BPF on Cybersecurity 2017 - Call for Contributions

1. **How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?**

   ✓ The Our lives have changed radically, our way of working, mobilizing, communicating on the basis of ICTs and internet technology, based on this new way of life, it is necessary that cybersecurity is hand in hand with each of us in a way systematic and sustainable.
   Each aspect of the implementation of ICTs and internet technologies in its early stages must be accompanied by cybersecurity, it is the way to contribute to growth of its probability analysis, conceptual bases and later on its implementation.
   From my point of view, a way that good cybersecurity can be implemented based on trust for ICTs and internet technologies, is for example with open technologies and / or protocols, with data accessible to those users who use them and who we can carry out some type of monitoring related.

2. **How does poor cybersecurity hamper growth and confidence in ICTs and Internet technologies and their ability to support the Sustainable Development Goals (SDGs)?**

   ✓ Cybersecurity being something that crosses any small or global area, poorly regulated, poorly implemented, poorly controlled, becomes an obstacle to growth and trust in ICTs and internet technologies and sustainable development objectives independently the massiveness of IoTs devices increases exposure, the bases for future generations of a good awareness, actions for people already adult is a good education, for cyber security professionals and their structures, is the constant updating and for the different geographical areas is collaboration and cooperation.

3. **Denial of service attacks and other cyber security issues that affect reliability and access to Internet services**

   ✓ The purpose of denial of service attacks is to render the service unusable. The events we have seen from distributed denial of service (DDoS) attack have increased from recent times, a unified strategy and contingency are some of the points to take into account.
   These events needs to be monitored and nations must play an important role in classification, monitoring and reaction, because depending on the systems that is affected they can be vital for the safety of the main assets, for example an attack of infrastructures considered vital for services to citizens.

4. **The security of mobile devices, which are the vehicle of Internet growth in many countries, and meet critical goals such as payments**

   ✓ Mobile technology has evolved and is growing very quickly fortunately. This also causes costs to fall, use is massive and more people use and connect to the Internet. This is excellent, people who previously could not have access to connectivity today access by means of mobile devices. Cyber-economy is a reality, how to select a product, how to buy it, how to pay it have changed. I wonder if in the future there will be supermarkets or only online. the security measures in the transactional means and contingency are a subject to

protect.

5. **Potential abuse by authorities, including monitoring the use of the Internet, or the use of user-provided data for purposes other than those intended**

- ✓ It is exposed that one of the greatest riches of today and immediate future time are the data, information, the limit between the use and abuse of them, regulation, acceptance, transparent control within the areas that can be applied , the balance between cost and benefit risk analysis, from the scope of a government, an organization and even an individual when manipulating data, it is necessary to respect the decision of the owner of the data, which is only used for the specific purposes that were collected. The amount of information we handle daily, the photos, the chats, the videos and the exposure of our digital identity, lead us to a responsible and safe use of the data.

6. **Confidentiality and availability of sensitive information, in particular in medical and health services**

- ✓ The privacy, availability and integrity of sensitive information, I believe, they are the three pillars to protect (against / from) in critical areas. it is known that there are more pillars to protect, but as mention of some serves.
  The stipulation of targeted attacks, the need to have access to online data, whether for professional review or self-storage,
  The risk exists both internal and external, expose devices, people, community health. Working in the degrees of trust and not only at this point but also in the speed of acting at critical times, are subjects to work hard in the health industry.

7. **Online abuse and gender violence**

- ✓ Personally, I believe that "the things that had happened to using internet" manifests the society in which we live, empowered by impersonality and / or anonymity.
  Violence has always existed, now it is cyber violence, towards the most fragile, towards the weakest.
  The cyber / security / breach we have to work on is giving more tools for people, we all deserve to have access to them possibilities and knowledge. Unfortunately, statistics show that women and / or children are the most affected in cyber-violence, a more equitable global / digital environment, awareness, prevention, education, containment are necessary measures to continue to implement.

8. **Use of the information collected for a particular purpose, being reused for other inappropriate purposes. For example, the theft of information from smart meters, smart grids and the Internet of Things devices for competitive reasons, or anonymisation of data anonymously anonymous citizens**

- ✓ One of the major challenges that we face is the management of information, within the management is the authorized and correct use of the information that has been ceded for its treatment and particular purpose, although, it is true that one loses control of this information it is necessary that companies take controls for the safeguard against our information,

9. The lack of Secure Development Processes combined with immense growth in the technologies that are created and used daily

- ✓ The good practices related to development processes exist, perhaps lacking processes of application of these good practices, perhaps because of ignorance or lack of control. Threats related to technology can be said to be incrementally proportional to its use, from our mobile device, you can get access to everything related to a person and taking the access and subsequent control to your device, access privileged, private information, sharing the same without the person having even a suspicion of the situation, this data can be sold and / or published damaging the honor or exposing it in a negative way.

10. Unauthorized access to devices that become increasingly important in people's daily lives

- ✓ The manifestation of the everyday about unauthorized access or denial of services. This indicates that technology, internet, cybersecurity is part of our daily life in every area of our lives, at home with devices connected to internet IoT; at work when we work with other localities or countries and we perform collaborative work, when we go to dentist and he has our clinical history in the cloud; at school, that our children's notes are on the campus of the academic institution, is our way of communicating with our friends, family, technology is in our daily life.

Nélida Carina Birarda – ISOC Cybersecurity SIG