FUTURE OF THE INTERNET POSSIBILITIES, PROBLEMS, OPPORTUNITIES AND OBSTACLES

INTERNET CAUGHT IN THE MIDDLE.

PAYMENT SERVICE DIRECTIVE 2

- **PRO**
  - **Financial Control.**
  - **Security.**
  - **Increased competition.**
  - **Fraud reduction.**
  - **Innovation.**

- **Transform banking.**
- **Improve PISP and ASIP.**
- **FinTec, Google, Alibaba.**
- **Stronger user authentication.**
- **Boost Blockchain and Bitcoin.**

- **CON**
  - **Ethics.**
  - **Cybercrime**
  - **Social Engineering.**
  - **Compliance.**
  - **Privacy.**

- **Can you trust TTP, profiling.**
- **New attack vectors, legacy IT**
- **More attack vectors, phishing**
- **Who is responsible. TTP – Bank?**
- **Will customer understand?**

THE INTERNET OF EVERYTHING - 2020

- Global Internet traffic will be **92 times** greater than in 2005
- Global Internet users **4.1 BN** – 52% global population
- The gigabyte equivalent of all the movies ever made will cross global IP networks every **two minutes**
- More than **26 billion** global IP networked devices or connections (up from 16.3 billion in 2015)
- More than **12 billion** global M2M connections (up from 4.9 billion in 2015)
- More than **600 million** global wearables (up from 96.7 million in 2015)
- Global social media users **2.8BN**
- More than **3.1 billion** global Internet-enabled TVs (up from 1.8 billion in 2015)
- **66% of global IP traffic** will come from wireless access technologies (up from 48% in 2015)
- IP traffic will **grow three-fold** from 2015-2020, reaching an annual run rate of 2.3 Zettanbytes (up from 870 Extabytes in 2015)
- The average Internet user will generate **44.1 gigabytes** of traffic per month (up from 18.9 gigabytes in 2015)
- 90% of the world's data was created in the last 2 years. Experts predict a **4,300%** increase by 2020
- Every day, we create **2.5** quintillion bytes of data

THE HYPERCONNECTED REALITY 2020

- IoT connected via cars, home, work, public space, medicare, boats, phones, TV
- The development in battery power and 'air' charging will fuel more sensors communicating with the above IoT tools
- More voice and face recognition. More 'smart' cities.
- Move from PC to mobile (5G) predominantly in 3rd World
- Big data fuels automation and ML and AI will offer new services
- Huge data repositories deployed in cloud. Who owns the data. Who have access?
- Balkanization of the Internet

DIFFERENCE BETWEEN ON-OFFLINE CRIME

- All normal crime regulation worldwide is based on the classic geographical judicial principle covering crime done in a defined jurisdiction (land/see/air) and the perception that in most crime the victim and perpetrator are in proximity.
  - **Proximity**: Criminals do not need to travel to a country to conduct crime
  - **Scalability**: Criminals can rob millions of computers in seconds without travelling – in physical world you rob one bank at a time
  - **Attribution**: It is easy to hide. Encryption, Bullet proof hosting etc.
  - **Expertise**: You do not need to be an expert to be a cybercriminal. Crime as a Service is designed to facilitate crime and operate with SLA's
  - **Prosecution**: Risk extremely low, no real LEA cooperation in this field

- ***All indicators point to surging crime based on the above factors.***

ONLINE CRIME ATTACKS FROM ANYWHERE, AT ANYTIME AGAINST ANYBODY

- **The global crime factory**:
  - Very resourceful
  - Still mainly Russian speaking in the development end of the chain
  - Have all competences in-house and work seamless with others (coding, translating, bots, implement, attack, mules, ml capabilities etc)
  - Blurred lines to Nation State activity
  - Heavy use of Dark and Deep Net to explore, exploit and communicate
  - Work flawless together and competition low
  - Utilize automation, AI and ML and have no legal constraint
  - Based on the 3 normal (business/market) assessment criteria they are running smooth: (low)**Investment** – (high)**Profit** – (minimal)**Risk**

THE SURGING CYBER CRIME FUELLED BY MORE VICTIMS, LOW INVESTMENT, HIGHER PROFIT, AND LIMITED RISK

- Estimated total financial losses due to cybercrime between **450 and 608 BN USD** in 2017
- **90,1 BN** cyber security events in 2017 – 1 MN per second!
- Every hour, every day **480.000** identity records stolen
- Every second we globally send 2 MN mails – **49 % are scam**
- 60% attacks are malware driven
- 40% attacks are malwareless!
- Surging **Ransomware** attacks focus on Healthcare, academia, retail and other soft targets
- **DDoS** attacks increased **91%** in 2017 thanks to IoT
- With DDoS for hire services, criminals can now attack and attempt to take down a company for **less than $100** and IoT supported firepower over **1TBps**
- Rapid development of dangerous second generation **Wipe Malware** is concerning (Shamoon2)
- The result of trickle-down in the field of cyber security has been a proliferation of military-grade weaponry for cyberwarfare being pushed down into the masses and commoditized

WHAT SEEMS TO BE THE PROBLEM?

- We are fighting 21 century crime with 19 century legislation
- The Internet makes crime relatively simple due to easily accessible tools provided on Deep Net as Crime as a Service
- Deterrence difficult. No Risk no crime reduction
- The rapid development of the Internet and new tools are done without building in security by design
- Attack vectors multiply and awareness of (new/old) users of Internet tools at a very low level
- Lack of competence/capacity in the overall security environment
- **The Elephant in the room:** No trust between Nation States, Law Enforcement and no cooperation in any field to prevent, protect and prosecute cybercrime. Counter Intelligence and 'spy' activity in cyberspace is confused with ordinary/organised crime against the average population, business, academia and governments

MY PREDICTION.

- **CRIME WILL SURGE.**
- **SO WILL COOPERATION**
- **PPP WILL BE KEY AND CRUCIAL – BALANCE SECURITY/PRIVACY**
- **PRIVACY UNDER PREASURE – WE WILL LIVE WITH TRANSPARENCY**
- **AWARENESS WILL IMPROVE**
- **TECH INEQUALITY**
- **NORMS WILL BE ESTABLISHED.**