Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Introductory Judicial Training Course on Cybercrime and Electronic Evidence

Session 2.2
Substantive Provisions of the Budapest &Analogous Provisions of the Malabo Convention - Part 1

Jennifer Mensah (Mrs.)
Cybersecurity and Data Privacy Legal Practitioner
National Communications Authority

Council of Europe

Jennifer.mensah@nca.org.gh

9th November 2021

Session contents

1. Definitions
2. Illegal access
3. Illegal interception
4. Data interference
5. System interference
6. Misuse of devices

Session aim

To provide the participants with a comprehensive understanding of the elements of offences against the confidentiality, integrity and availability of computer systems and data, established in accordance with the Budapest Convention.

Session objectives

By the end of the session, delegates will be able to:

- Understand the meaning of fundamental terms such as:
  - computer data
  - computer system
  - traffic data
  - service provider
- Identify the elements which constitute the offence of:
  - Illegal access
  - Illegal interception
  - Data interference
  - System interference
  - Misuse of devices

BUDAPEST AND MALABO CONVENTION

Budapest Convention (Convention on Cybercrime): Opened for signature in Budapest in 2001. 65 Countries have ratified the Budapest Convention including Ghana

Malabo Convention (African Union Convention on Cybersecurity and Personal Data Protection): Adopted by African leaders in 2014 at a meeting in Malabo, Equatorial Guinea. Out of the 55 Countries in Africa, 14 have signed, and 8 have ratified including Ghana

Section 1

Substantive Provisions of the Budapest Convention (Part 1)

DEFINITIONS

Computer System

"**computer system**" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

Device consisting of hardware and software which automatically processes computer data

Device can be standalone or connected in a network

Includes:

- Input devices
- Output devices
- Storage facilities

Computer data

"**computer data**" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

Computer data is any data that is in a form that can be directly processed by a computer system

Computer data that can be automatically processed may be the target of the criminal offences defined in the Budapest Convention or the object of the application of the investigative measures defined by the Budapest Convention

Service provider

"**service provider**" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Yes:

- communication or related data processing services (e.g. hosting and caching providers)
- private & public entities
- free or paid services
- provision to closed group or public

No:

- content providers

Traffic data

"**traffic data**" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Yes:

- category of computer data
- generated by computer that formed part in chain of communication
- Indicates communication’s:
  - origin
  - destination
  - route
  - time
  - date
  - size
  - duration
  - type of underlying service

No:

- content of communication

Poll question

Which of the following are NOT included in traffic data:

A. Time
B. Duration
C. Content
D. Subject heading
E. Size of a communication

The correct answers are C and D

Poll question

Which of the following is NOT included in subscriber information:

A. Address
B. Content
C. Email address
D. Credit card information
E. Cell phone number

The correct answer is B

WHAT IS CYBER CRIME?

How would you define Cybercrime?

Computer crime, or **Cybercrime**, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. **Netcrime** is criminal exploitation of the Internet

Wikipedia

“The criminal abuse of technology is commonly referred to as *cybercrime* and includes:

- offences aimed at computer systems and data such as hacking,
- traditional offences such as drug trafficking or fraud committed or facilitated with the use of technologies, activities concerning content;
- where technology is used in the making and dissemination of illicit materials”

GLACY Manual on international cooperation on cybercrime and electronic evidence

- Cybercrime (offences against the network, computers, program or data)
  - Offences against the confidentiality, integrity and availability of computer data and systems
  - Computer-related offences
  - Content-related offences
  - Offences related to intellectual property rights and similar rights
- Criminal use of the Internet to commit traditional crime
- Not everything is a Cybercrime

ARTICLE 25 (1) MALABO CONVENTION…”

Legislation against cybercrime: Each state party shall adopt such legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. State Parties shall take into consideration the choice of language that is used in international best practices.

Section 2

Substantive Provisions of the Budapest Convention (Part 1)

ILLEGAL ACCESS

Illegal access

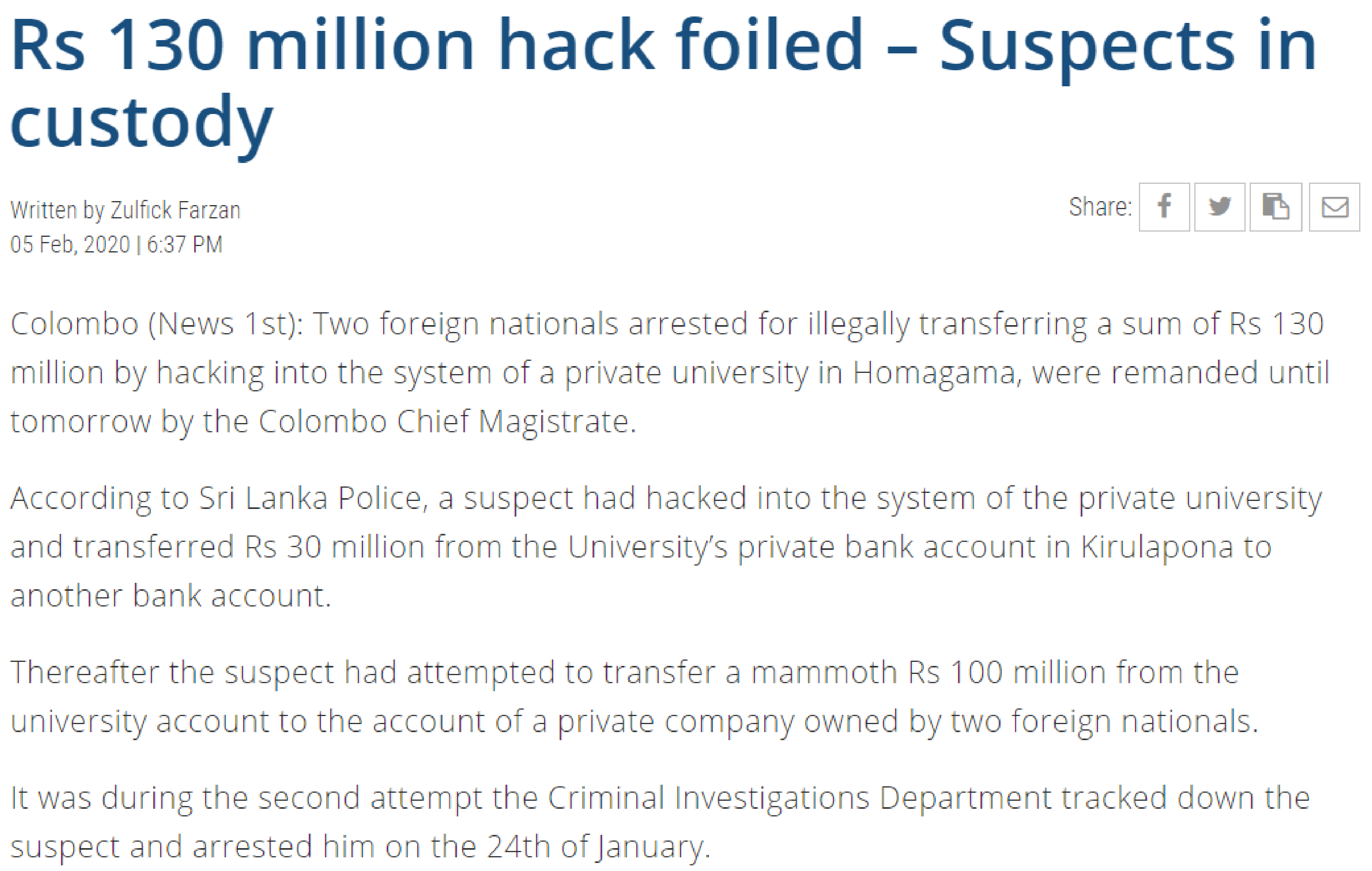
Illegal Access

(Article 2 – Budapest Convention)

- *To access to the whole or any part of a computer system without right*

- *Intentionally*

Illegal access: Example



Rs 130 million hack foiled – Suspects in custody

Written by Zulfick Farzan
05 Feb, 2020 | 6:37 PM

Share:

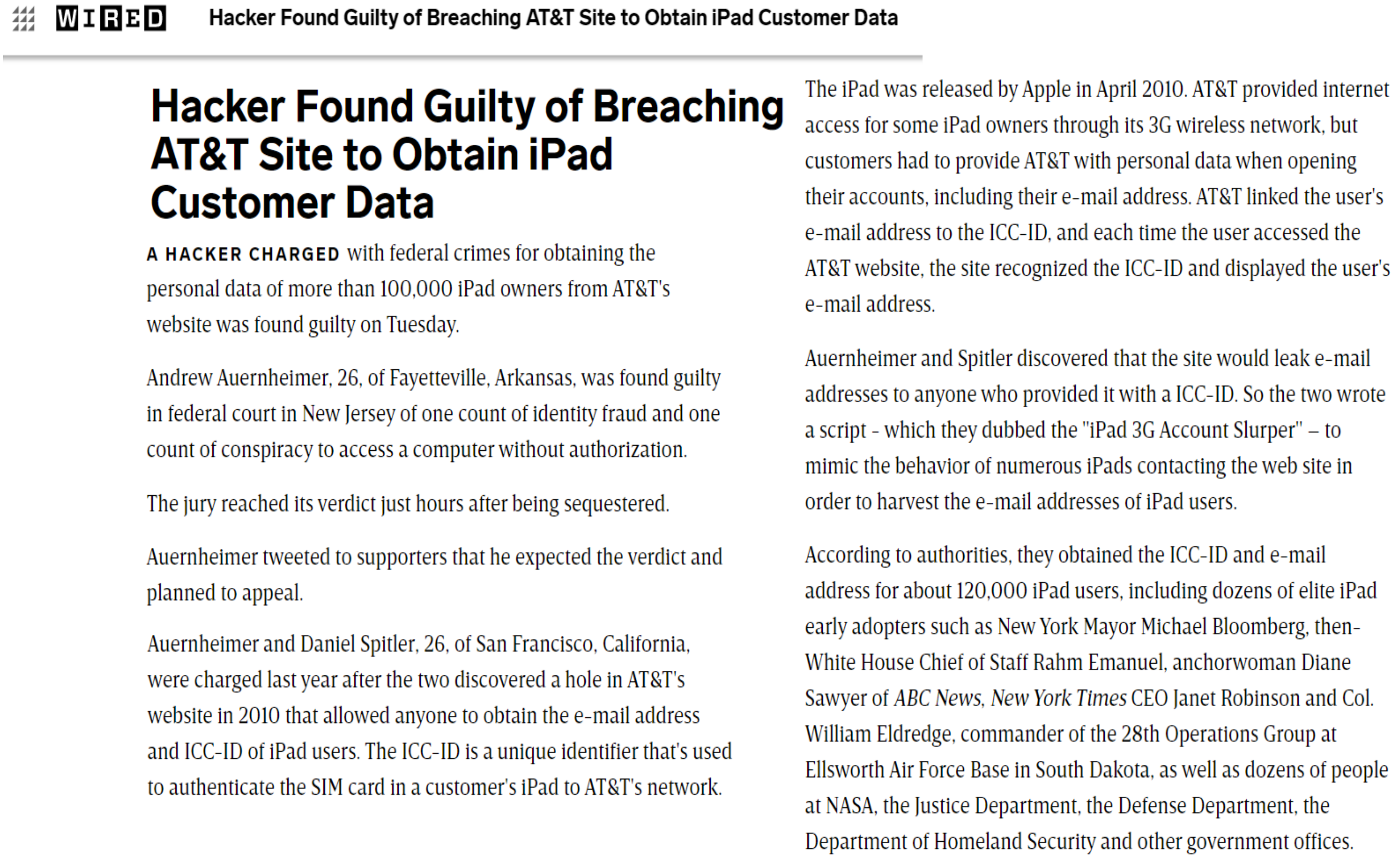
Colombo (News 1st): Two foreign nationals arrested for illegally transferring a sum of Rs 130 million by hacking into the system of a private university in Homagama, were remanded until tomorrow by the Colombo Chief Magistrate.

According to Sri Lanka Police, a suspect had hacked into the system of the private university and transferred Rs 30 million from the University's private bank account in Kirulapona to another bank account.

Thereafter the suspect had attempted to transfer a mammoth Rs 100 million from the university account to the account of a private company owned by two foreign nationals.

It was during the second attempt the Criminal Investigations Department tracked down the suspect and arrested him on the 24th of January.

Illegal access: Example



WIRED Hacker Found Guilty of Breaching AT&T Site to Obtain iPad Customer Data

Hacker Found Guilty of Breaching AT&T Site to Obtain iPad Customer Data

A HACKER CHARGED with federal crimes for obtaining the personal data of more than 100,000 iPad owners from AT&T's website was found guilty on Tuesday.

Andrew Auernheimer, 26, of Fayetteville, Arkansas, was found guilty in federal court in New Jersey of one count of identity fraud and one count of conspiracy to access a computer without authorization.

The jury reached its verdict just hours after being sequestered.

Auernheimer tweeted to supporters that he expected the verdict and planned to appeal.

Auernheimer and Daniel Spitler, 26, of San Francisco, California, were charged last year after the two discovered a hole in AT&T's website in 2010 that allowed anyone to obtain the e-mail address and ICC-ID of iPad users. The ICC-ID is a unique identifier that's used to authenticate the SIM card in a customer's iPad to AT&T's network.

The iPad was released by Apple in April 2010. AT&T provided internet access for some iPad owners through its 3G wireless network, but customers had to provide AT&T with personal data when opening their accounts, including their e-mail address. AT&T linked the user's e-mail address to the ICC-ID, and each time the user accessed the AT&T website, the site recognized the ICC-ID and displayed the user's e-mail address.

Auernheimer and Spitler discovered that the site would leak e-mail addresses to anyone who provided it with a ICC-ID. So the two wrote a script - which they dubbed the "iPad 3G Account Slurper" – to mimic the behavior of numerous iPads contacting the web site in order to harvest the e-mail addresses of iPad users.

According to authorities, they obtained the ICC-ID and e-mail address for about 120,000 iPad users, including dozens of elite iPad early adopters such as New York Mayor Michael Bloomberg, then-White House Chief of Staff Rahm Emanuel, anchorwoman Diane Sawyer of *ABC News*, *New York Times* CEO Janet Robinson and Col. William Eldredge, commander of the 28th Operations Group at Ellsworth Air Force Base in South Dakota, as well as dozens of people at NASA, the Justice Department, the Defense Department, the Department of Homeland Security and other government offices.

Illegal access (“access”)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the **access** to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

- Access includes the entering of another computer system:
  - Where it is connected via public telecommunications network;
  - To a computer system on the same network (LAN or Intranet within an organisation)

- Access does not include mere sending of e-mail message or file to computer system

- Method of communication with computer system does not matter (whether from distance via wireless links; or at a close range)

Illegal access (“whole or part”)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the **whole or any part of a computer system** without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Part of a computer system includes:

- Hardware
- Components
- Stored data of the system installed
- Directories
- Traffic data
- Content-related data

Illegal access (“without right”)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system **without right**. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

- Access must be unauthorised for it to constitute an offence
- Authorisation can be legislative, executive, administrative, judicial, contractual or otherwise
- Accessing a computer system that permits free and open access by the public should not be criminalised

Illegal access (“without right”)

No definition of “without authorisation” in the Budapest Convention

Countries which adopted definitions:

United Kingdom

Singapore

Antigua & Barbuda

Mauritius

Bermuda

Ghana

Elements:

- Entitlement to control access of the kind in question
- Consent from person with such entitlement

Examples of implementation of “without right”

E.g. UK Computer Misuse Act

- Access of any kind by any person to any program or data held in a computer is unauthorised if—

a) he is **not himself entitled to control access of the kind in question** to the program or data; and

b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled but this subsection is subject to section 10.

- The person accessing must not be entitled to control access of the kind in question

- The entitlement could be:
  - legislative
  - executive
  - administrative
  - judicial
  - contractual
  - based on established legal defenses, excuses or justifications

Examples of implementation of "without right"

E.g. UK Computer Misuse Act

- Access of any kind by any person to any program or data held in a computer is unauthorised if—

a) he is not himself entitled to control access of the kind in question to the program or data; and

b) he **does not have consent to access by him of the kind in question** to the program or data **from any person who is so entitled** but this subsection is subject to section 10.

- The person accessing must not have the consent of any person entitled to control access of the kind in question

- The consent from such a person could be express or implied

Illegal access ("infringing security measures…"

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by **infringing security measures**, with the **intent of obtaining computer data** or **other dishonest intent**, or in relation to a **computer system that is connected to another computer system**.

Parties may limit the criminalization of access with the following qualifying elements:

- Infringing security measures
- Intent to obtain computer data
- Dishonest intent
- Access in relation to a computer system that is connected to another computer system (excluding access to standalone computer systems)

- **Ghana’s Electronic Transactions Act, 2008 (Act 772)**
- **Access to protected computer**
- S.118. A person who secures unauthorised access or attempts to secure access to a protected system in contravention of a provision of this Act commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

ARTICLE 29 (1a&1b) MALABO CONVENTION…”

Offences specific to Information and Communication Technologies.

1. Attacks on Computer Systems: State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

a. Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access.

b. Gain or attempt to again unauthorized accesss to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence

MALABO CONVENTION DEFINE EXCEED AUTHORIZED ACCESS…”

Exceed Authorized Access means : to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter

United States v. Rodriguez .

Similarly, the Eleventh Circuit held in United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), that an employee of the Social Security Administration exceeded his authorized access under § 1030(a)(2) when he obtained personal information about former girlfriends and potential lovers and used that information to send the women flowers or to show up at their homes. The court rejected Rodriguez’s argument that his use was not criminal. The court held: “The problem with Rodriguez’s argument is that his use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access.”

Poll question

If an employee is authorised to access bank data, can he be charged with illegal access if the employee accesses the data to assist in committing a crime?

A. YES
B. NO

The correct answer is A

Section 3

Substantive Provisions of the Budapest Convention (Part 1)

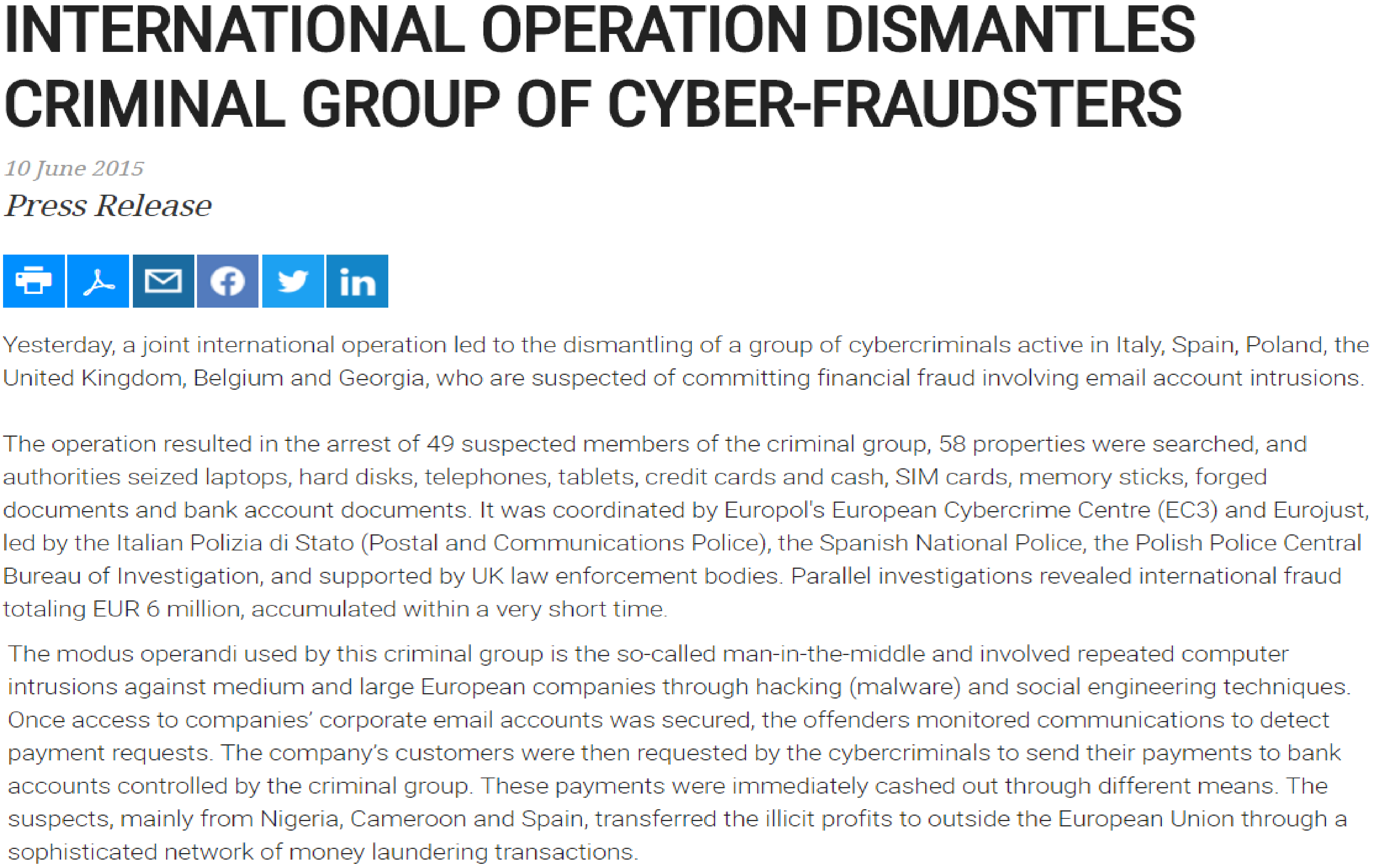
ILLEGAL INTERCEPTION

Illegal interception

Illegal Interception
(Article 3 –Budapest Convention)

- *Intentionally, and without right*
- *To intercept, by technical means, non-public transmissions of computer data*
- *To, from or within a computer system*

Illegal interception: Example



INTERNATIONAL OPERATION DISMANTLES CRIMINAL GROUP OF CYBER-FRAUDSTERS

10 June 2015

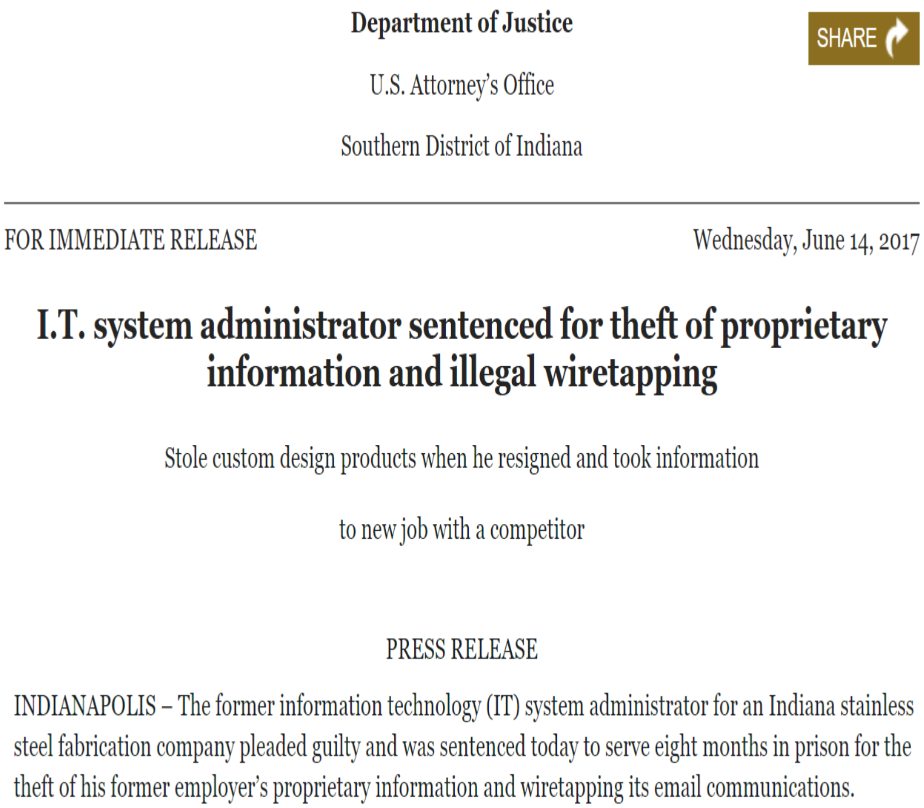
Press Release

Yesterday, a joint international operation led to the dismantling of a group of cybercriminals active in Italy, Spain, Poland, the United Kingdom, Belgium and Georgia, who are suspected of committing financial fraud involving email account intrusions.

The operation resulted in the arrest of 49 suspected members of the criminal group, 58 properties were searched, and authorities seized laptops, hard disks, telephones, tablets, credit cards and cash, SIM cards, memory sticks, forged documents and bank account documents. It was coordinated by Europol's European Cybercrime Centre (EC3) and Eurojust, led by the Italian Polizia di Stato (Postal and Communications Police), the Spanish National Police, the Polish Police Central Bureau of Investigation, and supported by UK law enforcement bodies. Parallel investigations revealed international fraud totaling EUR 6 million, accumulated within a very short time.

The modus operandi used by this criminal group is the so-called man-in-the-middle and involved repeated computer intrusions against medium and large European companies through hacking (malware) and social engineering techniques. Once access to companies' corporate email accounts was secured, the offenders monitored communications to detect payment requests. The company's customers were then requested by the cybercriminals to send their payments to bank accounts controlled by the criminal group. These payments were immediately cashed out through different means. The suspects, mainly from Nigeria, Cameroon and Spain, transferred the illicit profits to outside the European Union through a sophisticated network of money laundering transactions.

Illegal interception: Example



Department of Justice

U.S. Attorney's Office

Southern District of Indiana

FOR IMMEDIATE RELEASE

Wednesday, June 14, 2017

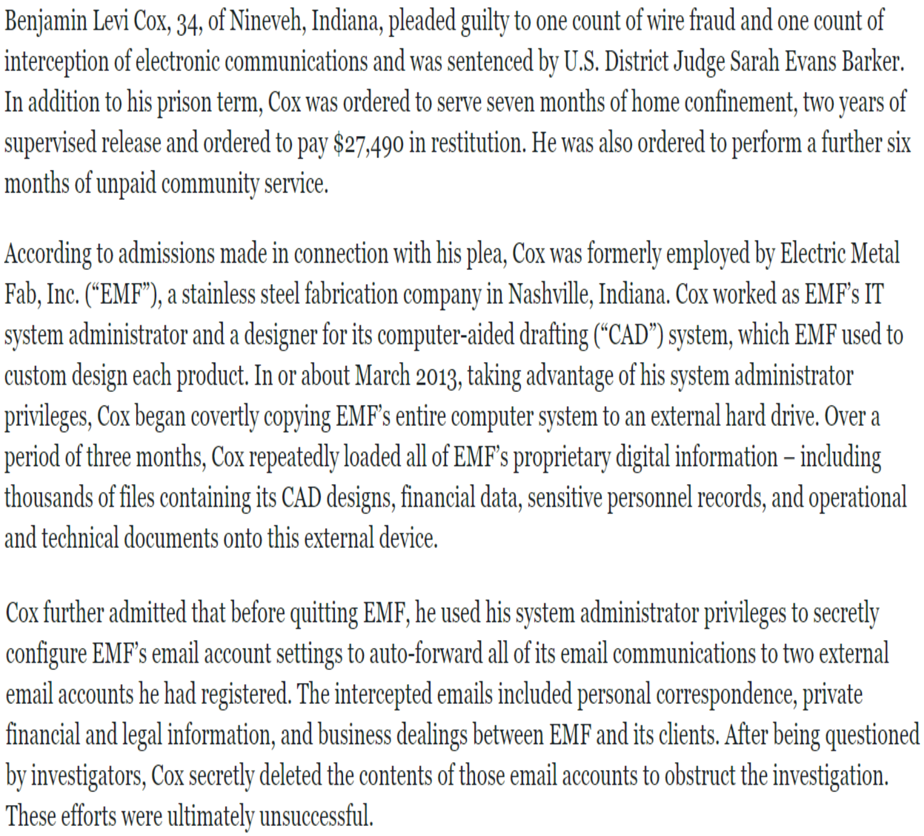
I.T. system administrator sentenced for theft of proprietary information and illegal wiretapping

Stole custom design products when he resigned and took information

to new job with a competitor

PRESS RELEASE

INDIANAPOLIS – The former information technology (IT) system administrator for an Indiana stainless steel fabrication company pleaded guilty and was sentenced today to serve eight months in prison for the theft of his former employer's proprietary information and wiretapping its email communications.



Benjamin Levi Cox, 34, of Nineveh, Indiana, pleaded guilty to one count of wire fraud and one count of interception of electronic communications and was sentenced by U.S. District Judge Sarah Evans Barker. In addition to his prison term, Cox was ordered to serve seven months of home confinement, two years of supervised release and ordered to pay $27,490 in restitution. He was also ordered to perform a further six months of unpaid community service.

According to admissions made in connection with his plea, Cox was formerly employed by Electric Metal Fab, Inc. ("EMF"), a stainless steel fabrication company in Nashville, Indiana. Cox worked as EMF's IT system administrator and a designer for its computer-aided drafting ("CAD") system, which EMF used to custom design each product. In or about March 2013, taking advantage of his system administrator privileges, Cox began covertly copying EMF's entire computer system to an external hard drive. Over a period of three months, Cox repeatedly loaded all of EMF's proprietary digital information – including thousands of files containing its CAD designs, financial data, sensitive personnel records, and operational and technical documents onto this external device.

Cox further admitted that before quitting EMF, he used his system administrator privileges to secretly configure EMF's email account settings to auto-forward all of its email communications to two external email accounts he had registered. The intercepted emails included personal correspondence, private financial and legal information, and business dealings between EMF and its clients. After being questioned by investigators, Cox secretly deleted the contents of those email accounts to obstruct the investigation. These efforts were ultimately unsuccessful.

Illegal interception ("interception")

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the **interception** without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

- Interception means listening to, monitoring or surveillance of communications

- Provision aims to protect the privacy of data communications

- Tackles equivalents of traditional tapping and recording of oral telephone conversations when done to transmission of computer data

Illegal interception ("without right")

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception **without right**, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Examples of possible interception with right:

- Person instructed or authorised by participants of transmission, including for:
  - Authorised testing agreed to by participants
  - Protection activities agreed to by participants
- Employing cookies on websites
- Lawfully authorised surveillance by law enforcement authorities

Illegal interception ("made by technical means")

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, **made by technical means**, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

- Technical means would cover interception through:
  - Access and use of computer system;
  - Use of electronic eavesdropping or tapping devices
- This may include:
  - Recording
  - Use of technical devices fixed to transmission lines
  - Use of devices to collect and record wireless communications
  - Use of software, passwords and codes

Illegal interception (“non-public transmissions”)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of **non-public transmissions** of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

- Offence limited to the interception of non-public transmissions of data
- Whether or not the data is not publicly available is irrelevant for this offence – what matters is whether the transmission is non-public
- The offence may criminalise publicly available information communicated through non-public transmissions

Illegal interception ("to, from or within a computer system")

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data **to, from or within a computer system**, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

- Interception relates to transmissions:
  - To a computer system (e.g. transmission flowing from a person to a computer through keyboard entry)
  - From a computer system (e.g. transmission flowing from one computer system to another computer system)
  - Within a computer system (e.g. transmissions flowing from a central processing unit to a connected printer

Illegal interception (“electromagnetic emissions”)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including **electromagnetic emissions** from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

- Computer systems may emit electromagnetic emissions which carry computer data

- Computer data may be reconstructed from such emissions

- Thus interception of electromagnetic emissions is included criminalised

Illegal interception ("dishonest intent…")

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with **dishonest intent, or in relation to a computer system that is connected to another computer system.**

- Parties may limit the criminalization of interception with the following qualifying elements:
  - Dishonest intent
  - Interception in relation to a computer system that is connected to another computer system (excluding interception related to standalone computer systems)

MALABO CONVENTION ARTICLE 29(2a)

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

a. Intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system

Section 4

Substantive Provisions of the Budapest Convention (Part 1)

DATA INTERFERENCE

Data interference

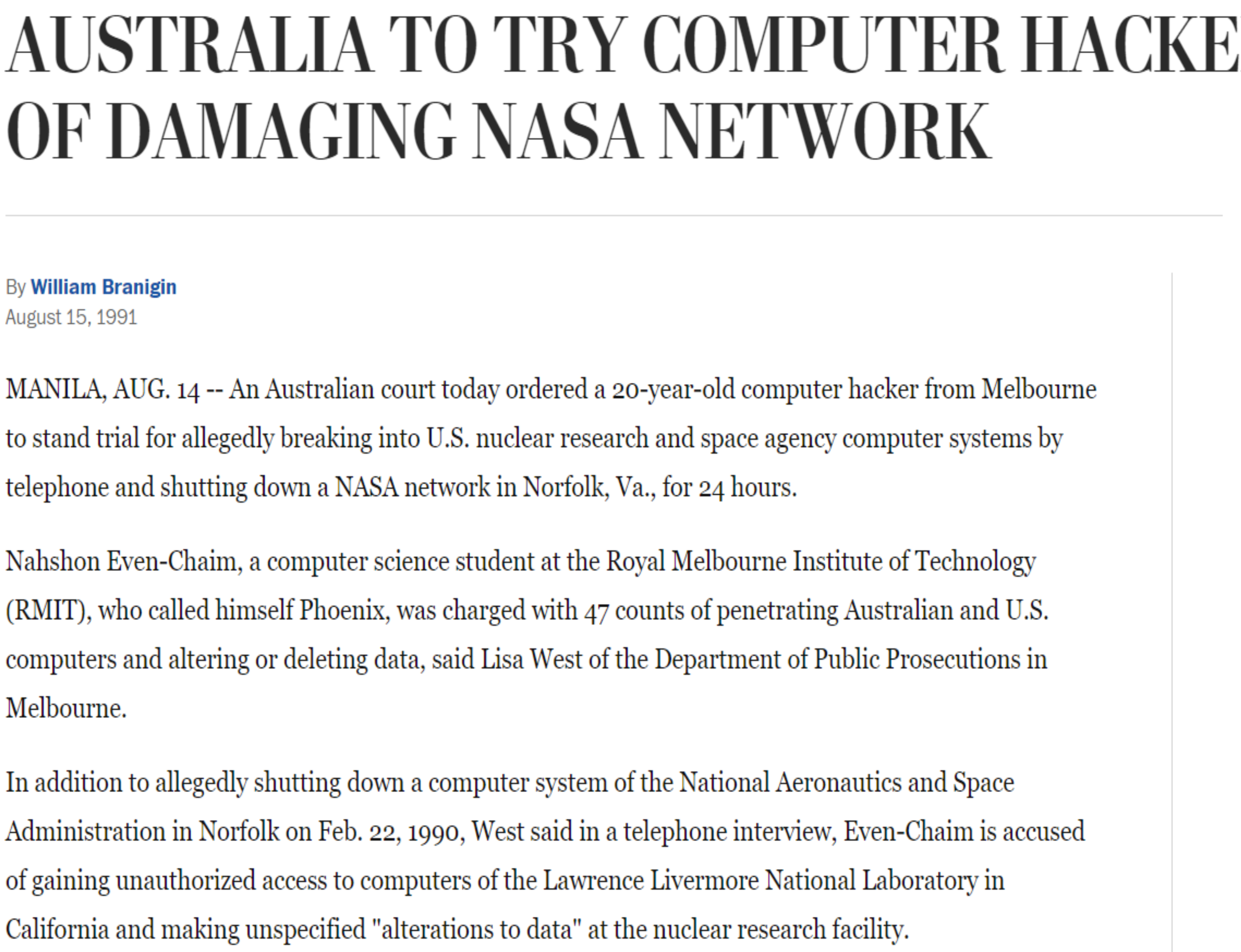
Data Interference

(Article 4 – Budapest Convention)

- *Damaging, deletion, deterioration, alteration or suppression of computer data*

- *Intentionally, without right*

Data interference: Example



AUSTRALIA TO TRY COMPUTER HACKER ACCUSED OF DAMAGING NASA NETWORK

By **William Branigin**
August 15, 1991

MANILA, AUG. 14 -- An Australian court today ordered a 20-year-old computer hacker from Melbourne to stand trial for allegedly breaking into U.S. nuclear research and space agency computer systems by telephone and shutting down a NASA network in Norfolk, Va., for 24 hours.

Nahshon Even-Chaim, a computer science student at the Royal Melbourne Institute of Technology (RMIT), who called himself Phoenix, was charged with 47 counts of penetrating Australian and U.S. computers and altering or deleting data, said Lisa West of the Department of Public Prosecutions in Melbourne.

In addition to allegedly shutting down a computer system of the National Aeronautics and Space Administration in Norfolk on Feb. 22, 1990, West said in a telephone interview, Even-Chaim is accused of gaining unauthorized access to computers of the Lawrence Livermore National Laboratory in California and making unspecified "alterations to data" at the nuclear research facility.

Data interference

Data interference ("damaging, deterioration"

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the **damaging**, deletion, **deterioration**, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

- Provision aims to protect the integrity and the proper functioning or use of stored computer data or computer program
- Damaging and deterioration are overlapping acts

- They refer to the negative alteration of the integrity or information content of data and programmes

Data interference (“deletion”)

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, **deletion**, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

- Deletion of data is equivalent to destruction of a corporeal thing

- Deletion has the effect of destroying data or making data unrecognisable

Data interference ("alteration"

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, **alteration** or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

- Alteration refers to the modification of existing data

- Includes the input of malicious codes such as viruses and Trojan horses and resulting modification of data

Data interference ("suppression")

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or **suppression** of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

- Suppression refers to any action that prevents or terminates availability of data to person who has access to the computer or storage medium in which it was stored

- Suppression of data does not affect the content of data itself but its availability

Data interference ("without right")

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data **without right**.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

- Examples of data interference with right:
  - Activities inherent in design of networks or common operating or commercial practices
  - Testing or protection of security system of computer authorised by owner or operator
  - Reconfiguration of computer's operating system at time of installation of new software
  - Modification of traffic data for purpose of facilitating anonymous communications (e.g. anonymous remailer systems)
  - Modification of data for purpose of secure communications (e.g. encryption)

Data interference (“serious harm”)

1. 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in **serious harm**.

- Parties may limit the criminalization of data interference to conduct which results in serious harm

- Definition of serious harm to be provided for in domestic legislation

- It may be qualified based on quantum of monetary harm arising out of conduct

MALABO CONVENTION Article 29: Attacks on Comuter systems

1. State Parties shall take the necessary legi shall take the necessary legislative and/or regulatory mechanisms to make it criminal offence to:

e. **Enter or attempt to enter data fraudulently in a computer system**

f. Damage or attempt to damage, delete or attempt to delete, deteriorate or attempt to deteriorate, alter or attempt to alter, change or attempt to change computer data fraudulently.

Poll question

If an employee is authorised to access bank data and if the employee accesses the data to assist in committing a crime by transferring the data to his coconspirator, which offence(s) would you charge the employee with?

A. Illegal access
B. Illegal interception
C. Data interference

The correct answers are A and C

Section 5

Substantive Provisions of the Budapest Convention (Part 1)

SYSTEM INTERFERENCE

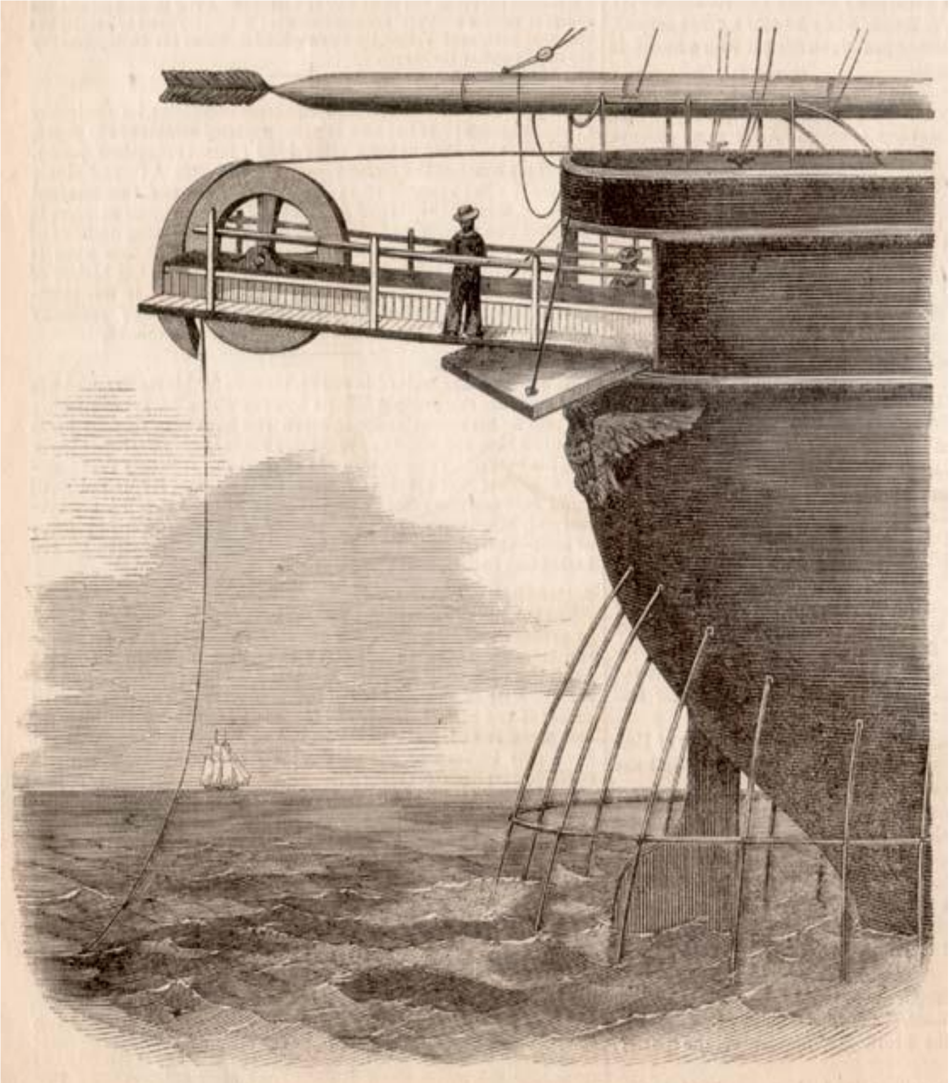
System interference

System Interference

(Article 5 – Budapest Convention)

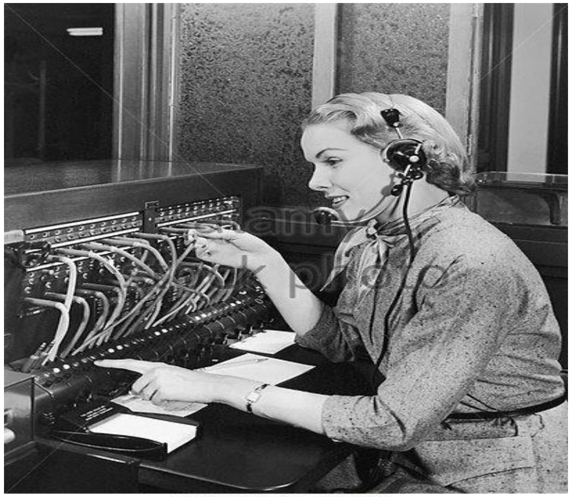
- *The serious hindering of the functioning of a computer system*
- *By inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data*
- *Intentionally, without right*

System interference

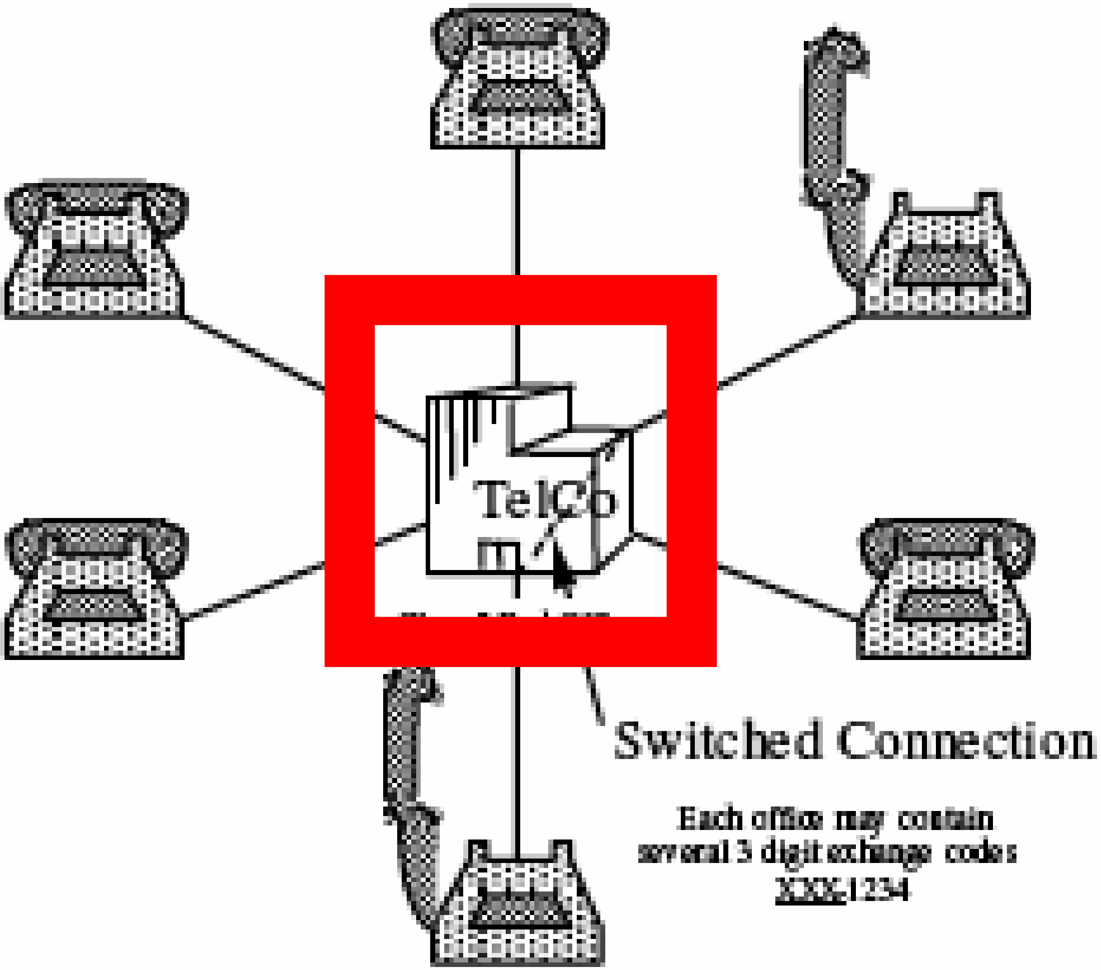


MACHINERY ON THE U. S. S. NIAGARA, PROVIDED FOR THE SECOND ATTEMPT TO LAY THE INTER-OCEANIC CABLE.

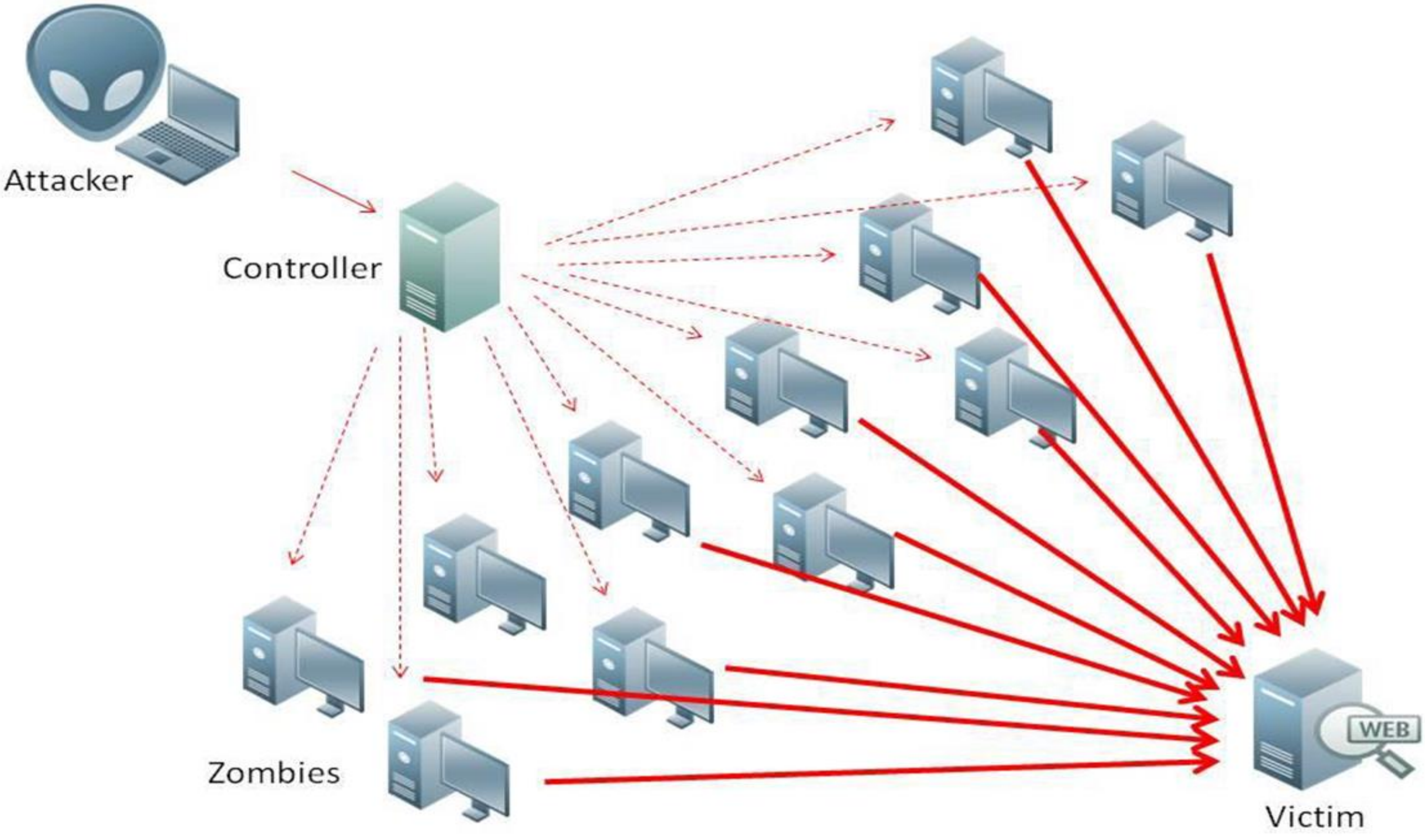
System interference


www.alamy.com - D1832G

System interference



System interference



ANOTHER CYBERATTACKS AFFECTING SUPPLY OF WATER

On March 27, 2019, the Post Rock Water District in Ellsworth, Kansas experienced a cyber security breach that threatened drinking water safety. The hacker was former employee Wyatt Travnichek, 22, who had worked at the plant from January 2018 until January 2019. Though Travnichek resigned, he remotely accessed one of a Post Rock Water District computer to shut down the cleaning and disinfecting procedures that make water potable. Travnichek was indicted on March 31, 2021 for tampering with a public water system and reckless damage to a protected computer which together carry a maximum sentence of 25 years and maximum fines of up to $500,000.

https://www.cshub.com/attacks/articles/another-cyber-attack-affecting-water-supply

System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the **serious** hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

- The term “serious” is expected to cover the sending of data to a particular system in such a form, size or frequency that it has a **significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems**
- Definition of what specifically constitutes serious hindering is to be provided for in domestic legislation

System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious **hindering** without right of the functioning of a computer system **by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data**.

- Hindering is an action that interferes with proper functioning of computer system

- Hindering must take place through:
  - Inputting
  - Transmitting
  - Damaging
  - Deleting
  - Altering
  - Suppressing
  - computer data

System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering **without right** of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

- Examples of system interference with right:
  - Activities inherent in design of networks, or common operational or commercial purposes
  - Testing of security of computer system authorised by owner or operator
  - Protection of computer system by owner or operator
  - Reconfiguration of computer's operating system where operator of system installs new software that disables previously installed programs

Malabo Convention : Article 29 (1) (d)

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

d) Hinder, distort or attempt to hinder or distort the functioning of a computer system

Substantive Provisions of the Budapest Convention (Part 1)

MISUSE OF DEVICES

Misuse of devices

Misuse of Devices

(Article 6 – Budapest Convention)

- *Intentionally and without right*
- *To possess an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5.*

Misuse of devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

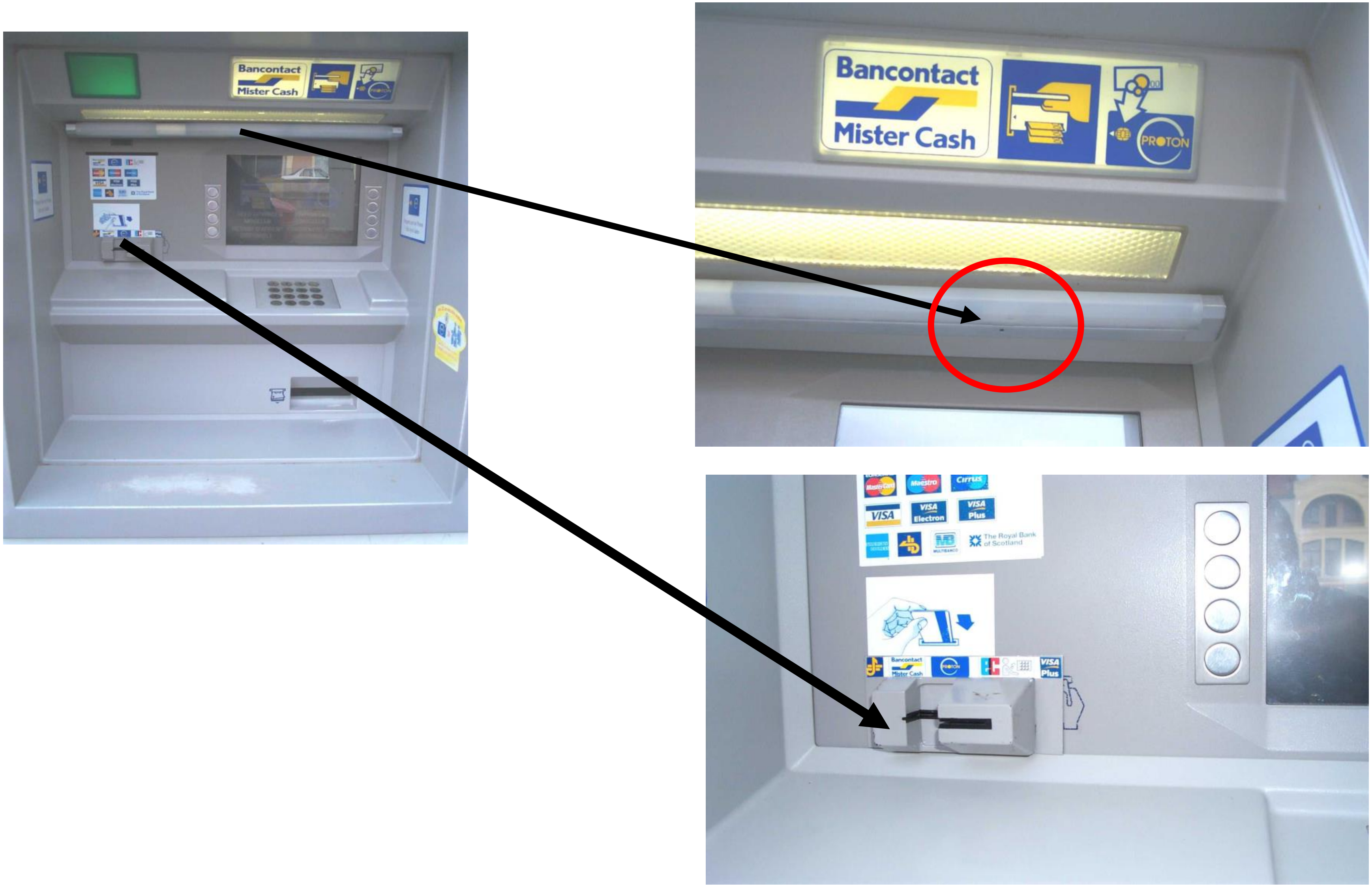
a. the **production**, **sale**, **procurement for use**, **import**, **distribution** or otherwise **making available of**:

   i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

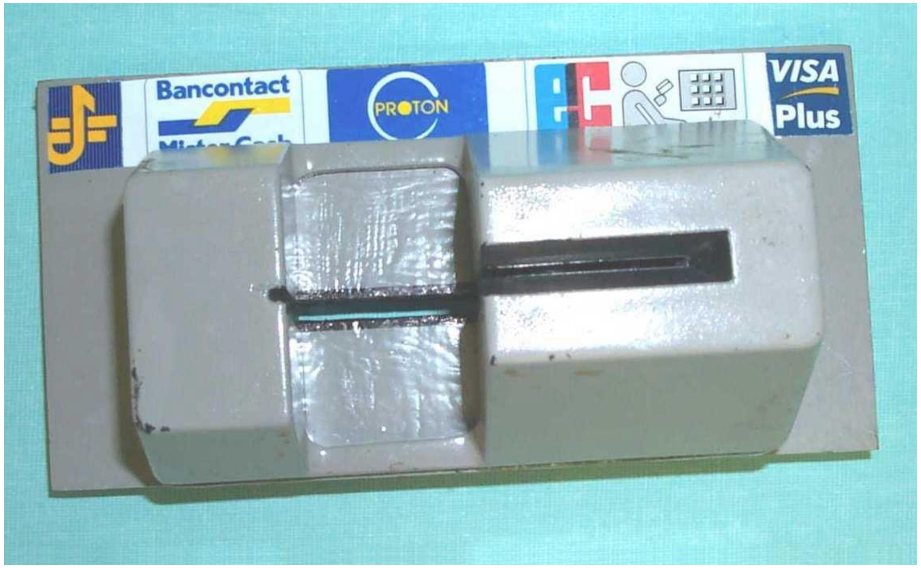
   ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

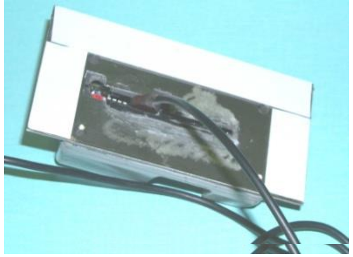
- Criminalisation of:
  - Production
  - Sale
  - Procurement for use
  - Import
  - Distribution (active act of forwarding to others)
  - Making available of (placing for the use of others, and includes creation or compilation of online hyperlinks in order to facilitate access to such devices/ passwords)

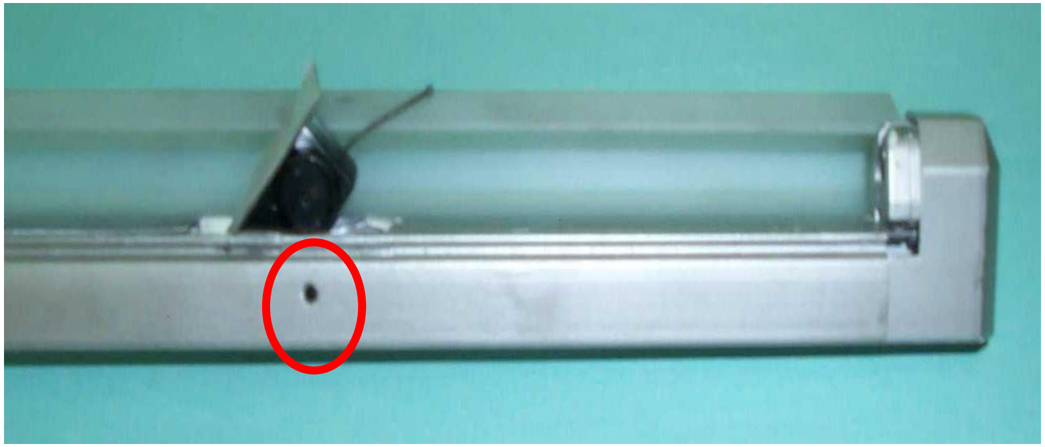
Misuse of devices



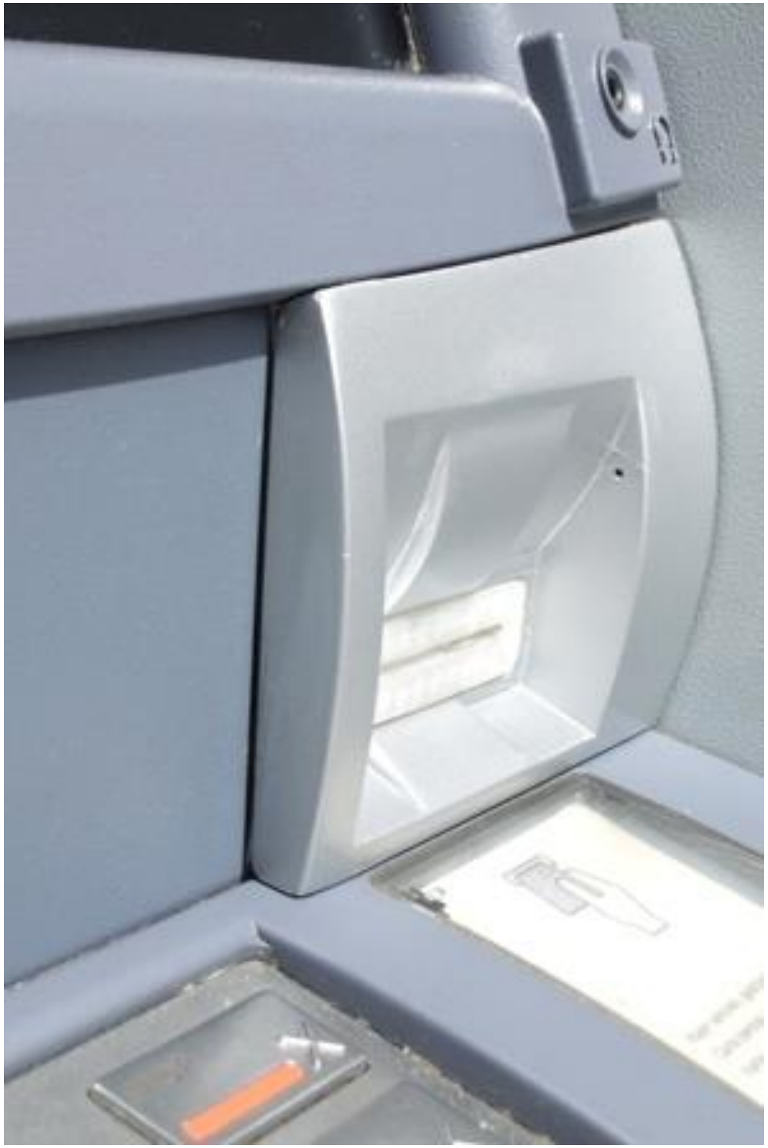
Misuse of devices



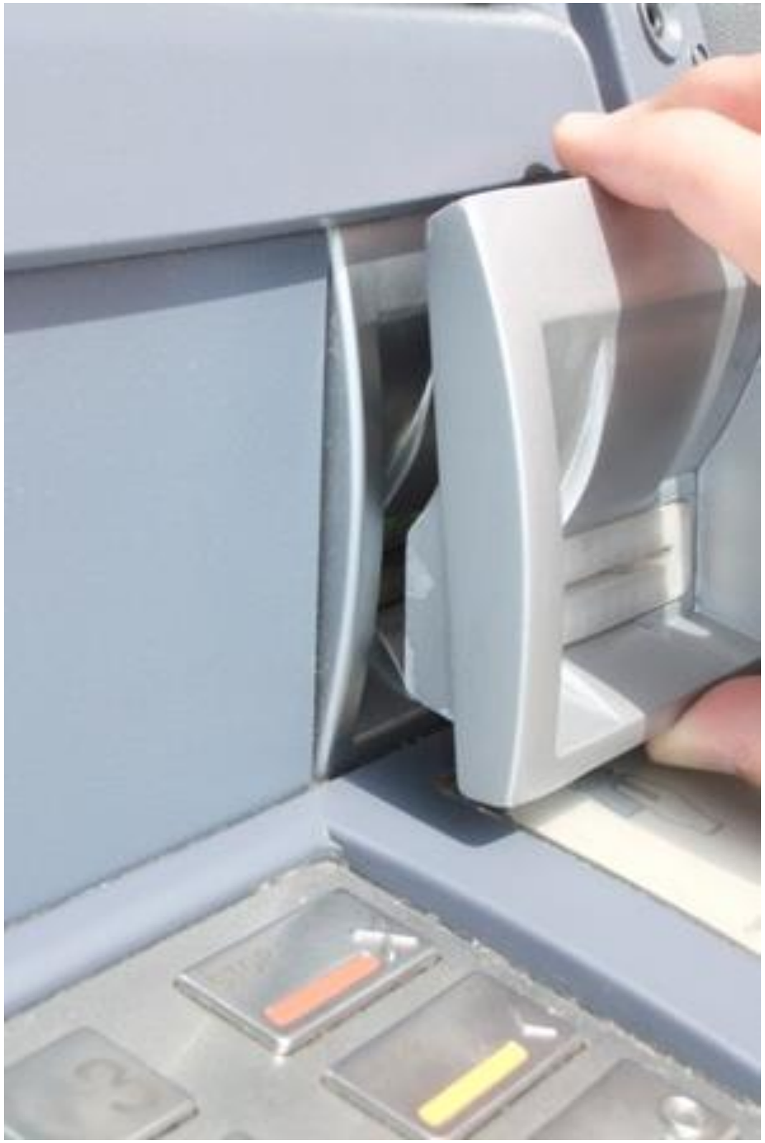


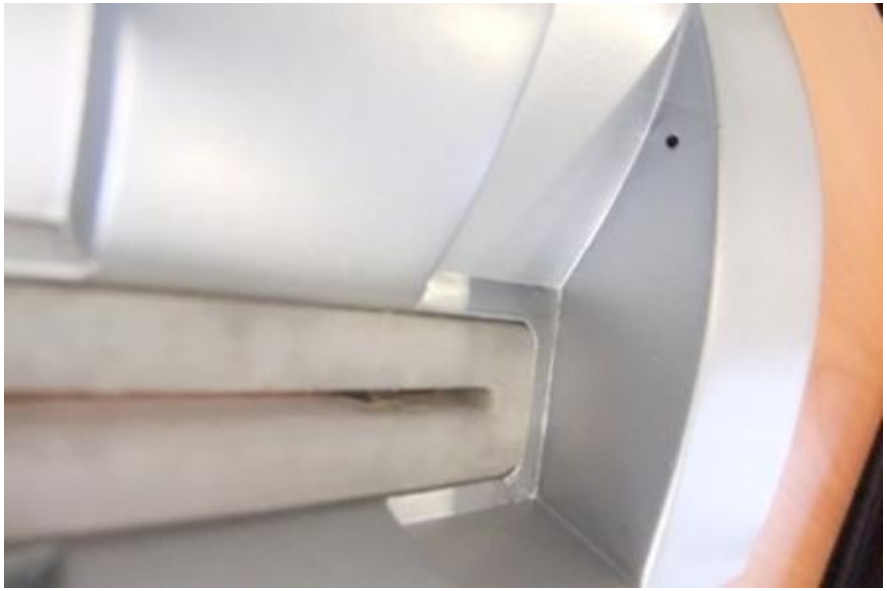


Misuse of devices

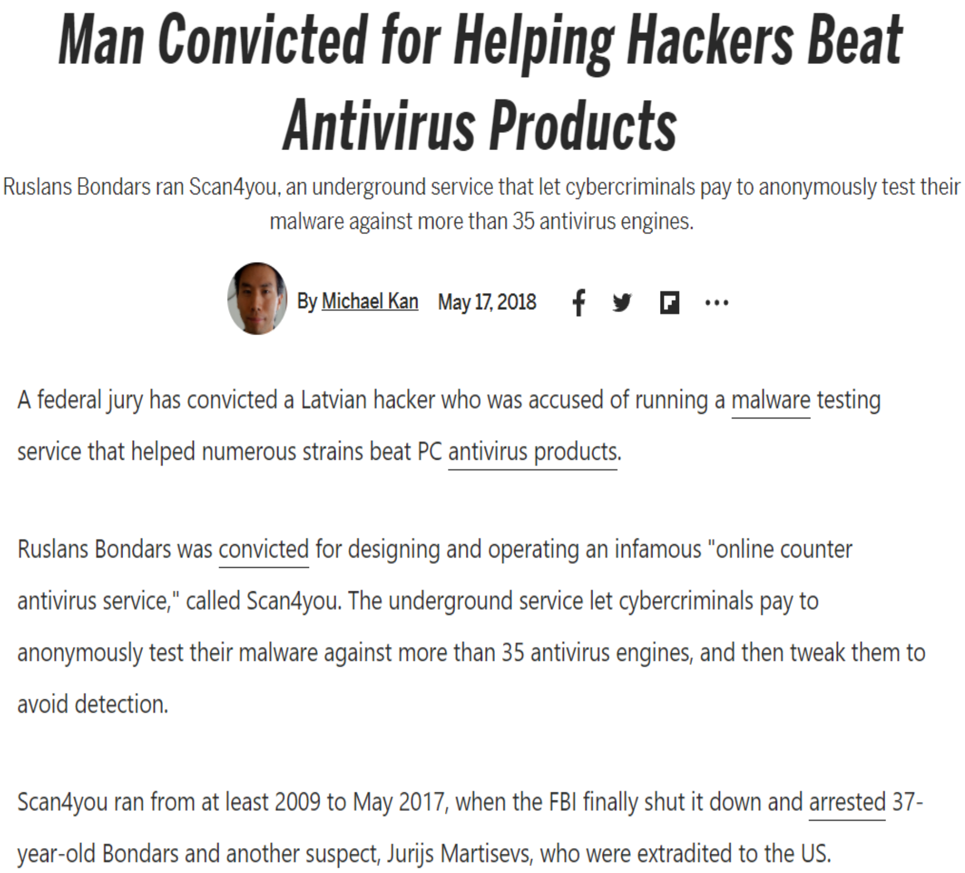


Misuse of devices





Misuse of devices



Man Convicted for Helping Hackers Beat Antivirus Products

Ruslans Bondars ran Scan4you, an underground service that let cybercriminals pay to anonymously test their malware against more than 35 antivirus engines.

By Michael Kan May 17, 2018

A federal jury has convicted a Latvian hacker who was accused of running a malware testing service that helped numerous strains beat PC antivirus products.

Ruslans Bondars was convicted for designing and operating an infamous "online counter antivirus service," called Scan4you. The underground service let cybercriminals pay to anonymously test their malware against more than 35 antivirus engines, and then tweak them to avoid detection.

Scan4you ran from at least 2009 to May 2017, when the FBI finally shut it down and arrested 37-year-old Bondars and another suspect, Jurijs Martisevs, who were extradited to the US.

Prosecutors say at its height, Scan4you was the largest service of its kind, and helped cybercriminals inflict "hundreds of millions of dollars in losses" on US companies and consumers.

For example, one customer used the service to test malware that ended up stealing about 40 million payment card numbers. Another customer relied on Scan4you to develop the "Citadel" malware strain, which infected 11 million computers, and resulted in over $500 million in fraud-related losses.

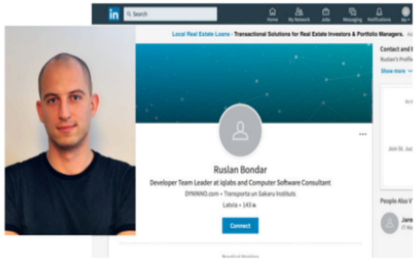

Search
Local Real Estate Loans - Transactional Solutions for Real Estate Investors & Portfolio Managers.
Ruslan Bondar
Developer Team Leader at iqlabs and Computer Software Consultant
DYNINNO.com • Transporta un Sakaru Instituts
Latvia • 143
Connect

Figure 6. Ruslans Bondars in 2012 and his LinkedIn profile.

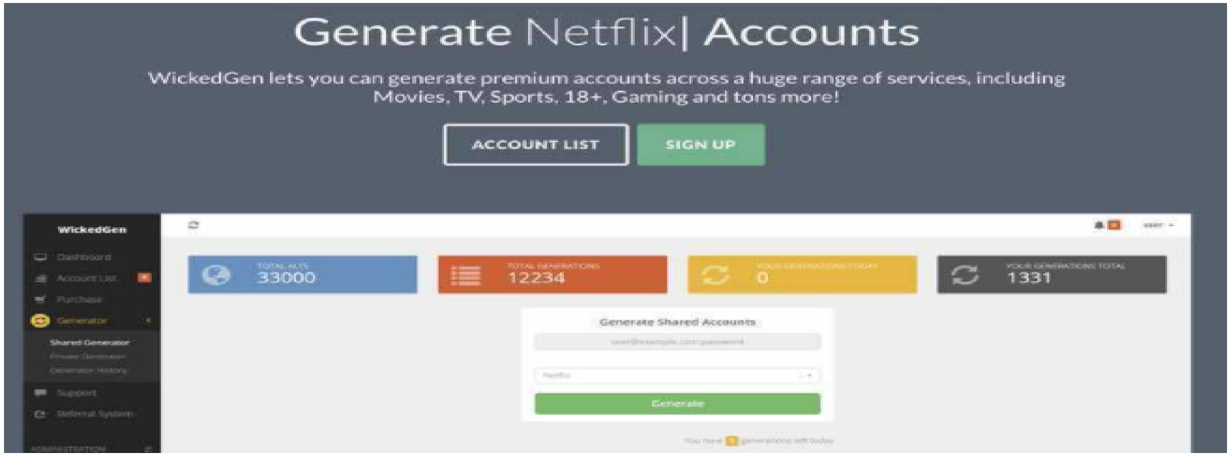
In a way, Scan4you was a counter to services like VirusTotal, which also let anyone test malware against antivirus engines. The big difference with VirusTotal is that all data submitted to the service is shared with the rest of the IT security community, which can help tip off the public about computer threats.

"Hence, cybercriminals generally stay away from these services and opt to use other third-party services that do not share any data with AV (antivirus) companies," said Trend Micro, a security firm that helped the FBI shut down Scan4you.

Misuse of devices

Australian man arrested for selling one million Netflix, Spotify, Hulu passwords

MARCH 14, 2019 23.21 EUROPE/LONDON BY ROBERT BRIEL



Police in Australia have arrested a 21-year-old Sydney man who allegedly made AU $300,000 (EUR187,000) selling passwords of services including Netflix, Spotify, Hulu, PSN, and Origin.

The arrest followed a joint international cybercrime investigation by the Australian Federal Police (AFP) and Federal Bureau of Investigation (FBI) involving online subscription service credentials stolen from Australian customers, and others around the world.

The investigation began after the FBI referred information to the AFP in May 2018 about an account generator website called WickedGen.com.

WickedGen operated for approximately two years selling stolen account details for online subscription services, including Netflix, Spotify and Hulu. The account details were obtained through credential stuffing, which sees a list of previously stolen or leaked usernames, email addresses and corresponding passwords re-used and sold for unauthorised access. The accounts details were from unknowing victims in Australia and internationally, including the United States.

Misuse of devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the **production**, **sale**, **procurement for use**, **import**, **distribution** or otherwise **making available of**:

   i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

   ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

- Criminalisation of:
  - Production
  - Sale
  - Procurement for use
  - Import
  - Distribution (active act of forwarding to others)
  - Making available of (placing for the use of others, and includes creation or compilation of online hyperlinks in order to facilitate access to such devices/ passwords)

Misuse of devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

   i. a **device**, including a **computer program**, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

   ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

- The scope of this offence relates to devices and computer programs
- It would include virus programs and programs designed or adapted to gain access to computer systems

Misuse of devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

   i. a device, including a computer program, **designed or adapted primarily** for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

   ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

- Budapest Convention requires that device be designed or adapted primarily (but not solely) for the commission of an offence corresponding to an offence under Article 2-5

- This provision seeks to strike a balance between:
  - Excluding dual-use devices (which would have been too narrow and difficult to prove) and
  - Including dual-use devices (which would have resulted in over-criminalisation by including all devices even if legally produced and distributed)

Misuse of devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

   i. i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

   ii. ii a **computer password**, **access code**, **or similar data** by which the whole or any part of a computer system is capable of being accessed, with intent that it **be used for the purpose of committing any of the offences established in Articles 2 through 5;** and

- Criminalisation of:
  - Production
  - Sale
  - Procurement for use
  - Import
  - Distribution
  - Making available of
  - a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed.

Misuse of devices

b. the **possession** of an item referred to in paragraphs a.i or ii above, **with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5**. A Party may require by law that a **number of such items** be possessed before criminal liability attaches.

This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

- Possession of devices or passwords with intent to commit an offence corresponding to Article 2-5 of Budapest Convention

- This could apply to possession of a certain minimum number

Misuse of devices

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is **not for the purpose of committing an offence** established in accordance with Articles 2 through 5 of this Convention, such as for the **authorised testing or protection** of a computer system.

Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

- Conduct only constitutes an offence if it is done for the purpose of committing an offence established in accordance with Article 2-5 of the Budapest Convention

- Conduct undertaken for the Authorised testing or protection of a computer system

Poll question

An individual procures for use a penetration testing device that is designed to enable accessing a computer without authorisation. The individual intends to use it to conduct authorised testing of a computer system.

Is this an offence under Article 6 of the Budapest Convention?

A. YES
B. NO

The correct answer is B

Session objectives

By the end of the session, delegates will be able to:

- Understand the meaning of fundamental terms such as computer data, computer system, traffic data and service provider
- Identify the elements which constitute the offence of:
  - Illegal access
  - Illegal interception
  - Data interference
  - System interference
  - Misuse of devices

Introductory Judicial Training Course on Cybercrime and Electronic Evidence

Thank you

Xxxxx XXXXXXXX

Council of Europe

email

DD Month YYYY