THE FIGHT AGAINST ILLEGAL WEBSITES

[**Issue Number 116 - April 2021**](https://www.lebarmy.gov.lb/en/content/116-d)

**The Fight Against Illegal Websites**
Prepared By: Chrystel Melhem
Student chemical engineering 2nd year

**Introduction**

Overview on the issue

Globalization. Internet. Computer systems. Three vital organs of today’s world, but was it always the case? From surviving World War II to fighting the COVID-19 pandemic, the world has always been ready to defy the challenges that come its way. But what if the biggest threat of all is so imperceptible that it is invisible to the naked eye; is the world ready then to make history again by fighting this global borderless war? Cybercrime is an illegal deed through which information and communication technology (ICT) is utilized to ease a crime or prey on systems, data, networks, websites, and technology. It comes in several aspects with one of them being illegal website activity (Katharina.kiener-Manu.). To highlight the urgency of the situation, the drastic growth in number of internet users was pushed from 413 million in 2000 to almost 3.4 billion with Lebanon accounting 4.57 million in 2016 (Roser, M. et al, 2015). Those statistics are not just numbers, they are people who are vulnerable to illegal websites.

Why this topic? Because Netflix didn’t offer the movie I wanted to watch, I decided to resort to one of the online websites that offered it. The horrific advertisements that resulted from the mere penetration to this “free” website alarmed me of the danger the internet is hiding behind its dreamy façade.

**Different types of types of illegal websites through case studies**

Case Study 1: Computer-Related Forgery

Exploitation of the COVID-19 pandemic: Vietnam residents Thu Phan Dinh, Tran Khanh and Nguyen Duy Toan started more than 300 sham websites to sell goods, such as hand sanitizers and wipes, that became short in supply because of their increase in demand due to the pandemic. To make matters worse, contact information was designed to deceive the customers leading to over 7,000 victims in the U.S. with almost 40,000 fake transactions valued at USD$975,000. Consequently, the U.S. Department of Homeland Security’s Office of Homeland Security Investigations (HSI) supplied the Vietnam Ministry of Public Security with the information needed to investigate and arrest the convicted individuals (U.S. Embassy & Consulate in Vietnam,2020).

Case Study 2: Computer-Related Identity Offenses

The Infraud Organization- In 2010, Ukrainian man Svyatoslav Bondarenko started the Infraud Organization, “one of the largest international cybercrime rings”, causing over USD$677 million in losses. With almost 11,000 members, the organization aimed at 4.3 million credit cards, debit cards and bank accounts to then sell them on an online forum. Along with international cooperation, the U.S. authorities managed to indict thirty-six individuals with the exception of Novak, “Goldenshop”, “Deputat”, and Musliu who were charged with “possession of 15 or more counterfeit and unauthorized access devices” (The United States Department of Justice, 2018).

Case Study 3: Content Related Offenses

Matthew Graham or “Lux” and child pornography- At only 22 years old, Matthew Graham faces jail time for founding websites and online forums that welcomed sexual and physical abuse towards children. Such websites, formerly known as “Hurt 2 The Core” and “Love 2 The Core”, attracted pedophiles and sadistic individuals who had to supply content in order to be admitted into the websites. The investigation took two years and was so prominent that it involved FBI, Europol, and Canadian authorities before moving the conviction to Melbourne, Australia (Johnston, C., 2016).

**Lebanon takes action**

Lebanon organizes Anti-Cybercrime Forum and launches the Cybercrime Combating Bureau- After the Lebanese authorities noticed that cybercrime rates have catalyzed especially in the bank sector with losses reaching USD$12 million, they organized the Anti-Cybercrime Forum in 2015 as well as issued a cybercrime guide. In this forum, Internal Security Forces (ISF) chief Maj. Gen. Ibrahim Basbous delivered a speech in honor of the launch of the Cybercrime Combating Bureau whose members went through extensive drilling (More than a banking scandal?).

ISF online report forms and number- Through their website, the ISF offers the public its phone number in addition to an online report form in case any individual faces any form of cybercrime or threat. Confidentiality is promised when dealing with the issue at hand (Internal security forces).

E-transaction law of 2018- Activists and civil society organizations have been fighting against the legislation of the e-transaction law and the Lebanese Internet Regulation Act (LIRA) for they feared it will restrict freedom of speech (Freedom on the Net, 2014). After several years, the e-transaction law, known now as Law No.81, was legalized in an effort to protect personal data and increase cybersecurity. Zooming into the law, articles 125 and 126 authorize the investigation in websites related to “terrorism, minors’ pornography, prohibited gambling, organized electronic frauds, money laundering…” The court’s final verdict includes suspending electronic services, blocking and cancelling accounts on the mentioned websites (SMEX).

The Ministry of Justice trains 20 judges to face cybercrime- In an effort to reinforce the implementation of law No.81 mentioned above, twenty judges were trained by the Ministry of Justice along with the help of the Council of Europe and the European Union as part of the CyberSouth project (United Nations).

Lebanon National Cybersecurity Strategy 2022- With the help of a National Committee founded by Resolution 173, designated and former Prime Minister Saad Hariri prepared a project to build a strong foundation for cybersecurity. For one, the report recognizes the state’s ineffectiveness and presents the different causes behind it. Next, a set of accomplishments is listed in addition to the different types of cyberthreat. Furthermore, responsibilities are divided among the state’s main three organs: the government, businesses and organizations and individuals. The different pillars targeted are introduced; to name some: “develop international cooperation in cyber security” and “promote industrial and technical capacity”. Finally, the National Cyber Security and Information System Agency (NCISA) would be established to increase cybersecurity effectiveness (Lebanon National Cyber Security Strategy, 2019).

**The world fights**

Laws: Almost all countries have adapted national laws to fight illegal website activity. For instance, the State of Qatar formulated the following one: Qatar’s Law No.14 of 2014- Chapter 1 in section 2 of the Cybercrime Prevention Law aims at criminalizing hacking into information programs systems or networks as well as founding illegal websites. Moreover, articles 6 and 7 are illustrations of the different sentences and fines that result from establishing websites that publish fraudulent news or the circulation of child pornography (Squire Patton Boggs, 2014).

Treaties: Cybercrime is not limited to the borders of a country but rather is a “virus” that can spread anywhere in the world. For this, harmonization of laws and international cooperation among states is vital to tackle effectively and expeditiously this issue. Treaties are one way of ensuring a united front against a threat, and an example for this: The Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime of 2011- This initiation obliges its member states to legislate national cybercrime laws and ease common legal aid, collaboration, and extradition when combatting cybercrime. In addition, this directive has a Convention on Mutual Assistance in Criminal Matters and a Convention on Extradition that makes investigation collaborations easier. The 66th council’s session report includes in its second chapter the different criminalized offenses such as computer data forgery (ECOWAS, 2011).

**Recommendations**

Enhancing Knowledge in Cybersecurity: Raising awareness is one of the core steps for moving forward. In fact, Cybersecurity Month, which occurs each October, can be utilized as a yearly event to inform the public about the dangers of surfing on the internet and the precautions one should take to protect himself and his personal data. This can be done through the national TV and radio broadcasting daily documentaries about different real-life cases that took place and were targeted by illegal websites. In addition, cartoons can be fabricated for children to inform them of the specific websites they are allowed to visit in the absence of their parents.

The United Nations Organization of Drugs and Crime’s Education for Justice (E4J) Initiative is a teaching guide that includes classroom exercises and information subdivided into modules about cybercrime types, international actions, prosecution procedure, and other topics (Katharina.kiener-Manu). The government is urged to implement it in its educational system by appending it to the social studies’ chapters.

Child Friendly Filtering: Children are pure and have no idea about the evil in the world awaiting to reach them. For this, it is their parents’ duty to protect them and limit their exposure to illegal websites. Software, such as Qustodio, is beneficial to block websites and filter the content exhibited (Best parental control software). As a result, the government is invited to provide parents with annual plans in such software in an attempt to build better citizens by aiming at the problem from its roots.

Credit Card Tracking: This initiative can be done to track illegal websites’ IP addresses as a person provides his or her credit or debit card information on a website. Once the website is tracked, the purchase can be blocked and further investigation can be initiated. This can limit identity fraud and phishing attempts through which fake websites are disguised as legitimate ones. Moreover, this can also reduce the number of report forms aiming at the same complaint.

Collaboration with the UNODC: The UNODC commenced the cybercrime repository which consists of the “legislation”, “case law” and “lesson-learned” databases on cybercrime and electronic evidence. For instance, the “database of legislation” includes different laws and evidence correlated to cybercrime in different countries which can be searched by naming the country, cybercrime committed and procedure (UNODC). Authorities can benefit from it in terms of reducing routine reading and accelerating investigations which in its turn reduces financial expenses. Another way is the government allowing law students to access it to catalyze their cybercrime knowledge in an attempt of shaping the lawyers and judges of tomorrow.

**References**:

- Katharina.kiener-Manu. (n.d.). Cybercrime module 1 key issues: Cybercrime in brief. https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html

- Roser, M., Ritchie, H., &amp; Ortiz-Ospina, E. (2015, July 14). Internet. https://ourworldindata.org/internet

- Vnmission 18 August, 2. (2020, August 18). U.s.-vietnamese law enforcement cooperation uncovers fraudulent websites exploiting the covid-19 pandemic. https://vn.usembassy.gov/us-vietnamese-law-enforcement-cooperation-uncovers-fraudulent-websites-exploiting-the-covid-19-pandemic/

- Thirty-six defendants indicted for Alleged roles in TRANSNATIONAL criminal organization responsible for more THAN $530 million in losses FROM CYBERCRIMES. (2018, February 09). https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

- Johnston, C. (2016, May 14). Lux captured: The simple error that brought down the world's worst hurtcore paedophile. https://www.smh.com.au/national/lux-captured-the-simple-error-that-brought-down-the-worlds-worst-hurtcore-paedophile-20160513-goum54.html

- More than a banking scandal? (n.d.). https://calert.info/details.php?id=59

- Internal security forces; قوى الأمن الداخلي - الموقع الرسمي. (n.d.). https://www.isf.gov.lb/en/cybersecurity

- LEBANON NATIONAL CYBER SECURITY STRATEGY. (2019, June).http://pcm.gov.lb/Library/Files/LRF/tamim/Strategie\_Liban\_Cyber\_EN\_V20\_Lg.pdf

- SMEX (n.d.). Law No. 81 Relating to Electronic Transactions and Personal Data. https://tahseen.ae/media/3197/e-transaction-law-lebanon-official.pdf

- United Nations (2019, July 30). Countering the use of information and communications technologies for criminal purposes. https://www.unodc.org/documents/Cybercrime/SG\_report/V1908182\_E.pdf

- Squire Patton Boggs (2014, September 18). Law No. (14) of 2014 Promulgating the Cybercrime Prevention Law. http://chato.cl/blog/files/QatarCybercrimeLaw\_unofficial\_translation.pdf

- ECOWAS (2011, August 19). Sixty-Sixth Ordinary Session of the Council of Ministers. https://issafrica.org/ctafrica/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS.pdf

- Katharina.kiener-Manu. (n.d.). Cybercrime module 4. https://www.unodc.org/e4j/en/cybercrime/module-4/index.html

- Best parental control software. (n.d.). https://www.qustodio.com/en/premium-special-promo-b/?utm\_source=google&utm\_medium=cpc&utm\_term=brand&utm\_campaign=adw\_ww\_web\_brand\_\_\_brand\_ww-Qustodio-WW-B-Exa-All-DT+TA-SE-RLSA-XX&gclid=Cj0KCQiAv6yCBhCLARIsABqJTjaPeBdtV5cgDIzAjaMMLdFx\_tAjUCoahQuJI1qdbmTqbbDgeIy6TpQaAiJ\_EALw\_wcB&gclsrc=aw.ds

- U. (n.d.). Cybercrime repository. https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html

- F. (2014).

https://www.ecoi.net/en/file/local/1125765/4232\_1417773760\_lebanon.pdf.