GFCE TRIPLE - I

GFCE Triple-I Panel @RIPE-NCC regional meeting in Almaty, Kazakhstan, 25 September 2018

Summary

On Friday 25 September, during the RIPE NCC Regional Meeting in Kazakhstan, RIPE NCC hosted the GFCE Triple-I Internet Infrastructure Security Panel. The Dutch Ministry of Economic Affairs and Climate as a member of the Global Forum on Cyber Expertise coordinated this initiative to look for ways forward towards more trusted use of Internet and email in the region. The panel included experts from local and global Internet stakeholder groups and was dedicated to finding solutions to strengthen an open end-to-end Internet in the region.

Inclusive and sustainable growth can only be accomplished within a trusted and robust internet ecosystem. The Internet infrastructure is its corner stone, operating based upon a set of core standards and protocols, including TCP/IP Protocol Suite, Domain Name System (DNS) and routing protocols. These layers could be regarded global public goods. The panel was opened by Maarten Botterman, GFCE Triple-I Coordinator. He welcomed the participants in the room and in the panel, and explained the importance of the topic and purpose of the panel: building a future together with justified trust in the use of the Internet and email through implementation of globally available state-of-the-art standards and local multi-stakeholder collaboration in deploying best practices.

Block I: Better Use of Today's Open Internet Standards

First, Hisham Ibrahim (RIPE NCC) talked about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, DMARC, DKIM, SPF and IPv6. All in the room were invited to participate and ask questions or contribute where useful.

DNSSEC and TLS are important in ensuring integrity of routing and of the data exchange itself. DMARC, DKIM and SPF are standards that help prevent email to be easily abused to confuse people with spoofing etc. There are examples of cyber extortion that could have been easily prevented when those standards had been taken into use.

A very good tool to measure the use of these standards by websites and mail servers is the website www.internet.nl. On this website, it is possible to fill in any website or email address to check whether it is up-to-date in its use of these open standards. The website also provides information on where a website fails, and what can be done to resolve this. As announced by the technical supplier (NLnet Labs), the software code will be made available for usage in other countries/regions in the world, within the coming month.

Block II: Inspiration from Good Practice Actions

The second block is the space where inspirational practices and useful ways forward are shared. Prof. Aiko Pras (University of Twente, Netherlands) started with an introduction on a Dutch collaborative initiative to jointly mitigate DDSOS attacks. Following that, 4 panelists (Kristina Hakobyan; Yuriy Kargapolov; Talant Sultanov; Bakhrom Nasirjanov) made short introductions on aspects that they felt require appropriate attention in the region. Bakhrom Nasirjanov talked about his experiences as Internet Service Provider with users on "things that go wrong" when using the Internet, and what they do about it. Kristina Hakobyan explained why awareness raising and education are key in the region, and called for more action on this. Talant Sultanov presented the Taza Koom initiative. And Yuri Kargapolov focused on IoT – the dangers that come with the inevitable deployment of IoT, and what can be done to mitigate those.

Prof. Pras explained what is done in the Netherlands by a consortium of Dutch critical infrastructure operators to better fight DDoS attacks on a national scale. The core of their strategy is a system called the “DDoS radar”, which facilitates a proactive and collaborative DDoS mitigation strategy. It resolves around providers of critical services (e.g., ISPs, banks, government agencies, and hosting providers) continually collecting information on potential and active DDoS sources and automatically sharing this information with each other. The information consists of a digest of the DDoS traffic that a critical service provider needs to handle (a so-called “DDoS fingerprint”). Sharing of fingerprints provides an additional layer of Internet security on top of to the (commercial) DDoS scrubbing services that service providers need to use as well, which separate DDoS traffic from benign traffic. The concept of a DDoS radar was proposed by the University of Twente and SIDN (the .NL Registry) after Dutch banks and government agencies were the victim of multiple DDOS attacks earlier in 2018. The initiative leaders hope that this strategy that may provide true inspiration for initiatives in other countries and regions.

Bakhrom Nasirjanov pointed out that a key problem is the uniqueness of each user and device on the network. By uniqueness it is understood that when you enter the Internet, each user does not have his own individual IP address. This factor allows attackers who pursue different goals, violate the work of ordinary users, causing various kinds of damage. Yet he points out that a better implementation to the global standards of the Open Internet and their competent application, would lead to higher justified trust. IPv6 is important in this, as it makes the structure of the network much easier as you can connect to all devices directly and other benefits. His company is developing a project to implement the IPv6 protocol for mobile data users. The goal of the project is to assign to each mobile device in the IPv6 network addresses, along with IPv4 (which works for NAT). Thanks to this project, it will be possible to improve the security of the network, increase users' trust in the Internet by identifying a specific attacker and improve the quality of the service.

Kristina Hakobyan focused on the user "element" of improving justified trust: digital literacy is key to be able to use the Internet, responsibly and effectively. This includes not only "right-clicking" or code writing, but also searching for information, correctly evaluating it, and more – to have enough skills to protect oneself from Internet threats. Therefore she calls for more attention to raising the level of digital literacy, starting with more attention in the school agenda. But also in dramatically strengthening the training of IT skills for people in all sectors, from archaeologists to actors. In the near future, curricula should also change in universities - towards a larger component of "digital" issues. In addition, there is a lack of people with IT specialties. In a labor market with high unemployment rates, providing training for new jobs to people without jobs is an opportunity. Last but not least, it is necessary to raise the awareness of the elderly audience about the advantages of digital knowledge and digital services, in particular, if and when also government commits to increasing digitization of its services. Opportunities for training are both when exiting the workforce, and through "twinning" – working with young people: a joint teaching time at the computer of "grandparents and grandchildren", where "digitally competent" adolescents act as knowledgeable gurus. As Kristina states: "Digital competence is not just a matter of IT, and not even of the economy as a whole, but is a general social problem – and it should be addressed at all levels."

Talant Sultanov furthered on the need for societies to move towards further digitization, and do so in a responsible way – step by step with increasing cybersecurity. For Kyrgystan, “rudimentary” is the word used by the World Bank in its report to describe the current state of cybersecurity. Whereas over a decade ago Kyrgyzstan was a leader in the region - ahead of Uzbekistan and even Kazakhstan - it is now trailing behind most of the countries in the region. And the trend is not positive. Partly because of national political turmoils since 2005 and constant changes of the government (Kyrgystan had 30 Prime Ministers over 27 years of independence) social and economic conditions suffered. The issue of internet development in general, and Cybersecurity in particular, have not been priorities for the government. As a result, there is now a system where people trust only paper. “Without paper, you are nothing” - loosely translates a popular post-Soviet proverb. If the neighbors are sprinting ahead with digital technologies, Kyrgyzstan still has to get up to speed. Recognizing these challenges, President Atambaev launched a major initiative in 2017 - National Digital Transformation Program Taza Koom (Transparent Society). Prime Minister Sapar Isakov set to implement ambitious projects on digitalization. It included the introduction of interoperability platform Tunduk, based on the latest version of Estonian X-Road platform. Unfortunately the government of Sapar Isakov was forced to resign for political reasons. Talant expressed the hope that the new government will undertake measures to deal with digital challenges, and says that the private sector and civil society stand ready to help. For example, Internet Society-Kyrgyz Chapter plans to open a School on CyberSecurity in the coming months. It would provide trainings the government officials as well as the wider public. A key question during the digitalization efforts is the digital security. People are concerned about personal data, especially biometric data. Government agencies worry about safety of information in databases. The private sector is also reluctant to participate actively due to reservations about the potential of government to keep data safe. In addition, there are global challenges that cannot be ignored when building a digital society. First is the prevention of violent extremism, which can and is being spread through online channels. Second is the commercial and financial data protection. Third is the child security. Last year, there was a wave of teenage suicides related to online game Blue Whale. Forth is the issue of fake news and misinformation. Activities like the GFCE work may help to place the issue of CyberSecurity high in the agenda of decision makers. Talant called for stakeholders to get on board, and suggested that such a comprehensive digital transformation program may benefit more countries in the region.

Yuri Kargapolov shared from his experiences with IoT. A key priority for successful implementation of IoT, in the benefit of the economy and of society at large, is to establish a trusted multi-stakeholder environment to provide an administrative and organizational basis for the management of systems in the communications and Internet industry. There are basically two risks: <1> vulnerability of individual devices themselves for tampering; and <2> wider society faces an increasing threat of large scale ddos attacks launched from large volumes of insecure IoT devices. How to reduce those risks is a high interest topic in many countries and regions. It is important that manufactures, suppliers and users all play a role to ensure adequate security in devices, and in systems consisting of multiple IoT devices working together to deliver specific services. Other important issues to tackle include the unsolved issue of the digital objects' Identity Management and security of the IoT networks including certification issues, reliability and trust properties of the IoT systems. Furthermore there are a lot of dissimilar types protocols and interfaces of the sensors and actuators, and different concepts for development of the basis networks aimed to support IoT. IoT deployment could benefit from better standardization. And last but not least, there is a lack of trained and skilled human potential, and inadequate curriculum due to rapidly changes the practical knowledge, approaches as well as modern theoretical basis. Many issues to tackle, and meetings like the GFCE panel help facilitate coming to solutions. It was also mentioned that ISOC recommends the adoption the OTA IoT Trust Framework as a guideline for safer IoT implementation. In this it is crucial that not all responsibility for security is dumped upon the users/consumers – they often cannot be expected to have the skills and/or means. According to the IGF DC IoT, Internet of Things Good Practice aims at developing IoT systems, products, and services taking ethical considerations into account from the outset, both in the development, deployment and use phases of the life cycle, thus to find an ethical, sustainable way ahead using IoT helping to create a free, secure and rights enabling based environment. How to make this apply to your region is a key concern that has now high political and increasing public interest around the world.

Block III: Planning for a more Trusted Internet

Following the introductions about open internet standards that can help enhance justified trust in use of the Internet and email (Block I) and the examples of good practice provided (Block II) a question and answer session was opened with a focus on the following question:

> *"What to do, together, to improve justified trust in using the Internet and email in the region"*

(1) Learning more from the DDOS Radar initiative, and possibly set up local collaborations to make this work should lead to more reliable networks with better protection to DDOS attacks. It is noted that this would require involvement of all key stakeholders, including government;

(2) IoT comes with many promises, yet it is clear that implementation is currently hindered by a lack of standards, awareness and IT expertise. Building in adequate security from the outset is important. Action to further raise awareness and agree on joint ways forward deserve priority;

(3) Awareness raising and training in IT skills and expertise are seen as crucial in this for development of the region. Adequate risk awareness and security is an important element of this;

(4) In general, there is growing interest in stepping up the speed of digitization of societies in the region. A key element here is to ensure that the systems providing services, collecting and sharing data can be trusted and are protected well against cyber-attacks. Again: real progress is only possible with involvement of all actors.

Conclusions

During the panel session in Almaty, there was a lot of interest in the room for the role of different stakeholders, and the need to work together. A challenge, as there is not an existing tradition of government to work with business, technical community and non-governmental organisations – yet working together was broadly seen as a necessity, as no single stakeholder can do what it takes, alone.

Emphasis was put on awareness raising – both within government, the industry and to the larger public. Without awareness, there is no inclination for collaboration. Learning from practice in other regions may help players in the region to step up. Standing at the beginning of a phase of increasing digitization, it will be crucial to build systems to be secure, by design, so that there can be justified trust in support of further uptake and wider deployment over time.

This was the second of a series of Triple I Workshops that will be organised in different regions of the world. Big thanks to all contributors to this workshop – co-organisers, presenters and participants. The results and outcomes will all be shared on the Triple-I event website.

For more information: maarten@gnksconsult.com.