Cyber security and Cybercrime
Background & Global outlook

Jan KERKHOFS

Council of Europe Expert
Federal Magistrate, Federal Prosecutor’s Office, Belgium

jan.Kerkhofs@just.fgov.be

Addis Ababa, Ethiopia, 11-12 April 2018
Cyber Security and cybercrime: hand in hand

Cyber Security
Prevention
Policy
Malabo
Convention

Cybercrime
Repression
Judiciary
Budapest
Convention
Cyber Security

- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by (cyber) criminals.

Cybercrime

- Criminal activities carried out by means of computers or the Internet (Oxford Dictionary).
- Computer crime, ICT crime, high tech crime, computer/ICT/high tech enabled crime, ...
**Cybersecurity** addresses
SECURITY/ TRUST/ RESILIENCE/ RELIABILITY

<table>
<thead>
<tr>
<th>Non-intentional ICT security incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disasters</td>
</tr>
<tr>
<td>Technical Failures</td>
</tr>
<tr>
<td>Human Failures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intentional attacks against ICT by</th>
</tr>
</thead>
<tbody>
<tr>
<td>State actors</td>
</tr>
<tr>
<td>Non-state actors</td>
</tr>
<tr>
<td>Terrorists</td>
</tr>
<tr>
<td>Criminals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Critical Infrastructure Attacks</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Offences by means of ICT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frauds</td>
</tr>
<tr>
<td>Child exploitation</td>
</tr>
<tr>
<td>Terrorist use of ICT</td>
</tr>
<tr>
<td>IPR-offences</td>
</tr>
<tr>
<td>Extortion</td>
</tr>
<tr>
<td>Etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Offences involving ICT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any offence involving electronic evidence</td>
</tr>
</tbody>
</table>

**Cybercrime** (tit. 1-2 of Budapest Convention) covers
RULE OF LAW/ CRIMINAL JUSTICE/ HUMAN RIGHTS

- Offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computer data and systems, including illegal access, illegal interception, data and system interference, misuse of devices, offences committed by means of computer systems. This list is limited to those ‘old’ forms of crime that obtain a new quality through the use of computers, that is, computer-related forgery and fraud, child pornography and offences related to infringements of copyright and related rights on a commercial scale.

Source: Council of Europe, Cybercrime strategies, March 30th 2012
What is at stake? - Critical infrastructures
• 3500 BC: the abacus

• 1820: the first cybercrime!

• 1978: first spam-mail via Arpanet

• 1982: the first virus installed on an Apple
• 1969 – ARPANET
  – Militaire Advanced Research Projects Agency (ARPA) – cold war
  – Dynamic Rerouting

• The first step in cyberspace:
  – “That's one small step for a man, one giant leap for crime.”

• Build so it can not be blocked or seized
A brief history

ARPANET anno 1974

www.coe.int/cybercrime
How the internet works: dynamic rerouting
How the internet works: dynamic rerouting
• A part of the daily life of the citizens
  • workplace,
  • home
  • most of the leisure moments

• There is no physical distances between people in different places in the world

• Political frontiers are indifferent to the cyber world
Information Society

• Information is open and available to everybody
• No States sovereignty
• Cyberspace is independent, anarchic and unгovernable
• It is everywhere and it is nowhere
• Any person can express himself
Internet of things (IoT)
• Around 40% of the world population has an internet connection today. In 1995, it was less than 1%.

• The number of Internet users has increased tenfold from 1999 to 2013.

• The first billion was reached in 2005. The second billion in 2010. The third billion in 2014.
Annual growth

**Internet Users**: +10% since Jan 2016, +354 million

**Active Social Media Users**: +21% since Jan 2016, +482 million

**Unique Mobile Users**: +5% since Feb 2016, +222 million

**Active Mobile Social Users**: +30% since Jan 2016, +581 million

**Sources**: Population: United Nations; U.S. Census Bureau; Internet: Internet World Stats; ITU; Internet Live Stats; CIA World Factbook; Facebook; National Regulatory Authorities; Social Media and Mobile Social Media: Facebook; Tencent; Vontaktel; LiveInternet.ru; Kakao; Naver; NIK; Aghaaj; CafeBazaar; SimilrWeb; Ding;

*Extrapolation of the data: Mobile: GfK Intelligence; Extrapolation of Emarketer and Erosion Data: Comparisons to We Are Social’s “Digital in 2015” report.

Quarterly growth

AUG 2017
QUARTERLY GROWTH
CHANGE IN KEY STATISTICAL INDICATORS IN THE PAST QUARTER

INTERNET USERS

+0.2%
SINCE APR 2017
+8 MILLION

ACTIVE SOCIAL MEDIA USERS

+4%
SINCE APR 2017
+121 MILLION

UNIQUE MOBILE USERS

+2%
SINCE APR 2017
+92 MILLION

ACTIVE MOBILE SOCIAL USERS

+3%
SINCE APR 2017
+82 MILLION

https://www.slideshare.net/wearesocialsg/global-digital-statshot-q3-2017
Internet Use: Regional overview

INTERNET USE: REGIONAL OVERVIEW
INTERNET USERS (IN MILLIONS), AND INTERNET PENETRATION, BY REGION

EAST ASIA: 923 (57%)
SOUTH ASIA: 505 (33%)
AFRICA: 362 (29%)
WESTERN EUROPE: 353 (84%)
SOUTHERN EAST ASIA: 339 (53%)
NORTH AMERICA: 320 (88%)
EASTERN EUROPE: 284 (67%)
SOUTHERN AMERICA: 281 (66%)
MIDDLE EAST: 147 (60%)
CENTRAL AMERICA: 117 (53%)
CENTRAL ASIA: 33 (48%)
OCEANIA: 28 (68%)

SOURCES: INTERNETWORLDSTATS; INTERNATIONAL TELECOMMUNICATION UNION (ITU); INTERNETLIVESATIS; CIA WORLD FACTBOOK; FACEBOOK; NATIONAL REGULATORY AUTHORITIES.
Time spent on the Internet

Average number of hours spent using the Internet per day, split by computer use and mobile phone use (Survey Based)

Note that times can be added together to find total Internet time by country, rankings are in order of total time spent using the Internet each day.

Sources: GlobalWebIndex, Q3 & Q4 2016, based on a survey of internet users aged 16-64.

Social Media use

**SOCIAL MEDIA USE**

Based on the monthly active users reported by the most active social media platform in each country.

- **Total number of active social media users**: 3.028 billion
- **Active social users as a percentage of the total population**: 40%
- **Total number of social users accessing via mobile**: 2.780 billion
- **Active mobile social users as a percentage of the total population**: 37%

*Hootsuite* - [Source](https://www.slideshare.net/wearesocialsg/global-digital-statshot-q3-2017)
Active Users by Platform

https://www.slideshare.net/wearesocialsg/global-digital-statshot-q3-2017
Time spent on Social Media

JAN 2017

TIME SPENT ON SOCIAL MEDIA
AVERAGE NUMBER OF HOURS THAT SOCIAL MEDIA USERS SPEND USING SOCIAL MEDIA EACH DAY [SURVEY BASED]

PHILIPPINES
BRASIL
ARGENTINA
MEXICO
UNITED ARAB EMIRATES
MALAYSIA
EGYPT
TURKEY
SPAIN
ARABIA
SOUTH AFRICA
THAILAND
VIETNAM
INDIA
RUSSIA
SINGAPORE
UNITED STATES
ITALY
CHINA
UNITED KINGDOM
CANADA
POLAND
HONG KONG
SPAIN
AUSTRALIA
FRANCE
SOUTH KOREA
GERMANY
JAPAN

SOURCES: GLOBALWEBINDEX, Q3 6 Q4 2016. BASED ON A SURVEY OF INTERNET USERS AGED 16-64.

The regional African situation

AFRICAN COUNTRIES BY REGIONAL REPORT

NORTHERN AFRICA
- Algeria
- Egypt
- Libya
- Morocco
- Sudan
- Tunisia
- Western Sahara

WESTERN AFRICA
- Benin
- Burkina Faso
- Cabo Verde
- Côte d’Ivoire
- Ghana
- Guinea
- Guinea-Bissau
- Liberia
- Mali
- Mauritania
- Niger
- Nigeria
- Saint Helena
- Senegal
- Sierra Leone
- Togo

MIDDLE AFRICA
- Angola
- Cameroon
- Central African Republic
- Chad
- Dem. Rep. of the Congo
- Republic of the Congo
- Equatorial Guinea
- Gabon
- São Tomé & Príncipe

EASTERN AFRICA
- Burundi
- Comoros
- Djibouti
- Eritrea
- Ethiopia
- Kenya
- Madagascar
- Malawi
- Mauritius
- Mayotte
- Mozambique
- Réunion
- Rwanda
- Seychelles
- Somalia
- South Sudan
- Tanzania
- Uganda
- Zambia
- Zimbabwe

SOUTHERN AFRICA
- Botswana
- Lesotho
- Namibia
- South Africa
- Swaziland

• New illegal activities are being “invented” everyday
  • within the networks
  • using the networks
  • against the networks

• A global crime

• Always multiple territorial connections
  • the action of the criminals reach computers and victims in countries other than their countries
  • inherent to the nature of cybercrime
  • because of the expansion of the networks it is impossible, to each country, to act alone against this problem
• Crimes are committed remotely
  • Evidence is volatile and often on the “cloud”
  • National law enforcement agencies are limited to their geographical borders
    • International assistance in criminal investigations require proper legal channels
    • No jurisdiction online, if outside national borders
    • International cooperation deals with very distant countries with different cultures, with different legal tradition and different criminal law frameworks
# How criminals use Technology

<table>
<thead>
<tr>
<th>TECHNOLOGY AS A VICTIM</th>
<th>Traditionally considered to be true “computer crime” and involves such offences as hacking, denial of service attacks and the distribution of viruses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TECHNOLOGY AS AN AID TO CRIME</td>
<td>Computers and other devices are used to assist in the commission of traditional crimes, for example, to produce forged documents, to send death threats or blackmail demands or to create and distribute illegal material such as images of child abuse.</td>
</tr>
<tr>
<td>TECHNOLOGY AS A COMMUNICATION TOOL</td>
<td>Criminals use technology to communicate with each other in ways which reduce the chances of detection, for example by the use of encryption technology</td>
</tr>
<tr>
<td>TECHNOLOGY AS A STORAGE DEVICE</td>
<td>Intentional or unintentional storage of information on devices used in any of the other categories and typically involves the data held on computer systems of victims, witnesses or suspects</td>
</tr>
<tr>
<td>TECHNOLOGY AS A WITNESS TO CRIME</td>
<td>Evidence contained in IT devices can be used to support evidence to which it is not obviously related, for example to prove or disprove an alibi given by a suspect or a claim made by a witness.</td>
</tr>
</tbody>
</table>
Europol IOCTA – key findings

- RANSOMWARE - MALWARE
- ONLINE CHILD SEXUAL EXPLOITATION
- PAYMENT FRAUD
- SOCIAL ENGINEERING
- DATA BREACHES AND NETWORK ATTACKS - DDOS
- ATTACKS ON CRITICAL INFRASTRUCTURES - DDOS
- CRIMINAL ACTIVITIES ONLINE – ONLINE CRIMINAL MARKETS
- BIG DATA, IOT AND THE CLOUD
- TERRORISM
A few examples: cybercrime and threats today
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

[Bitcoin Address]
WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

Most first encountered ransomware after an outbreak shut down hospital computers and diverted ambulances this year. Is it here to stay?

Alex Hem
@alexhem
Sat 30 Dec 2017 05:00 GMT

For thousands of people, the first time they heard of “ransomware” was as they were turned away from hospitals in May 2017.

The WannaCry outbreak had shut down computers in more than 80 NHS organisations in England alone, resulting in almost 20,000 cancelled appointments, 600 GP surgeries having to return to pen and paper, and five hospitals simply diverting ambulances, unable to handle any more emergency cases.
How to make money on the internet

Information via Phishing

Sell the information

Social Engineer

Malware creator

Malware user

Data seller
**30.04.2003: Fresh arrivals - a thousands of Gold, Platinum, Business, Corporate dumps from Europe, Caribbean, Japan, Asia, Australia. You can select it by Bin, bank, country, type from here.**

You have to stay in minimum quantities mentioned in the batches below, we can’t sell dumps by units.

<table>
<thead>
<tr>
<th>Availability</th>
<th>Description</th>
<th>Country</th>
<th>Dumps per batch, pieces</th>
<th>Cost per batch, $ USD</th>
<th>Cost per unit in batch, $ USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>MC unsorted (incl. Gold etc.)</td>
<td>unsorted</td>
<td>10,000</td>
<td>8000.00</td>
<td>0.89</td>
</tr>
<tr>
<td>Available</td>
<td>Visa unsorted (incl. Gold etc.)</td>
<td>unsorted</td>
<td>10,000</td>
<td>8000.00</td>
<td>0.89</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Classic Debit</td>
<td>USA</td>
<td>100</td>
<td>595.00</td>
<td>5.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Classic Credit</td>
<td>USA</td>
<td>100</td>
<td>595.00</td>
<td>5.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Classic unsorted</td>
<td>USA</td>
<td>100</td>
<td>595.00</td>
<td>5.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Gold Debit</td>
<td>USA</td>
<td>40</td>
<td>1198.00</td>
<td>29.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Gold Debit</td>
<td>USA</td>
<td>100</td>
<td>2495.00</td>
<td>24.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Gold Credit</td>
<td>USA</td>
<td>40</td>
<td>1198.00</td>
<td>29.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Gold Credit</td>
<td>USA</td>
<td>100</td>
<td>2495.00</td>
<td>24.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Gold Credit</td>
<td>USA</td>
<td>40</td>
<td>1198.00</td>
<td>29.95</td>
</tr>
<tr>
<td>Available</td>
<td>Visa Gold unsorted</td>
<td>USA</td>
<td>100</td>
<td>2495.00</td>
<td>24.95</td>
</tr>
</tbody>
</table>
Phishing – social engineering
The cybercrime threat map

Success factors

- Cyber security policy – Cybercrime legislation – legal framework
  - CERT – Cyber Emergency Plan
  - Malabo Convention, 2014
  - Budapest Convention, 2001
- Capacity building
  - Skill and competence development
- Research and development
- International cooperation
Questions?

In this corner, we have firewalls, encryption, antivirus software, etc. And in this corner, we have Dave!!

www.coe.int/cybercrime
Thank you

Jan KERKHOFS
Council of Europe Expert
Federal Magistrate, Federal Prosecutor’s Office, Belgium

jan.Kerkhofs@just.fgov.be

Addis Ababa, 11-12 April 2018