collateral damage, according to IHL. What that means with regard to data and networks is still under debate between law makers. While the researchers expressed their preference in having a "specific treaty for cyber warfare" that would be "easier than applying these kind of archaic conventional warfare rules", they do not expect a ban, as cyber warfare could be "less dangerous" for civilians, they proposed. So a new convention "would more than just change the rules and make them very specific to cyber warfare but not be a blanket ban."

Address-Spoofing – Defence or regulation?

In one of the Bird of Feathers (BoF) sessions, Andrei Robachevsky (ISOC) initiated a discussion on next possible steps with regard to IP address spoofing and DDoS attacks resulting from it. Participating operators were divided over focusing on technology or regulation to fix the long-standing problem. Often repeated calls by the operator community to implement BCP38 have not done much to resolve the issue. The problems (lack of incentive to invest to protect other networks) only focusing on expanding capacity to defend one's services against DDoS attacks could result in only large operators surviving in the end, said Gerd Doering (SpaceNet).

Calls to make those not filtering their networks liable is nevertheless still eyed with suspicion, mainly because legislation/regulation tends to miss the intended target, many operators think. Possible technical measures (sFLOW / NetFlow / SPAN traffic monitoring, TTL checks, amplification monitoring, FastNetMon) proposed by Robachevsky were seen as incomplete solutions at best.

In his summary, Robachevsky underlined there was still interest to work on measurements and possible incentives.

Next RIPE meeting: Copenhagen, 23-27 May 2016

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 52 full and 9 associate members – together, they are responsible for over 80% of all registered country code 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