# IGF 2017 Workshop Report

| | |
|---|---|
| Session Title | **Cybersecurity: Balancing security, openness and privacy (WS 31)** |
| Date | 19.12.2017 |
| Time | 10.10 am - 11.40 pm |
| Session Organizer | Mr. Arsene Tungali - Rudi International / Internet Governance Caucus<br>Mr. Samme - Nlar Tomslin - Consultant |
| Chair/Moderator | Martínez Cervantes Luis Miguel |
| Rapporteur/Notetaker | JoashNtengaMoitui-FAO/IFAD |
| List of Speakers and their institutional affiliations | Duncan Macintosh- CEO, APNIC Foundation<br>Tatiana Tropina - Researcher, Max Planck Institute for Foreign and International Criminal Law<br>Arsene Tungali - Rudi International (Contributed remotely)<br>Michael Oghia - Independent consultant<br>Kai Rehnelt - CEO, SECLOUS GmbH |
| Key Issues raised (1 sentence per issue): | Most of our cybersecurity issues are caused due to trying to combine those three topics: security, openness and privacy<br><br>There is need to explore other alternatives rather than resorting to internet shutdowns<br><br>How do we reconcile efforts by the law enforcement agencies and data privacy advocates?<br><br>Privacy needs to be integrated as part of the data. It is the only way to be able to revoke data at the end, there is need for a paradigm shift |
| If there were presentations during the session, please provide a 1-paragraph summary for each Presentation | **Presentation: Kai Rehnelt - CEO, SECLOUS GmbH**<br><br>Most of our cybersecurity issues are caused due to trying to combine those three topics, leading to a lack of end-2-end protection, weak encryption implementations or even backdoors.<br>We need to treat digital privacy as a human right, with the individual being the one controlling his data.<br>“Openness” can’t mean uncontrolled/unknown access to our data, instead we have to establish an access control requiring multiple trusted parties to grant access to our data if needed.<br><br>A paradigm shift is needed on how we protect our data, as todays data protection mechanisms reminds of the middle ages (building electronic walls around the data which need to be removed if data has to be processed, with a digital form of a yes/no access control to verify whether I’m allowed to enter/access my data). We must integrate the protection within the data itself and get rid of todays old-fashioned authentication methods.<br>One key aspect of future data protection is enabling users to actively revoke previously shared data (not hoping that a provider will perform the revocation request - as today).<br>Individual (data) privacy will be essential to improve cybersecurity, but also an enabler for future business models(e.g. generating an income by selling parts of the individual data record).<br><br>**Presentation: Duncan Macintosh- CEO, APNIC Foundation**<br>The technical community plays an important role in cyber security, particularly in the area of training and capacity building. This includes ISPs (network engineers); CERT/CSIRTS (security specialist); and law enforcement. All of theseplayers face different challenges including growing connectivity and bandwidth being provided to small communities to the many different players and their different agendas, especially in the development space. |

| | |
|---|---|
| | The technical community seeks to encourage collaboration and cooperation as a key cyber security strategy.<br>Law enforcement has aparticular interest in technical processes. Ipv6 – for example - presents a situation where every device will have a unique address and the implications of this will be discussed this morning.<br><br>In cybersecurity, we need to bring people from all fields, technical, civil society and law enforcement together as different stakeholders. These multi stakeholder groups are passionate about security, and need to be talking to each other. We cannot have a robust cyber security space until we ensure the privacy and security of the users and networks.<br><br>Building trust between the private sector and intermediaries, civil society and advocacy groups, the corporate sector and law enforcement groups requires them to understand each other perspectives. They have to co-exist.<br><br>It takes trust and transparency to ensure that we are able to solve the security problems we face. How do we build trust, transparency and connect all stakeholders to be able to have successful security dialogues?<br><br>**Presentation: Michael Oghia - Independent, consultant.**<br><br>Privacy and security is not a black and white, good and bad issue. We need both. Any party that frames the relationship between privacy and security as mutual exclusive and unwinnable is lazy. What's harder is building trust. Talking to each other does nothing. Various Internet governance actors and stakeholders need to work together to build trust and generate meaningful, creative, inclusive, and effective solutions. Transparency and collaboration are key to this process. He also stressed that civil society especially should not demonize or vilify law enforcement agencies, as they "are not simply the enforcement arm of big brother". |
| Please describe the Discussions that took place during the workshop session: (3 paragraphs) | **Intervention from remote: Arsene Tungali - Rudi International on Internet shutdowns**<br><br>There should be no reason for shutting down the internet. There are many cases, where this is happening in Africa mainly when ordered by governments. Internet shutdowns cannot solve the problem of fake news. We anticipated internet shutdowns internet in Kenya and in Ghana during elections.<br><br>There are alternatives to addressing the incidents. There ought to be other alternatives to shutting down the internet. If we have to save lives, governments should be able to save lives using other ways at their possession, not through Internet shutdown.<br><br>Kenya has a very liberal constitution and government respects the rights of citizens. There is a focus on various accounts, rather than shutting down the internet. Finding right alternatives and shutting down is no option.<br><br>There is a need to be brave enough to change things and therefore the need to bring together the different parties (stakeholders) to define the right solution.<br><br>But rules are not followed, information is abused and we need to find solutions to this problem.<br><br>**Digital Privacy as a Human Right**<br>Most of our cybersecurity issues are caused due to trying to combine those three topics, leading to a lack of end-2-end protection, weak encryption implementations or even backdoors. We need to treat digital privacy as a |

| | |
|---|---|
| | human right, with the individual being the one controlling his data. “Openness” can’t mean uncontrolled/unknown access to our data, instead we have to establish an access control requiring multiple trusted parties to grant access to our data if needed. A paradigm shift is needed on how we protect our data, as todays data protection mechanisms reminds of the middle ages (building electronic walls around the data which need to be removed if data has to be processed, with a digital form of a yes/no access control to verify whether I’m allowed to enter/access my data). We must integrate the protection within the data itself and get rid of todays old-fashioned authentication methods.<br>One key aspect of future data protection is enabling users to actively revoke previously shared data (not hoping that a provider will perform the revocation request - as today). Individual (data) privacy will be essential to improve cybersecurity, but also an enabler for future business models(e.g. generating an income by selling parts of the individual data record).<br><br>**Data literacy**<br>There are many people who do not understand what data is and why privacy is required. People are concerned about internet access but do not understand data privacy. It takes a lot of training for even political actors to understand data privacy.<br><br>**Interception**<br>How do we reconcile between law enforcement and data privacy advocates? It is important for consumers to understand that there is a party both at the end point or at the network. Interception was implemented at a time when hacking was not put in as a priority. However, anything on the web was put under legal justice. The possibility of detecting the interception is decreasing and becoming more difficult. How can we find a compromise between the two communities? What are the procedures for interception in different countries? There are many safeguards to intercept emails. Germany issued a call called "bermudas triangle in June" that allows, government hacking on information. The German case is not well balanced. In France to intercept email, the crime has to be with more than 3 years of prison punishment and<br>It is important to start trusting law enforcement, but there is no need to mix intelligence and interception. The cybersecurity debate is increasing becoming of importance. |
| Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs) | 1) There is need for training to understand data privacy. Mandatory privacy and information management training for government employees and contractors and service providers may be one way to conduct training. This kinds of training provide an understanding and support personal information and privacy awareness, handle personal and confidential information responsibly and prevent information incidents in the workplace, including privacy breaches<br>2) In cybersecurity, we need to bring people from all fields, technical, civil society and even law enforcement are required to bring all stakeholders on board. Multi Stakeholder groups passionate about security, need to be talking to each other. We cannot have a robust cyber space until we have privacy and security of the users and networks.<br><br>3) Switching off the internet is no option – however we need to be prepared to handle the existing and future challenges (e.g. caused by fake news) |

**Gender Reporting**

- ✓ Estimate the overall number of the participants present at the session:

**50 Participants in the session**

- ✓ Estimate the overall number of women present at the session:

  **9 Women in the session**

- ✓ To what extent did the session discuss gender equality and/or women's empowerment?

  **N/A**

- ✓ If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion

  **N/A**