**STANDARDIZATION OF THE SRI LANKAN CYBER-CRIME REGIME: THE UNDERLYING PRINCIPLE OF ‘PROPORTIONAL PUNISHMENT’**

***B. Soorya***

*Department of Law, University of Jaffna*

1. **INTRODUCTION**

As Black’s Law Dictionary (1910) defines, a crime “is an act committed or omitted, in violation of public law, either forbidding or commanding it.”[[1]](#footnote-1) ‘Criminal Law’ is the body of legal principles governing the sphere of crimes and its related matters. Generally, criminal prosecutions are undertaken by the State since the crimes are grave as opposed to civil actions. ‘Punishment’ is one of the core principles among Seven[[2]](#footnote-2) related to the Criminal Law, which is the central feature of criminal law to attain its prime objectives of deterrence, retribution, incapacitation, and rehabilitation.

The modern era of the legal jurisprudence has evolved with the development of Information Technology. Since it involves Digital Development, modern crimes significantly vary from more traditional crimes. Further, as modern-day crimes aggregate with the most severe damages to the victims, the urge to standardize the legal framework and the principle of ‘Proportional Punishment’ is paramount to achieve the fundamental objectives of Criminal Law.

The core objectives of this research are,

1. to identify and study the legal frameworks on the cyber-crime regime in Sri Lanka.
2. to analyze and compare such standards along with the principle of ‘Proportional Punishment’.
3. if such measures are unmatched, discuss the adverse effects of such lacunas in the criminal justice system, and
4. to specify the urge to bridge these gaps and sum-up with the possible solutions to overcome.

**2. METHODOLOGY**

This is a qualitative inquiry. The author collected data for this research from primary and secondary sources. Laws passed by the Parliament of Sri Lanka and other countries, International Laws such as conventions, directives, treaties, resolutions, and judicial decisions are the primary sources for the research. Further, the journal articles, statistic reports, and other articles were referred to as the secondary sources through library and digital databases. Moreover, the paper limits its scope to the principle of ‘Proportional Punishment’ in the cyber-crime framework, and future research may resume the substances to develop the cyber-crime regime and new findings.

1. **RESULTS AND DISCUSSION**

The development of the information technology (IT) regime has significantly contributed to the evolution of the world. These developments materially help towards the advancements of the globe in different dimensions on the one hand and, the exploitation and the malfunctions of IT lead results in detrimental consequences such as theft, privacy invasions, cyber-crimes, and many more crimes. Sri Lanka is no exception to these challenges. Computer literacy is consistently in the upward trend in Sri Lanka. During the past decade, there has been a dramatic growth. According to the Department of Census and Statistics of Sri Lanka, the computer literacy among Sri Lankans was 20.3 per cent[[3]](#footnote-3) in 2009 and it came up to 30.1 per cent[[4]](#footnote-4) within a decade. The increasing computer literacy results in the public’s involvement in different cyber-space platforms such as e-commerce, social media, e-documents, e-banking, education through digital platforms, etc.

Since Sri Lanka is emerging through the IT regime as a developing nation, the cyber-space is prone to severe threats in the cyber regime such as cyber defamation, hacking incidents (Example: Hon. Past President Maithripala Sirisena’s Website hacked in November 2016), spreading of fake news and misinformation, scamming (Reported over many years as continues through the methods of E-mail & Mobile SMS), DDoS attacks, intellectual property violations, child-pornography and e-commerce related legal issues (such as consumer protections, return policy, amendment of terms and conditions). As countermeasures, the government has attempted to respond through five primary pieces of legislations[[5]](#footnote-5). Also, the Intellectual Property Act, No. 36 of 2003 relevant to this realm when the cases fall under Intellectual Property law violations. Similarly, to satisfy the emerging need of protecting digital security and cyber privacy, Sri Lanka is going through the process of implementing Personal Data Protection Bill and Cyber Security Bill which are still in the bill stage. However, the Computer Crimes Act (From now on CCA) enacted along with the standards prescribed under the Budapest Convention, is the only piece of legislation which deals with cyber-crimes. Despite the numerous countermeasures, cyber-crimes are continuously reported in Sri Lanka.

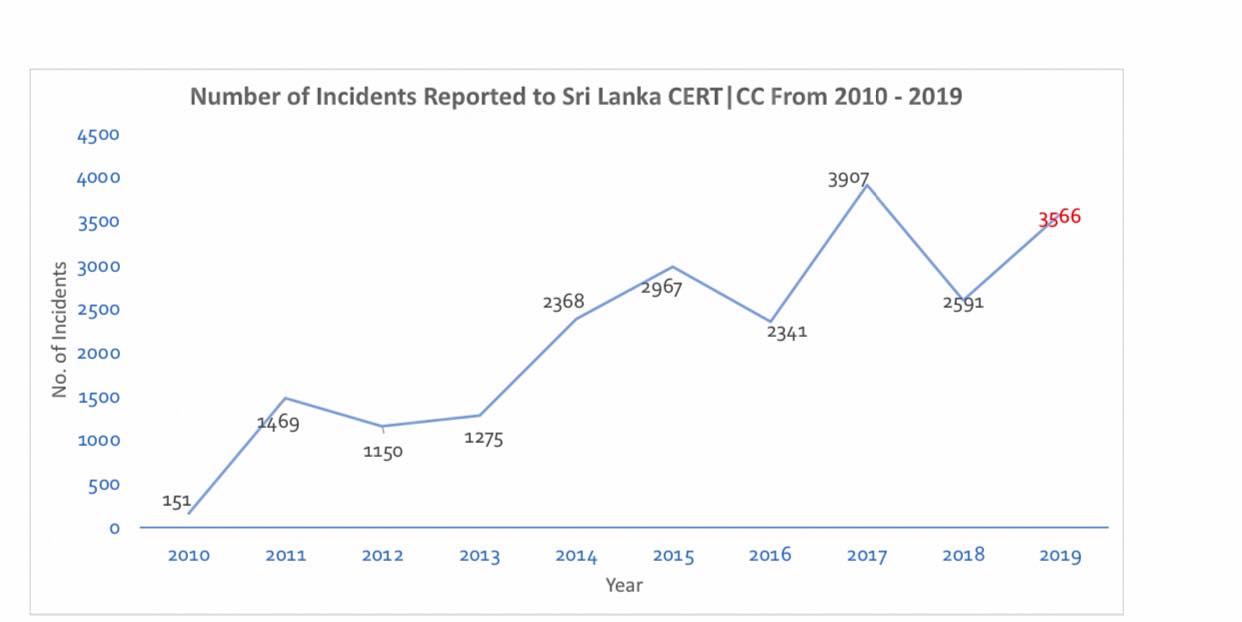


Figure 1. Growth of the number of incidents reported

(Source – SLCERT Annual Activity Report 2019[[6]](#footnote-6))

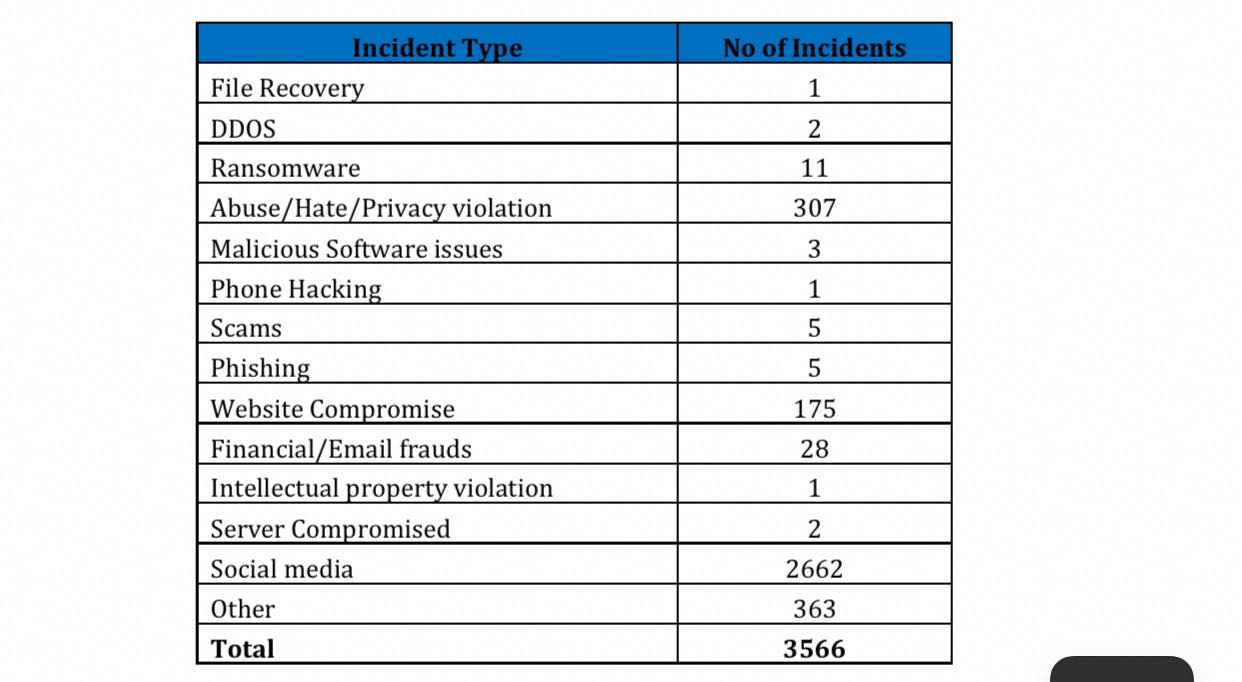


Table 1. Types of incidents reported in 2019

(Source – SLCERT Annual Activity Report 2019[[7]](#footnote-7))

Table 1 lists the types of incidents reported to SLCERT last year (2019) and Figure 1, compares the number of crimes reported to the SLCERT during the previous decade. Even though the trend is not stable, the graph provides an overview of how cyber-security related incidents reported to Sri Lanka have rapidly increased in 2019. In 2019, a total of 3,566 incidents were reported to Sri Lanka CERT while it was 2598 during the year 2018. Further, it would be pertinent to point, the number of reported incidents multiplies by more than twenty times during the last decade (151 Cases in 2010 to 3566 Cases in 2019). The statistics question the effectiveness of the protection framework since the above analysis was done entirely in the post-legislative period of CCA after the Act came into operation in 2007.

Nonetheless, Sri Lanka has many significant drawbacks within its cyber framework such as ambiguous definitions in the legislation, ineffective enforcement mechanism and power devolution, inadequate punishments, the lack of technical facilities and knowledge among practitioners and many[[8]](#footnote-8). The continuing cyber victimizations depict the ineffectiveness of the Sri Lankan cyber framework, and this paper spotlights the problem of inadequate punishments for the offences committed in the cyberspace.

Punishment is the cardinal feature of criminal law, as it aims towards the five core objectives of retribution, deterrence, incapacitation, rehabilitation and restoration. Adequate punishment to the perpetrators is a significant element to achieve these aims. On this regard, the principle of ‘Proportional Punishment’ mandates the standardizations of punishments are to be proportionate to the gravity of the crime[[9]](#footnote-9). The background of this idea is to regulate punishment that should not be too harsh or too lenient for such a crime[[10]](#footnote-10). The punishments for grave offences should be severer than those for minor offences.

In Sri Lanka, the CCA, the solo piece of legislation which deals with cyber-crimes identified various offences as cyber-crimes and listed-out the punishments. This includes unauthorized access to the computer [[11]](#footnote-11)(Generally known as Hacking), unauthorized access in order to commit an offence [[12]](#footnote-12)(computer cracking), unauthorized modification or damage or potential damage to any computer[[13]](#footnote-13), offences committed against national security[[14]](#footnote-14) and a few more. As a quality feature, CCA comprises almost all crimes identified under the Budapest Convention. Also, the Act has a provision for punishments for each offence in the method of either a fine or imprisonment. In addition to the identification of the cyber-crimes and punishments, the Act empowers the court of law to make orders where necessary such as order to pay damages caused to the victim(s) to balance the loss caused by such crimes or order to pay the amount to the State where any unlawful monetary gains accrued to the offender, in addition to the punishment prescribed[[15]](#footnote-15).

|  |  |  |
| --- | --- | --- |
| **CCA Section** | **Offence** | **Punishment(Fine & Imprisonment)** |
| **Section 3** | Unauthorised access to a computer | ≤ 100,000 or 5 Years or Both |
| **Section 4** | Unauthorised access to commit an offence. | ≤ 200,000 or 5 Years or Both |
| **Section 5** | Unauthorised modification or damage or potential damage to any computer | ≤ 300,000 or 5 Years or Both |
| **Section 6** | Offences committed against national security, national economy or public order, | Up to 5 Years |
| **Section 7** | Dealing with data or information unlawfully obtained | ≥100,000 ≤ 300,000 or Not Less than 6 Months and up to 3 Years or Both |
| **Section 8** | Illegal interception of data | ≥100,000 ≤ 300,000 or Not Less than 6 Months and up to 3 Years or Both |
| **Section 9** | Using of illegal devices | ≥100,000 ≤ 300,000 or Not Less than 6 Months and up to 3 Years or Both |
| **Section 10** | Unauthorised disclosure of information enabling access to a service | ≥100,000 ≤ 300,000 or Not Less than 6 Months and up to 3 Years or Both |

Table 2. Offences and Punishments under CCA 2007 of Sri Lanka

As Table 2 lists, the CCA attempts to incorporate the principle of ‘Proportionate Punishment’ within its arrangement since it provides severe punishment for the grave offences and small-scale ones to the minor crimes. The offences such as hacking, cracking, unauthorized modifications such as worm virus, cyber-attacks are generally understood as ‘grave’ since they materially affect the reputation, business or operations adversely in an immense scale. The hacking of the official website of the President of Sri Lanka 2016[[16]](#footnote-16), continuous cyber-attacks including the recent attack on five websites including two government websites[[17]](#footnote-17) are few incidents which hampered the reputation and integrity of the cyber framework and rendered potential losses in Sri Lanka. Therefore the punishments for such offences are comparatively severer with imprisonment up to five years or a fine up to Rs.300, 000. Similarly, minor punishments apply to the small scale offences as illustrated by the Act since its potential damages are comparatively tiny in scale.

However, a more in-depth analysis of CCA provisions reflects that the penalties set out in the Act are fixed and inadequate to combat modern cyber-crimes. The offences listed-out in the Act amount with penalties up to Rs.300, 000 or up to five years of imprisonment. The articulation enables judicial discretion to fix a penalty within these criteria. However, the Act itself failed to articulate and distinguish the different degree of offence (Such as First degree, Second degree) on the grounding of potential damage rendered by such crime. As an example, the Act itself attempts to balance a criminal committed a mobile pay hacking worth Rs.5, 000 with a criminal who committed hacking into the Sri Lankan Central Bank system which rendered a loss of one million Sri Lankan Rupees(As both of them fall under the same category of offences). This approach resembles the failure of the CCA to comply with the principle of ‘Proportionate Punishment’.

Secondly, it is evident that the cyber-crimes are too sensitive and they can cause substantial, reputational and financial damages to victims on a large scale. The various offences prescribed under CCA outbreaks with the losses vary from a small level of monetary damages up to trillions. Reports suggest that the annual cost to the global economy from cybercrime is more than $445 billion, and a conservative estimate would be $375 billion in losses[[18]](#footnote-18). Further, statistics suggest that low and middle-income earning countries, including Sri Lanka, have minor losses, but this will radically change shortly as these countries increase their usages of the Internet[[19]](#footnote-19). However, as a countermeasure, our legal framework prescribes the punishment up to Rs.300, 000 which is drastically low when we compare and contrast with the possible potential damages from these offences. On this ground, the Sri Lankan legal framework should step-up to match the standards of the principle of ‘Proportionate Punishment’ which mandates that the punishment should be adequate to match-up with the possible damages hampered by such offence.

CCA of Sri Lanka is in force for more than a decade, without any substantial amendments. Thus, the urge to refine our framework is recognized to combat modern challenges in the cyberspace. ‘Proportional Punishment’ is a cardinal element to consider for a pragmatic cyber framework in Sri Lanka. Therefore it is necessary to reform our framework by incorporating the principles to achieve the core objectives of criminal law.

On this regard, the United States of America adopts one of the best practices. Though the United States adopts various approaches and laws to countermeasure cybersecurity threats, the Penal Code of the United States fosters the principle of ‘Proportional Punishment” within its articulation as a significant feature.

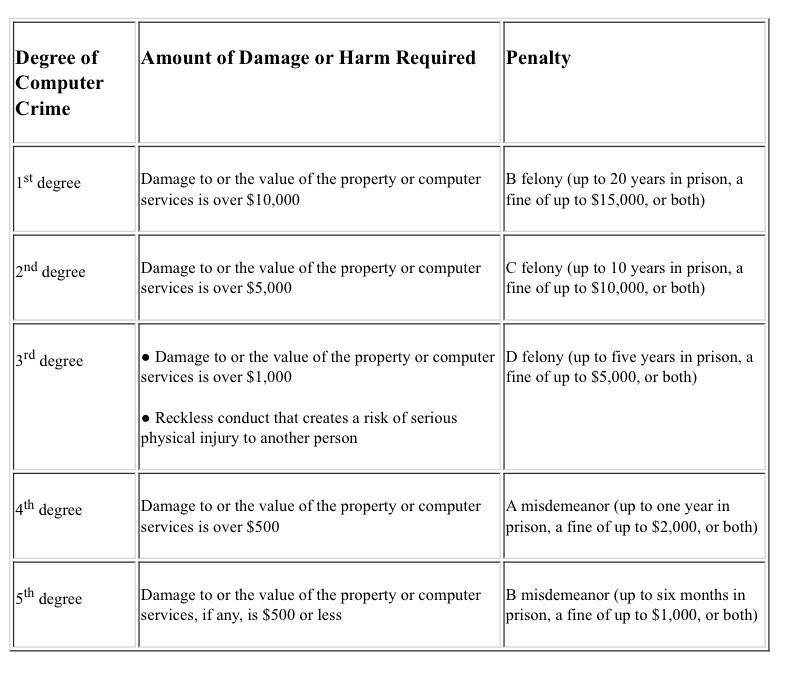


Table 3. Degrees of Computer Crime and the Requirements for Each Penalty in U.S[[20]](#footnote-20)

Source: OLR Research Report[[21]](#footnote-21)

As Table 3 lists, the United States brings up the best practices into the cyber framework through identifying and distinguishing different degrees of the offences and as well as incorporates modern developments through the adequate punishments which are proportionate to the possible potential damages. The framework provides a fine up to 15,000 USD and up to 20 years of imprisonment considering the gravity of the offence which is drastically higher than Sri Lanka which even does not steer up to half a million rupees.

1. **CONCLUSION& RECOMMENDATIONS**

Cyber-space is an emerging platform with modern features which is playing a pivotal role in the digital era. Different sectors are adopting digital platforms as a significant part of their daily routine, specifically after COVID ’19. These platforms are dealing with specific data and information which carry privacy, security and economic values. Therefore it is highly necessary to safeguard these cyber platforms from different security threats.

The study points out the ineffectiveness of the cyber legal framework of Sri Lanka and highlights the need to refine to safeguard the cyber-space from modern security threats. More particularly, the research identifies the failure of incorporating proportional punishment into the cyber framework since the penalties provided by the CCA is inadequate and disproportionate to its possible potential damages.

The findings of this research urge the need to absorb the principle of ‘Proportional Punishment’ in our cyber framework as an efficient countermeasure to combat modern cyber-crimes. The idea could be accompanied by the relevant amendments into the legal framework to overcome the emerging challenges. The proposed strategy will escort the justice system towards the objectives of Criminal Law and empower the development of the country through the pillars of the digital space with high certainty, authenticity, security and reliability.

1. **REFERENCES**

AlthafMarsoof,(2007), ‘Privacy related computer crimes: A critical review of the computer crimes act of Srilanka’

Center for Strategic and International Studies (CSIS) (2019), ‘Net Losses: Estimating the Global Cost of Cybercrime’

Christopher Reinhart, Chief Attorney : OLR Research Report (2012): ‘Penalties for Computer Hacking’ Retrieved: <https://www.cga.ct.gov/2012/rpt/2012-r-0254.htm#:~:text=The%20law%20punishes%20hacking%20under,to%20%2415%2C000%2C%20or%20both).>

DamithWalpita(2019), ‘Are the Sri Lankan Cyber-crime laws Sufficient to safeguard IT Professionals and the victims of cyber-attacks in Sri Lanka?’

Department of Census and Statistics Sri Lanka (2009) - Computer Literacy Statistics. Retrieved: <http://www.statistics.gov.lk/CLS/BuletinComputerLiteracy_2009.pdf>

Department of Census and Statistics Sri Lanka (2019) - Computer Literacy Statistics. Retrieved: <http://www.statistics.gov.lk/education/ComputerLiteracy/ComputerLiteracy-2019Q1-Q2-final.pdf>

Dinithi Jayasekara (2015), Conference Paper on Internet and Law (special Reference to Sri Lanka) Retrieved :<https://medwelljournals.com/abstract/?doi=sscience.2015.841.844>

General Sir John Kotelawala Defence University (KDU) SYNDICTATE 10 INTAKE 28, ‘Cyber Terrorism; Is Sri Lanka Ready?’

JesperRyberg (2004), ‘The Ethics of Proportionate Punishment’ (Kluwer Academic Publishers 2004)

Joel Goh, ‘Proportionality - An Unattainable Ideal in the Criminal Justice System’, Manchester Student Law Review [Vol 2:41]

KalaniKumarasinghe(2020) ; ‘Presidential Poll: A digital wake-up call’- Newspaper Article

KalingaIndatissa, ‘The Law Relating to Computer Crimes and Credit Card Frauds’ (1st edn, KalingaIndatissa 2005)

Perera, W.M. Y. (2017); 'Cyber-attacks: The evolving threat landscape in Sri Lanka’s National Security' 1st International Studies Students’ Research Symposium-2017 (ISSRS 2017)

[Sewmal Tharindu](https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=3301601), (2020), Sufficiency of Sri Lankan Cyber Crime Law ‘Critically Analysis of the Legal Frame Work Applicable to the IT Industry Comparing With European Union Law’, E-Journal Retrieved : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3522038>

SLCERT (2019): Annual Activity Report 2019. Retrieved: <https://www.cert.gov.lk/Downloads/General/Sri_Lanka_CERT_Annual_Activity_Report_2019.pdf>

Sunil D. B Abeyaratne, ‘Introduction to Information and Communication Technology Law’ (1st ed, Sunil D, B. Abeyaratne 2008)

VishniGanepola (2017), ‘Effectiveness of the Existing Legal Framework governing Cyber-Crimes in Srilanka’

1. **ABBREVIATIONS**

CCA- Computer Crimes Act

IT- Information and Technology

SLCERT- Sri Lanka Computer Emergency Readiness Team

1. Black’s Law Dictionary; ‘A **crime** is an act committed or omitted, in violation of a public **law**, either forbidding or commanding it; a breach or violation of some public right or duty due to a *whole community, considered as a community. In its social aggregate capacity, as distinguished from a civil injury*’.(Pp 444-445) [↑](#footnote-ref-1)
2. The other six principles of criminal law are, i. Legality (must be a law); ii.*Actusreus* (Human conduct); iii. Causation (human conduct must cause harm); iv. Harm (to some other/thing); v. Concurrence (State of Mind and Human Conduct) and vi. *Mens Rea* (State of Mind; "guilty mind") [↑](#footnote-ref-2)
3. Department of Census and Statistics Sri Lanka; Computer Literacy Statistics of 2009. [↑](#footnote-ref-3)
4. Department of Census and Statistics Sri Lanka; Computer Literacy Statistics of 2019. [↑](#footnote-ref-4)
5. Information and Communication Technology Act No.27 of 2003; Electronic Transactions Act No. 19 of 2006; Computer Crimes Act No. 24 of 2007; Payment and Settlement Systems Act No. 28 of 2005 and Payment Devices Frauds Act No.30 of 2006. [↑](#footnote-ref-5)
6. SLCERT; Annual Activity Report (2019);(pp. 5) [↑](#footnote-ref-6)
7. SLCERT; Annual Activity Report (2019); (pp. 5) [↑](#footnote-ref-7)
8. VishniGanepola (2017), ‘Effectiveness of the Existing Legal Framework governing Cyber-Crimes in Srilanka’ [↑](#footnote-ref-8)
9. Joel Goh, ‘Proportionality - An Unattainable Ideal in the Criminal Justice System’ , Manchester Student Law Review [Vol 2:41] pp.42 [↑](#footnote-ref-9)
10. JesperRyberg; ‘The Ethics of Proportionate Punishment-A Critical Investigation’; Library of Ethics and Applied Philosophy- Volume 16; pp.1-3 [↑](#footnote-ref-10)
11. Section 3 of CCA [↑](#footnote-ref-11)
12. Section 4 of CCA [↑](#footnote-ref-12)
13. Section 5 of CCA [↑](#footnote-ref-13)
14. Section 6 of CCA [↑](#footnote-ref-14)
15. Section 14 of CCA [↑](#footnote-ref-15)
16. BBC News; ‘Sri Lankan teenager held over hacking of president's website’ on 29 August 2016 [↑](#footnote-ref-16)
17. Daily News, ‘Cyber-attack on two govt. websites’ on May 30 2020 [↑](#footnote-ref-17)
18. CSIS Report “Net Losses: Estimating the Global Cost of Cybercrime” - Economic impact of cybercrime II [↑](#footnote-ref-18)
19. *ibid* [↑](#footnote-ref-19)
20. Penal Code Section 53a-25 of United States [↑](#footnote-ref-20)
21. OLR Research Report on Computer Crimes(2012) [↑](#footnote-ref-21)