Legal measures against cyber crimes

A Leash on Persistent Threats

Legal measures against cyber crimes

With the revolutionary growth in the number of ICT service providers and users, this globally-interconnected digital infrastructure forms a platform for various interactions essential to modern life. Securing this widely employed system of computers has “ traditionally been a battle of wits: the penetrator tries to find the holes, and the designer tries to close them”-Gosser. With the number of such penetrators constantly on the rise and the targets of cyber attacks being so diverse, the frequency of these attacks is seen to increase rapidly with the establishment of sophisticated methods for the execution of the same.

Legal Provisions against a number of Cyber Crimes

“ While a viable cybersecurity policy includes a wide range of considerations, legal measures play a key role in the prevention and combating of cybercrime. In particular, at the national level, cybercrime laws most often concern criminalization – establishing specialized offences for core cybercrime acts.” [1]

Enhancing cybersecurity contributes to the protection of critical information infrastructures thereby ensuring the security and economic well-being of a nation. Moreover, cybersecurity also helps facilitate the development of information technology and the Internet.

1. Illegal Access (Hacking)

A provision on illegal access is included inThe Council of Europe Convention on Cybercrime [2] , protecting the integrity of computer systems by criminalizing unauthorized access to a system. 2002 Commonwealth Model Law's *section 5* also aims to protect computer systems from illegal access. The2005 EU *Article 2 of the* Council Framework Decision on attacks against information systemscontains a provision that allows the criminalizing of such access. Illegal access is a criminal offence according to *Article 3* of the1999 Stanford Draft International Conventionas well. [3]

2. Illegal Remaining

Continuing to remain in a computer system after unauthorized access or expiration of permission also compromises the integrity of such systems. TheConvention on Cybercrimesigned in 2001 saw the addition of a clause that criminalized the " intentional failure to exit a computer system" [4] after inadvertent access.

3. Illegal Acquisition of Computer Data

Legal and regulatory provisions for illegal interceptionare present inThe Council of Europe Convention on Cybercrime, Stanford Draft International Conventionand theCommonwealth Model Law.

§ 1831of theEconomic Espionage Act of 1996protects content of any format, also addressing computer-related offences which are covered by § 1831(a)(2)-(5). *Section 8* of theHIPCAR1475cybercrime legislative text protects the secrecy of stored and protected computer data. S *ection 202a* of theGerman Penal Codealso contained a provision that covers all stored computer data in general that is protected against unauthorized access. [4]

4. Illegal Interception

Numerous providers and a number of points form a part of Internet enabled data transfer processes. The weakest point for interception of these processes remains the user often unequipped with adequate protection against such attacks.

The integrity of nonpublic transmissions is upheld by theThe Council of Europe Convention on Cybercrimecriminalizing such unauthorized interception. 2002 Commonwealth Model Law's *section 8* also functions similarly.

5. Data Interference

Critical business information is stored in digital infrastructure as data. Such information when attacked or accesed without authorization can result in financial losses.

Article 4 of theCouncil of Europe Convention on Cybercrimeprotects the integrity of data against unauthorized interference, providing required protection to computer data and programs. S *ection 6* of the2002 Commonwealth Model Lawfurther also criminalizes both reckless acts. Moreover, this provision mentions in subsection 2 that temporary effects are also covered. [5] The informal1999 Stanford Draft International Conventionlists two provisions that criminalize activities pertaining to data interference " if it interferes with the functioning of a computer system (Article 3, paragraph 1a) or if the act is committed with the purpose of providing false information in order to cause damage to a person or property (Article 3, paragraph 1b)." [4]

6. System Interference

Attacks on computer systems of people, critical infrastructures or businesses offering ICT services can cause serious financial losses and affect other powerful systems as well.

The intentional hindering of authorized use of computer systems is criminalized under *Article 5* of theThe Convention on Cybercrime. [2]

Section 7 of the2002 Commonwealth Model Lawis in line with Article 5 of the Council of Europe Convention on Cybercrime with the addition of the criminalization of reckless acts as well. It also lists more acts in the definition of " hindering". [5] TheEU Council Framework Decisionalso criminalizes illegal data interference in *Article 3* . Also, *Article 3* of the1999 Stanford Draft International Conventioncovers all activities of computer system manipulation.

7. Pornographic material

The criminalization of illegal sexually-explicit content considering its gravity is a must but is seen to differ with countries. An example is the consideration of exchange of pornographic material as a criminal act under 184 of the German Penal Code. [4]

Child Pornography

The prohibition of exchange of child pornographic content aims to decrease the access to such material thereby also avoiding subsequent sexual abuse of children.

In order to facilitate the protection of children against sexual exploitation, theConvention on Cybercrimeincludes “ an article addressing child pornography, criminalizing the abuse of children, as well as traditional methods of distribution of child pornography.” [4] Three subsections on the same can be seen in *paragraph 2* of *Article 9* . *Article 20* also addresses the Protection of Children against Sexual Exploitation and Sexual Abuse. S *ection 10* of the2002 Commonwealth Model Lawalso functions similarly, criminalizing the publishing, production and possession of such material. [5]

8. Copyright Crimes

Digital sources make possible the generation of quality copies of academic work, artwork etc. thereby also increasing copyright violations against them. *Article 10* ofthe Convention on Cybercrime [2] covers such offences.

Conclusion

While aiming to tackle threats of a widespread nature such as cyber crimes, international cooperation is a necessity. Considering the implications cybersecurity has on security, economic prosperity and public safety, each nation will have to develop a strong foundation through its own national cybersecurity strategy and reforms also ensuring effective functioning of said legal measures.

References

[1] Appazov, Artur. (2014). *Legal Aspects of Cybersecurity.* Retreived 9 th May, 2019, fromhttp://www. justitsministeriet.

dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity. pdf

[2] Council of Europe – Convention on Cybercrime ETS No. 185 (2001). Retreived 9 th May, 2019, from

http://www. europarl. europa. eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en. pdf

[3] Abraham D. Sofaer, Gregory D. Grove & George D. Wilson, *Draft International Convention To Enhance Protection from Cyber Crime and Terrorism* , in Abraham D. Sofaer & Seymour E. Goodman, eds., The Transnational Dimension of Cyber Crime and Terrorism, Stanford, CA: Hoover Institution, 2001, pp. 249-265. Retreived 10 th May, 2019, from

http://stanford. edu/~gwilson/Transnatl. Dimension. Cyber. Crime. 2001. p. 249. pdf

[4] A Cyber. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Retreived 9 th May, 2019, from

http://www. itu. int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6. pdf

[5] The Commonwealth Office of Civil and Criminal Justice Reform (Commonwealth Secretariat 2017). *Model Law on Computer and Computer Related Crime.* Retreived 10 th May, 2019, from

http://thecommonwealth.
org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Compute
r_Related_Crime. pdf