IGF 2017 Workshop Report

- Session Title: State-led interference in encrypted systems: a public debate on different policy approaches

- Date: December 20th, 2017

- Time: 9h - 10h30

- Session Organizer: Carlos Alberto Afonso, Instituto Nupef, Hartmut Glaser, Diego Canabarro and Jamila Venturini, Brazilian Network Information Center (NIC.br)

- Chair/Moderator: Cristine Hoepers, CERT.br, and Carlos A. Afonso, Instituto Nupef

- Rapporteur/Notetaker: Jamila Venturini and Vinicius Santos

- List of Speakers and their institutional affiliations:

Christoph Steck, Telefonica
Demi Getschko, NIC.br
Estelle Masse, Access Now
Monica Guise Rosina, Facebook Brazil
Neide Oliveira, Federal Prosecution Service, Brazil
Riana Pfefferkorn, CIS Stanford
Seth Bouvier, U.S. State Department
Sunil Abraham, CIS India
Elinor Buxton, government of the United Kingdom
Nina Leemhuis Janssen, government of The Netherlands

- Key Issues raised (1 sentence per issue):

- Multistakeholder approach to the development of policies related to encryption
- Encryption is also used by law enforcement agencies and is fundamental for security
- Open technologies can be used by criminals to develop their own systems
- There are policy options, but the developing world is still discussing proscriptive measures
- Challenges will continue as society gets more digitized and technology evolves, including encryption
- Forcing specific companies/services to restrain the use of encryption puts them in disadvantage in comparison to others
- Private actors are developing mechanisms to fight terrorism and child pornography

- Several governments are reportedly developing hacking techniques and tools in disrespect of human rights
- Weak encryption is worse than no encryption because it leads users to think they are protected
- Different policy options for dealing with encryption may raise legal and technical "interoperability" issues and companies have to adapt to different jurisdictions to remain compliant with the Law
- Over the last century, telcos had to adapt their practices and policies in order to comply with government legitimate requests
- Artificial intelligence can only be trusted if encryption can also be trusted

- If there were presentations during the session, please provide a 1-paragraph summary for each presentation:

The session was structured as a debate with no presentations. Government representatives made their initial intervention sharing their countries' policy approach to encryption and explaining how they were developed. Other participants reacted to those initial statements, making comments, raising concerns and posing questions to the group. Finally, there was a long dialogue between the panel and participants in the audience, who could raise other questions and bring their comments to the floor.

- Please describe the Discussions that took place during the workshop session (3 paragraphs):

The debate focused on possible policy options for encryption and it departed from the perspectives of two different countries: the Netherlands and the United Kingdom. The UK representative presented the updates incorporated to their legislation by the Investigatory Powers Act and a secondary piece of legislation that obliges certain actors to remove encryption or to provide communications in intelligible form in specific cases. She mentioned some challenges to the enforceability of those measures were presented. Additionally, the UK representative reflected upon the issue of overseas "lawful hacking", highlighting the need for requests as such to be necessary and proportionate. In her opinion challenges inherent to those matters tend to remain and increase due to the fact that end-to-end encryption is becoming more popular and terrorist attacks continue to occur.

The representative from the Netherlands declared the country is against any restrictive measure with regards to the availability and use of encryption and has been promoting that position in the European Union. She explained that the Netherlands' position was developed on a multistakeholder basis during a five-year process that involved 140 people from academia, law enforcement agencies, security companies and agents from the intelligence community.

Follow-up discussions focused on different types of threats that could result from weakening encrypted systems. Several of the speakers highlighted the importance of encryption to guarantee the security of communications and basic digital operations in a

connected world. Others focused on a shift from regulating encryption to developing government hacking techniques and the impacts that trend may have to different fields. The debate mostly dealt with the tension between protecting privacy and security through encryption on the one hand and on the other the legitimate interest by law enforcement agencies in accessing private communications to fight crime.

- Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):

There was a call for multistakeholder debate on local discussions around policy options for encryption. Several participants advocated against backdoors, arguing it could weaken the security of the network and of the digital economy as a whole. They defended strong encryption for security and cybersecurity reasons.

One of the speakers suggested that safeguards for individuals and private actors be developed in cases of government hacking as the debate moves from encryption to access to stored data and intervention in devices. Other speaker mentioned that different rules for different players may create different opportunities for businesses, which would be unfair, implying that the same standards should be applicable in order to ensure competition. Another participant brought a concern regarding the "interoperability" of those policies and suggested it is worth considering how different possible approaches might fit together.

During the debate with the audience, several participants pointed out that strong encryption cannot be reconciled with full access to information by governments.

Gender Reporting

- Estimate the overall number of the participants present at the session: 70 in the audience

- Estimate the overall number of women present at the session: Around 20

- To what extent did the session discuss gender equality and/or women's empowerment? None.

- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion: The session didn't address gender equality or women's empowerment issues.