මාධ්‍ය සමීක්ෂා - 5

උපදේශක සංස්කරණය

මහින්ද පතිරණ
සභාපති, ශ්‍රී ලංකා පුවත්පත් මණ්ඩලය
ජ්‍යෙෂ්ඨ කථිකාචාර්ය, ශ්‍රී ලංකා සබරගමුව විශ්වවිද්‍යාලය
BA, MPhil (Kelaniya)

සංස්කාරක මණ්ඩලය

සම්මානිත මහාචාර්ය සුනන්ද මහේන්ද්‍ර
BA, MPhil, PhD (London)

මහාචාර්ය ටියුඩර් වීරසිංහ
MA in Journalism, MA in Philosophy, PhD (Moscow)

මහාචාර්ය නිර්මාල් රංජිත් දේවසිරි
BA, M.Phil , PhD (Leiden)

මහාචාර්ය එස්. රඝුරාම්
BSc, MA (India), PhD (India)

ජ්‍යෙෂ්ඨ මාධ්‍යවේදී
ආරියනන්ද දොඹගහවත්ත

ආචාර්ය උදිත ගයාෂාන්
BSc, M.Phil, Dip in Journalism (Colombo), PhD (Kelaniya)

ආචාර්ය සේනානි හරිස්චන්ද්‍ර
BA, MCMS (India), PhD (Kelaniya)

ජ්‍යෙෂ්ඨ කථිකාචාර්ය අරුණ ලොකුලියන
BA, Mphil (Kelaniya)

නීතිඥ ජගත් ලියනාරච්චි
LLB (Colombo), MA (Kelaniya)

නිරෝෂණ තඹවිට
පුවත්පත් කොමසාරිස්, ශ්‍රී ලංකා පුවත්පත් මණ්ඩලය
BA, P.G. Dip (Jayewardenepura)
MA, MPhil (Kelaniya)

සහාය සංස්කරණය

සුරෝෂන ඉරංග
සහකාර පුවත්පත් කොමසාරිස්, ශ්‍රී ලංකා පුවත්පත් මණ්ඩලය
BA (Hons) in Mass Media (Colombo)

දිල්හානි විජේරත්න
සහකාර පුවත්පත් කොමසාරිස්, ශ්‍රී ලංකා පුවත්පත් මණ්ඩලය
BA, P.G. Dip (Jayewardenepura), MSSc (Kelaniya)

මෙහි අන්තර්ගතයේ ශ්‍රී ලංකා පුවත්පත් මණ්ඩලයේ අදහස් පිළිබිඹු නොකරන බවටත් ඉදිරිපත් කර ඇති අදහස් පිළිබඳ වගකීම ඒ ඒ ලේඛකයා සතු බවටත් සැලකිය යුතුය.

මාධ්‍ය සමීක්ෂා - 5

ප්‍රථම මුද්‍රණය: 2023

© ශ්‍රී ලංකා පුවත්පත් මණ්ඩලය

ISBN 978-624-5912-01-8

සෝදුපත් බැලීම	-	ගාමිණී කන්දේපොළ
පරිගණක අක්ෂර සංයෝජනය	-	ඒ.එම්. විදුරංගි වත්සලා
සහාය	-	පවනි නිරාශා ආරියරත්න
		ඩිල්ෂා හර්ෂණී
		පබසරා ෆොන්සේකා
		චතුරිකා උමේෂි
		හිමාෂා කාවින්දි
පිටු සැකසුම	-	දිනුක මලින්ද හේරත්
පිට කවරය	-	දිනුක මලින්ද හේරත්
මුද්‍රණය	-	වාණිජ මුද්‍රණ අංශය,
		සී/ස එක්සත් ප්‍රවෘත්ති පත්‍ර සමාගම.

27

සයිබර් අපරාධ නියාමනයට ශ්‍රී ලංකාවේ සහ ජාත්‍යන්තර අණ පනත්වල උපයෝගිතාව පිළිබඳ විමසුමක්

අමිල ලොකුමාන්නගේ

නව මාධ්‍ය යනු

නව මාධ්‍ය යනු පරිගණකවලට ආවේණික වූ, පරිගණකමය සහ යළි බෙදාහැරීම සඳහා පරිගණක මත යැපෙන මාධ්‍ය ආකාර වේ. දූරකථන (Telephone), පරිගණක (Computer), අතථ්‍ය ලෝක (Virtual World), වෙබ් අඩවි ක්‍රීඩා (Website games), මානව-පරිගණක අතුරුමුහුණත (Human computer interface), පරිගණක සජීවීකරණය (Computer animation) සහ අන්තර්ක්‍රියාකාරී පරිගණක (Interactive computer) ස්ථාපනයන් නව මාධ්‍ය සඳහා උදාහරණ වේ. අන්තර්ජාලය (Internet) යනු ලොව පුරා අන්තර් සම්බන්ධිත පරිගණක ජාලවල ගෝලීය පද්ධතියයි. අන්තර් සම්බන්ධිත අධිපෙළ ලේඛන සහ ලෝක ව්‍යාප්ත වෙබ් යෙදුම් (World Wide Web), විද්‍යුත් තැපැල (e-mail), දූරකථන සහ ලිපිගොනු බෙදාගැනීම වැනි විශාල පරාසයක තොරතුරු සම්පත් සහ සේවාවන් අන්තර්ජාලය දරයි. සමාජ මාධ්‍ය (Social Media) යනු අතථ්‍ය ප්‍රජාවන් (Virtual communities) සහ ජාල (Network) හරහා තොරතුරු, අදහස්, වෘත්තීය අවශ්‍යතා සහ වෙනත් ආකාරයේ ප්‍රකාශන නිර්මාණය කිරීමට සහ බෙදා ගැනීමට පහසුකම් සපයන අන්තර්ක්‍රියාකාරී පරිගණක තාක්ෂණය වේ (වීරමන්ත්‍රි, 1998). අද වන විට අන්තර්ජාලය භාවිත කරන්නන් බිලියන 3.2 ක් පමණ ඇත, දළ වශයෙන් ලෝක ජනගහනයෙන් 40% ද 2020 වන විට, ස්මාර්ට් ජංගම දූරකථන, වැ ඔරලෝසු සාදන්නන් සහ සෞඛ්‍ය ආශ්‍රි උපාංග, රෙදි සෝදන යන්ත්‍ර සහ ශීතකරණ ඇතුළුව අප භාවිත කරන සෑම ඉලෙක්ට්‍රොනි උපාංගයකටම වෙනම අන්තර්ජා ප්‍රොටෝකෝලය (Internet Protocol) ලිපිනය සහ එවැනි උපාංග අන්තර්ජාලයට සම්බන් වනු ඇත. "සම්බන්ධිත උපාංග ගණන" බිලිය 50 දක්වා ළඟා වනු ඇතැයි අපේක්ෂා කෙ (Fernando, 2016).

සයිබර් අපරාධ යනු

Henson, Reyns and Fisher (2011) අනුව, ඔවුන් නිර්වචනය කළේ "සයිබ අපරාධ (Cybercrime) යනු සයිබර් අවකාශ අතථ්‍ය ලෝකයේ සිදුවන ඕනෑම නීති විරෝ ක්‍රියාකාරකමක්" (Henson, Reyns & Fishe 2011). "පරිගණකයක්, ජාලයක් හෝ දෘඩාං උපාංගයක් භාවිතයෙන් පහසුකම් සලසා ඇ හෝ සිදු කරන ලද ඕනෑම අපරාධයක් සයිබ අපරාධ ගණයට ඇතුළත් වේ" (Gordon and Ford, 2006).

සමහර ඇස්තමේන්තු යෝජනා කරන්නේ සයිබර් අපරාධවලින් ගෝලීය ආර්ථික පාඩුව වසරකට බිලියන සිය ගණනක් වෙත ළඟා වන නමුත්, වාර්තාකරණයේ

ලෙහෙනාව නිසා පැහැදිලිව ඇස්තමේන්තු කළ නොහැකි බවයි. සයිබර් අපරාධ ජාත්‍යන්තර සාමයට සහ ස්ථාවරත්වයට ද තර්ජනයක් වන අතර මිලිටරි ගැටුම් සහ දේශපාලන ගැටුම් වැඩි වැඩියෙන් සයිබර් ප්‍රහාර සමඟ ඇත. එබැවින් අපගේ සමකාලීන අන්තර්ජාල යුගයේ සයිබර් අපරාධ යථාර්ථයකි. එය යන්ත්‍රවලට එරෙහි ප්‍රහාර පමණක් නොව ප්‍රජාතන්ත්‍රවාදී සමාජවල මූලික වටිනාකම්වලට තර්ජනයකි. සයිබර් අපරාධවලට සීමා මායිම් නොමැති අතර ලොව පුරා මෙය පෞද්ගලික දත්ත සොරකම්වල ව්‍යාප්තිය මගින් පෙන්නුම් කෙරේ. මාධ්‍ය, සිවිල් සමාජ සංවිධාන, පාර්ලිමේන්තු සහ පුද්ගලයන්ට එරෙහිව සයිබර් ප්‍රහාර හරහා සිදු කරන ලද; රාජ්‍ය ආයතනවලට සහ තීරණාත්මක යටිතල පහසුකම්වලට එරෙහිව සේවා ප්‍රතික්ෂේප කිරීමේ ප්‍රහාර; දරුවන්ට එරෙහි ලිංගික හිංසනය; විජාතික භීතිකාව, ජාතිවාදය සහ අන්තර්ජාලය පදනම් කරගත් රැඩිකල්කරණයේ මෑත කාලීන ප්‍රවණතා; සහ තොරතුරු තාක්ෂණය ත්‍රස්තවාදී අවභාවිතය ඒ අතර වේ.

Norton Cybercrime Report (www.symantec.com) අනුව ලොව පුරා රටවල් 24 කින් (ඕස්ට්‍රේලියාව, බ්‍රසීලය, ඩෙන්මාර්කය, තුර්කිය, දකුණු අප්‍රිකාව, එක්සත් ජනපදය ඇතුළුව) දත්ත අධ්‍යයනය කළ මුළු සංඛ්‍යාව 378 කි. පාරිභෝගික සයිබර් අපරාධ සඳහා දිනකට ගොදුරුවන සංඛ්‍යාව මිලියනයකට අධිකය. මෙම වාර්තාවේ දක්වා ඇති සයිබර් අපරාධවල පිරිවැය අධ්‍යයනය කරන වර්ෂය සඳහා ඩොලර් බිලියන 113 කි. ලතින් ඇමරිකාවේ, තතුබෑම් (Phishing) හේතුවෙන් සෑම වසරකම බැංකු ගනුදෙනුකරුවන්ට ඩොලර් මිලියන 26ක් පමණ අහිමි වේ. ඇස්තමේන්තුගත සමාගම්වලින් සියයට 50ක් 2012 දී අනිෂ්ට මෘදුකාංග ප්‍රහාර (malware attacks) වාර්තා කර ඇත. බ්‍රසීලියානුවෝ මිලියන 22 ක් ද, මෙක්සිකානුවෝද මිලියන 10 ක් සහ කොලොම්බියානුවෝ මිලියන හයක් ද සයිබර් අපරාධවලට ගොදුරු වූහ. The Organization of American හි 2014 වාර්තාව පවසන්නේ සයිබර් අපරාධ වැඩි වී ඇති බවයි. වැඩි සංඛ්‍යාතයකින් සිදුවීම් වන්නේ තතුබෑම් සහ මූල්‍ය වංචා කිරීමට හෝ සමාජ මාධ්‍ය හරහා අනන්‍යතා සොරකම් කිරීමයි (identity theft). සමාජ ජාලවල ව්‍යාප්තිය නිසා අපහාස, තර්ජන සහ සයිබර් හිරිහැර (cyber-bullying) කිරීම් ද ඉහළ ගොස් තිබේ (Fernando, 2016).

Working Group on Internet Governance වාර්තාව (2005) අන්තර්ජාල පාලනයේ ප්‍රධාන ක්ෂේත්‍ර හතරක් හඳුනාගෙන ඇත.

01) යටිතල පහසුකම් සහ තීරණාත්මක අන්තර්ජාල සම්පත් කළමනාකරණය සම්බන්ධ ගැටලු.

02) ජාල ආරක්ෂාව, සහ සයිබර් අපරාධ ඇතුළු අන්තර්ජාල භාවිතය සම්බන්ධ ගැටලු.

03) අන්තර්ජාලයට අදාළ නමුත් අන්තර්ජාලයට වඩා පුළුල් බලපෑමක් ඇති සහ බුද්ධිමය දේපල හිමිකම් (intellectual property rights) හෝ ජාත්‍යන්තර වෙළඳාම (international trade) වැනි පවත්නා සංවිධාන වගකිව යුතු ගැටලු.

04) සංවර්ධනය වෙමින් පවතින රටවල විශේෂයෙන්ම ධාරිතා ගොඩනැගීමේ, අන්තර්ජාල පාලනයේ සංවර්ධන අංශවලට අදාළ ගැටලු (Fernando, 2012).

ශ්‍රී ලංකාවේ සයිබර් අපරාධ සහ නියාමනය

ශ්‍රී ලංකාව තුළ සයිබර් අපරාධ වැළැක්වීම සඳහා ප්‍රධාන පනත් හතරක් භාවිත කර ඇත. ඒ 2007 අංක 24 දරන පරිගණක අපරාධ පනත, 2006 අංක 16 දරන දණ්ඩ නීති සංග්‍රහය

(සංශෝධන) පනත, 2006 අංක 30 දරන ගෙවීම් උපාංග වංචා පනත, 1995 අංක 22 දරන දණ්ඩ නීති සංග්‍රහය (සංශෝධන) ශ්‍රී ලංකා පොලිස් වාර්තා අනුව, සාමාන්‍ය අපරාධ සංඛ්‍යාව අඩු වී ඇති බව පොලිසිය සඳහන් කරයි. එහෙත් අධ්‍යයනය සයිබර් අපරාධ විශ්ලේෂණය කරයි. මෙවැනි අපරාධ ක්‍රමයෙන් වැඩි විය. තතුබෑම්, පෞද්ගලිකත්වය අපයෝජනය, අනිෂ්ට මෘදුකාංග, විද්‍යුත් තැපෑලෙන් හිරිහැර කිරීම, ව්‍යාජ ෆෙස්බුක් ගිණුම් සහ බුද්ධිමය දේපළ පිළිබඳ සිද්ධීන් ශ්‍රී ලංකා පරිගණක හදිසි සූදානම කණ්ඩායම වෙත වාර්තා කර ඇත. මෙම විද්‍යුත් බැංකු සිද්ධීන්ට අමතරව, වෙබ් අඩවි අනවසරයෙන් ඇතුළුවීම (website hacking), විද්‍යුත් තැපෑලෙන් හිරිහැර කිරීම (e-mail harassment), ළමා අසභ්‍ය දර්ශන (child pornography) ශ්‍රී ලංකා පොලිසියේ සයිබර් අපරාධ ඒකකයට වාර්තා වී ඇත (ජයසේකර, 2015).

සයිබර් අපරාධ පනත පුළුල් පරාසයක වැරදි ආවරණය වන අතර එය කාණ්ඩ දෙකකට බෙදිය හැකිය. ඒවා පරිගණක ආශ්‍රිත අපරාධ සහ අනවසරයෙන් ඇතුළුවීමේ වැරදි විය. පරිගණකයකට අනවසරයෙන් ප්‍රවේශ වීම, වරදක් සිදුකිරීම සඳහා අනවසරයෙන් ප්‍රවේශය ලබා ගැනීමට ඕනෑම ක්‍රියාවක් කිරීම, නීත්‍යානුකූල අධිකාරියකින් තොරව පරිගණකයකට කාර්යක් ඉටු කිරීමට සැලැස්වීම, ජාතික ආරක්ෂාවට සහ ජාතික ආර්ථිකයට සහ මහජන සාමයට එරෙහිව සිදු කරන වැරදි, නීති විරෝධී දත්ත සමග කටයුතු කිරීම සහ නීති විරෝධී ලෙස ලබාගත් දත්ත නීති විරෝධී ලෙස බාධා කිරීම, නීති විරෝධී උපාංග භාවිත කිරීම, සේවාවකට ප්‍රවේශය ලබා දෙන තොරතුරු අනවසරයෙන් හෙළිදරව් කිරීම ද වරදකි. 2003 බුද්ධිමය දේපළ පනතේ 36 බුද්ධිමය දේපළ විධිවිධානවල විෂය පථය වැඩි දියුණු කරන ප්‍රතිපාදනයක් පනතේ ඇත. 2006 දී දණ්ඩ නීති සංග්‍රහයට කරන ලද සංශෝධනයකින් සයිබර් කැෆේ වැනි පරිගණක සේවාවක් සපයන සියලුම පුද්ගලයන් සහතික කළ යුතු බව හඳුන්වා දෙන ලදී. ළමයෙකුට සිදුවන ලිංගික අපයෝජන සම්බන්ධ වැරදි සඳහා එවැනි සේවාවක් භාවිත නොකරන බවයි. (ජයසේකර සහ රූපසිංහ 2016)

මීට අමතරව, තොරතුරු සන්නිවේදන හා තාක්ෂණ පනත සහ ඉලෙක්ට්‍රොනික ගනුදෙනු පනත් ද අන්තර්ජාලය පදනම් කරගත් අපරාධ සම්බන්ධයෙන් විශේෂයෙන් කටයුතු කරයි. ඉලෙක්ට්‍රොනික ගනුදෙනු පනත මගින් කොන්ත්‍රාත්තු සැකසීම, දත්ත පණිවිඩ, විද්‍යුත් ලේඛන සහ විද්‍යුත් වාර්තා නිර්මාණය කිරීම සහ හුවමාරු කිරීම සඳහා පහසුකම් සපයයි. මෙම අපරාධ වැළැක්වීම සඳහා දණ්ඩ නීති සංග්‍රහ සංශෝධන සහ සාක්ෂි (විශේෂ විධිවිධාන) පනත (1995 අංක 14) ද භාවිත වේ. දණ්ඩ නීති සංග්‍රහ සංශෝධන 286(ඉ) අනුව "ළමයෙකුට ලිංගික අපයෝජන වැලැක්වීම සඳහා පරිගණකය මගින් සේවාව සපයන පුද්ගලයාගේ රාජකාරිය" හි ප්‍රතිපාදන ඇත. නීතිවිරෝධී අන්තර්ජාල භාවිතයෙන් දරුවන් ආරක්ෂා කර ගැනීමට මෙය උපකාරී වේ (ජයසේකර සහ රූපසිංහ 2016).

ජයසේකර සහ රූපසිංහ 2016 ට අනුව, සයිබර් අපරාධ වැළැක්වීමට සාක්ෂි පනත ද උපකාරී වේ. තෝරාගත් අවස්ථා විශ්ලේෂණය කර සම්මුඛ පරීක්ෂණ පැවැත්වීමෙන් පසු, ඔවුන් යෝජනා කරන්නේ:

01) පෞද්ගලික දත්ත ආරක්ෂණ පනත හඳුන්වා දීම

02) අපහාස නීති ප්‍රතිසංස්කරණය කිරීම සහ සයිබර් අපහාස නීති හඳුන්වා දීම

03) නව මාධ්‍ය සාක්ෂරතාව පිළිබඳ දැනුවත් කිරීම (විශේෂයෙන් භාෂා තුනකින්)

04) විශේෂයෙන්ම දෙමාපියන් සඳහා හඳුන්වා

දී ඇති අන්තර්ජාල ආරක්ෂණ ක්‍රමය

(ඇ) සයිබර් අපරාධ ගැන පැමිණිලි කිරීමට පෙලඹවීම

(ඈ) නිර්පාක්ෂික නොවන අන්තර්ජාල ආචාර ධර්ම පද්ධතියක් හඳුන්වා දීම

නඩු පවරන්නා, විමර්ශකයා සහ විනිශ්චයකරු සම්බන්ධීකරණ ආකාරයෙන් කටයුතු කළ යුතුය. පළපුරුදු පරීක්ෂකයන් සයිබර් අපරාධ සම්බන්ධයෙන් කටයුතු කළ යුතුය. නව මාධ්‍ය සාක්ෂරතාව සහ තොරතුරු තාක්ෂණය පිළිබඳ දැනුවත් කිරීම සයිබර් අපරාධ අවම කිරීමේ එක් ක්‍රමයකි. ඒ වගේම ලංකාවේ නීති පද්ධතියත් වෙනස් කළ යුතුය.

එක්සත් ජාතීන්ගේ මත්ද්‍රව්‍ය හා අපරාධ කාර්යාලය (United Nations Office of Drugs and Crime) (2013) විසින් කරන ලද අධ්‍යයනයකට අනුව "ජාත්‍යන්තර, ජාතික සහ කලාපීය නීති තුළ සයිබර් අපරාධ වැලැක්වීම සහ ඒවාට එරෙහිව සටන් කිරීම සඳහා කාර්යභාරයක් ඉටු කරයි. අපරාධකරණය, කාර්ය පටිපාටික බලතල, අධිකරණ බලය සහ ජාත්‍යන්තර සහයෝගීතාව ඇතුළුව සියලුම ක්ෂේත්‍රයන්හි නීති සම්පාදනය අවශ්‍ය වේ (Fernando, 2016).

අපරාධ නීතිය යනු රාජ්‍යයේ දණ්ඩන බලය නියාමනය කරන නෛතික පද්ධතියේ කොටසක් වන අතර එය ව්‍යවස්ථානුකූල වැදගත්කමක් ඇති වටිනාකම් සහ අවශ්‍යතා ආරක්ෂා කිරීම, සම්බන්ධිත දඬුවම් හෝ ආරක්ෂක පියවර සමඟ නීතිමය ප්‍රතිවිපාක ඇති කරන ඇතැම් හැසිරීම් වැරදි ලෙස අර්ථ දක්වයි. මහජන තොරතුරු වෙත ප්‍රවේශ වීමේ අයිතිය, මහජනතාවට බැඳීමක් ඇති නිල ආයතන හෝ ආයතන සතු දත්ත සහ පොදු වාර්තා වෙත ප්‍රවේශ වීමට සහ පරීක්ෂා කිරීමට සෑම කෙනෙකුගේම වරප්‍රසාදය ලෙස වටහා ගත යුතුය. පොදු කාර්යයන් ක්‍රියාත්මක කරන්නේ කවුරුන්ද යන්න පිළිබඳව සක්‍රීය පරීක්ෂණයක් සිදු කිරීමටත්, තීරණ ගැනීම සඳහා පාලකයන් සහ ආණ්ඩුකාරවරුන් වඩාත් සුදුසු බව ප්‍රවර්ධනය කිරීමටත් ආණ්ඩුකාරයාට අයිතිය තිබේද (Weeramantry, 1998).

අන්තර්ජාලය හා සම්බන්ධ සමහර මානව හිමිකම්වලට ප්‍රකාශනයේ නිදහස, අධ්‍යාපනය, තොරතුරු ලබාගැනීමේ අයිතිය, සංස්කෘතික, භාෂාමය සහ සුළුතර විවිධත්වය ඇතුළත් විය හැකිය. මානව හිමිකම් සහ ශුද්ධ මධ්‍යස්ථභාවය, (ප්‍රවේශ වීමේ අයිතිය, අදහස් ප්‍රකාශ කිරීමේ නිදහස සහ නිර්නාමිකභාවය වැනි) සහ සයිබර් ආරක්ෂාව සමඟ කටයුතු කිරීමේදී සමහර ගැටලු සොයාගත හැකිය (Kurbalija, 2012). එබැවින්, සයිබර් අපරාධ නීතිවල ප්‍රවණතා පිළිබඳ වැඩිදුර සංසන්දනාත්මක පර්යේෂණ සඳහා තොරතුරු සැපයිය හැකිය. 2015 සැප්තැම්බර් 1 වන දින, ශ්‍රී ලංකාව "බුඩාපෙස්ට් සම්මුතිය" (Budapest Convention) ලෙසින් වඩාත් හොඳින් හඳුන්වනු ලබන සයිබර් අපරාධ පිළිබඳ යුරෝපා කවුන්සිලයේ සම්මුතියට රාජ්‍ය පාර්ශවයක් බවට පත් විය. මෙය ඓතිහාසික ප්‍රතිපත්තිමය ජයග්‍රහණයක් වූයේ ශ්‍රී ලංකාව මෙම වැදගත් සම්මුතියට එකඟ වූ දකුණු ආසියාවේ ප්‍රථම රට (ජපානයෙන් පසු ආසියාවේ 2 වැනි රට) බවට පත්වීම නිසාය. ශ්‍රී ලංකාව මෙන්ම ලෝක බැංකු හදිසි ප්‍රතිචාර කණ්ඩායමේ (Computer Emergency Response Team) සහාය ඇතිව මණ්ඩලය බලාත්මක කිරීමේ අධිකාරීන්, බැංකුකරුවන්, පෞද්ගලික අංශය සහ ශාස්ත්‍රාලිකයන්ගෙන් සමන්විතව නිර්මාණය කරන ලදී. තවමත් එම සයිබර් අපරාධ අවම කිරීම සඳහා, සැබවින්ම නව මාධ්‍ය සාක්ෂරතාව (New Media Literacy) සහ තොරතුරු තාක්ෂණ දැනුවත් කිරීමේ වැඩසටහන් සහ නීති පද්ධතිය සඳහා වෙනස් කිරීම් අවශ්‍ය වේ.

ආශ්‍රිත මූලාශ්‍ර

Fernando, J. (2012). Cybercrime Legislation in Sri Lanka. ICTA.

Fernando, J. (2016). The impact of the Budapest Cybercrime convention on Sri Lankan legal system. 28th Anniversary Convention.

Henson, B., Reyns, B., & Fisher, B. (2011). Internet crime. In W. Chambliss (Ed.), Key issues in crime and punishment: Crime and criminal behavior. Sage Publications.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal of Computer Virology, 2(1).

Jayasekara, D. (2015). Internet and law (special reference to Sri Lanka). The Social Sciences, 10(6).

Jayasekara, A. H. D., Rupasinghe, W. (2016). Cyber-crime in Sri Lanka. ww.researchgate.net/publication/294725446.

Kurbalija, J. (2012). Internet Governance. 5th edi. Geneva.

Weeramantry, C. G. (1998). Justice without frontiers: Protecting human rights in the age of technology (Vol. 2). The Hague: Kluwer Law International.