په ا فغانستان کې د سایبري جرمونو د مخنیوي لپاره اغېزمنې لارې چارې؛ ننګونې او فرصتونه

پوهنیار [1]سمیع الله حسن او پوهنیار [2]حبیب الله سلیمانزی ، شیخ زاید پوهنتون، کمپیوټرساینس پوهنځی، د معلوماتي ټکنالوژۍ ځانګه
برېښنالیک: samiullah.szu@gmail.com

لنډیز

په نړۍ کې د ټکنالوژۍ پراختیا له یوې خوا د پرمختګونو لامل شوې، خو له بلې خوا یې د سایبري جرمونو د پراختیا لپاره زمینه برابره کړې ده. په دې څېړنه کې په افغانستان کې د سایبري جرمونو د مخنیوي لپاره د اغېزمنو لارو چارو په برخه کې ننګونې او فرصتونه څېړل شوي دي، چې موخه یې د مؤثرو حل لارو موندل وو. څېړنه د کمي (quantitative) میتود په کارولو سره ترسره شوې، چې په یاده څېړنه کې سروې په لاره اچول شوې وه. په ترڅ کې له ۵۸ ګډونوالو، چې په یاده برخه کې ماهرین وو، سروې کې برخه اخیستې وه. پایلې څرګندوي چې د سایبري امنیت د متخصصینو کمښت، د پرمختللو ټکنالوژیو او زیربناوو نشتوالی، د قوانینو کمزورۍ تطبیق او د خلکو ټیټه پوهه هغه جدي ننګونې دي، چې د سایبري امنیت پر وړاندې موجودې دي. سره له دې، څېړنه د نړیوالو سایبري معیارونو د تطبیق، د ټکنالوژۍ نوښتونو، د عامه پوهاوي د لوړولو او د امنیتي ټکنالوژیو لپاره د بودیجې ځانګړې کولو په ګډون یو شمېر مهم فرصتونه هم په ګوته کوي. څېړنه څرګندوي چې د سایبري امنیت پیاوړتیا د سایبري جرمونو د مخنیوي لپاره بنسټیز رول لري. همداشان دا څېړنه د سایبري امنیت په برخه کې د پالیسیو جوړونکو سره، د پام وړ مرسته کولای شي. د دې څېړنې اهمیت په دې کې دی، چې د افغانستان د سایبري امنیت د حالت د ښه والي لپاره د مهمو ننګونو او فرصتونو پېژندنه کوي.

کلیدي ټکي: افغانستان، سایبري امنیت، سایبري جرمونه، فرصتونه، مخنیوی، ننګونې.

سریزه

بسم الله الرّحمن الرّحیم و الحمدلله ربّ العالمین و الصّلاة و السّلام علی سیدالمرسلین و علی آله و أصحابه أجمعین، اما بعد:

په اوسني دور کې د ټکنالوژۍ چټک پرمختګ سایبري فضا د ګنیو اسانتیاوو ترڅنګ له جدي ګواښونو سره هم مخ کړې ده. په وروستیو کلونو کې سایبري جرمونه په نړۍ کې په بېساري ډول زیات شوي او افغانستان هم له دې ناوړه وضعیت څخه مستثنا نه دی. له همدې امله، د سایبري جرمونو د مخنیوي لپاره د مؤثرو حلالارو موندل یوه جدي اړتیا ده.

دغه څېړنه کې به هڅه وشي، چې په افغانستان کې د سایبري جرمونو د مخنیوي لپاره ځانګړې ننګونې او فرصتونه وڅېړي او د داسې ستراتیژیو وړاندیز وکړي چې په سیمه ییزه او نړیواله کچه اغېزمنې وي. په تېرو لسو کلونو کې، نړۍ د ټکنالوژۍ په سمندر کې لامبو وهي، چې د ډېرو فرصتونو دروازې یې پرانیستې

دي. په ټېرو دوو لسیزو کې د انټرنیټ اهمیت په بې ساري ډول زیات شوی. انټرنیټ نه یوازې د ملتونو د سیالۍ وړتیا لوړه کړې، بلکې د نوښتونو وده یې چټکه کړې، نړیوال اړیکې یې پراخې او اسانه کړې او د خلکو ورځنی ژوند یې د پام وړ بدل او اسانه کړی، همداشان په ننني نښلول شوې نړۍ کې د سایبري بریدونو او ګواښونو ستونزه هم یوه جدي نړیواله مسئله ګرځېدلې ده. دا ګواښونه په څو دقیقو کې پراخه مشکلات رامنځته کولی شي. حکومتونه، سوداګري او افراد په پرمختللو مخابراتي شبکو کې د ذخیره او انتقالېدونکو معلوماتو په کارولو لا ډېر متکي شوي دي[۲،۱]. د سایبري بریدونو له امله رامنځته کېدونکي لګښتونه حیرانوونکي دي، چې په کې د عوایدو له لاسه ورکول، د حساسو معلوماتو افشا، د تجهیزاتو زیان، د خدمتونو بندیدو بریدونه او د شبکې د بندیدو پېښې شاملې دي. په ټېرو څو لسیزو کې، کمپیوټرونو د ټولنې په مختلفو برخو کې له ټمې څخه زیات بدلون راوستی، ټولنیز، اقتصادي او کلتوري واټنونه یې راکم کړي او بې ساري اسانتیاوې یې رامنځته کړې دي. په هر حال، په معلوماتي او کمپیوټري ټکنالوژۍ باندې زیاته تکیه ټولنه د سایبري جرم ګواښ سره مخ کړې ده. د انټرنیټ د اهمیت زیاتوالی او زمونږ پر هغه مخ په ډېریدو تکیه د نوو جرمونو لپاره ګڼ شمېر فرصتونه رامنځته کړي دي. سایبري جرم یوه نړیواله پدیده ده چې نړۍ ته ګڼ شمېر زیانونه رامنځته کوي[۵،۴،۳]. په افغانستان کې هم د انټرنیټ او ټیکنالوژۍ وده په چټکۍ سره روانه ده. سره له دې چې دا پرمختګ ګڼې اسانتیاوې رامنځته کړي، خو له بده مرغه سایبري جرمونه هم په زیاتېدو دي. له همدې امله اړینه ده چې د سایبري جرمونو د مخنیوي لپاره اغېزمنې لارې چارې وڅېړل شي.

موخې: په دې څېړنه کې به په افغانستان کې د سایبري جرمونو د مخنیوي لپاره موجودې ننګونې او فرصتونه وڅېړل شي. همداراز، د سایبري جرمونو د مخنیوي لپاره به اغېزمنې ستراتیژۍ هم وړاندیز شي.

فرعي موخې: د سایبري جرمونو د مخنیوی په لاره کې د موجودو ننګونو څېړل.

- په افغانستان کې دسایبري امنیت په برخه کې د موجودو فرصتونو څېړل.
- د سایبري جرمونو د مخنیوي لپاره د اغېزمنو ستراټژیو وړاندیز کول.

مېتودولوژي: د دې څېړنې لپاره د کمي (quantitative) مېتود کارول شوی، چې د سایبري جرمونو په برخه کې د ننګونو، فرصتونو او اغېزمنو ستراتیژیو د ارزولو لپاره مناسبه لاره ده .د څېړنې د نمونې انتخاب لپاره د (purposive sampling)مېتود کارول شوی. په دې مېتود کې هغه ګډونوال انتخاب شوي چې په افغانستان کې د سایبري امنیت د ننګونو او فرصتونو په اړه مناسبې پوهې او تجربې لري .د څېړنې لپاره پوښتنلیک ترتیب شوی، چې د ګډونوالو نظریات د سایبري امنیت په اړه د مختلفو اړخونو په هکله راټول کړي. د راټول شوو ډاټا تحلیل د احصائیوي تخنیکونو په مرسته ترسره شوی، ترڅو د سایبري جرمونو د مخنیوي په برخه کې د موجودو ننګونو او فرصتونو واضح انځور وړاندې شي.

ټېرو اثارو ته کتنه

د سایبري جرمونو د مخنیوي په اړه ګڼې څېړنې ترسره شوې، چې د دې ستونزې د پېژندلو او د هغې د حل لپاره بېلابېلې لارې چارې وړاندې کوي. څېړنې ښیي چې سایبري جرمونه د ټکنالوژۍ د پراختیا او

د ډیجیټل نړۍ د ودې سره په زیاتېدو دي، چې نه یوازې اقتصادي زیانونه اړوي بلکې د خلکو د شخصي حریم او امنیت لپاره هم جدي ګواښونه دي. سایبري جرمونه په چټکۍ سره زیاتېږي،که څه هم د دې جرمونو بشپړ مخنیوی ستونزمن دی، خو د اغېزو کمولو لپاره اړین تدابیر نیول او د معلوماتو د خوندیتوب لارې تعقیبول اړین دي. سربېره پر دې، د سایبري جرمونو په اړه پوهه او هغه قوانین چې خلک د دې جرمونو پر وړاندې ساتي، د دې جرمونو اغېزې کمولی شي[٦].

د انټرنیټ او سایبري نړۍ پرمختګ یوازې مثبت پرمختګونه رامنځته نه کړل، بلکې ځینې منفي پایلې هم ورسره مل وې. له دغو منفي پایلو څخه یو د سایبري جرمونو زیاتوالی دی. د انټرنیټ د فضا او وخت محدودیت له منځه تلل کولی شي هر څه اغېزمن کړي. بېلابېلې ستراتیژۍ د سایبري جرمونو د مخنیوي لپاره رامنځته شوي دي. سایبري جرمونه یوازې د انټرنیټ له لارې نه ترسره کېږي، بلکې دا د داسې شبکو له لارې هم ترسره کېدای شي چې سیګنالونه انتقالوي، لکه د ټیلیفون اړیکې. د اندونیزیا حکومت د آنلاین جرمونو پر وړاندې د مبارزې لپاره قوانین نافذ کړي دي. ځینې له دغو قوانینو مخکې له مخکې په جزایي قانون کې شامل دي، په ځانګړې توګه د معلوماتو او بربنایي اړیکو قانون د دې سیستم د پلي کولو له لارې، د سایبري جرمونو پېښې هر کال کمېدای شي [٧]. د انټرنیټ کاروونکو لپاره د ټکنالوژۍ د اغېزمنې کارونې په اړه روزنه ضرور دي ، ځکه چې د سایبري جرمونو پر وړاندې مبارزه یوازې د قانون د تنفیذ ادارو مسؤلیت نه دی، بلکې د انټرنیټ د کاروونکو لپاره مناسب او ښه جوړ شوي د پوهاوي پروګرامونه باید طرحه شي[٧]. ملي حکومتونه باید د خلکو د ځان ساتنې د مهارتونو لوړولو لپاره د عامه پوهاوي کمپاینونه پیل کړي چې د آنلاین جرمونو مخه ونیسي. د ساده امنیتي احتیاطي تدابیر نیول، په ځانګړي ډول د ځوانانو ترمنځ، د سایبري جرمونو کچه د پام وړ راکمولی شي. د دې هدف د ترلاسه کولو لپاره د رسنیو له لارې دوامدار کمپاینونه، د تلویزیوني اعلانونو او ځانګړو ویب پاڼو کارول یو له ممکنه لارو څخه دی. په پای کې، د کمپیوټر خوندیتوب په اړه د عامه پوهاوي لوړول نه یوازې د خلکو معلوماتو د غلا مخنیوی کولی شي ، بلکې هغوی د سایبري جرمونو له قرباني کېدو هم ژغوري[٨].

په دې لسیزه کې د انټرنیټ کاروونکو شمېر په بې سارې توګه زیات شوی دی، او دا زیاتوالی په ټوله نړۍ کې روان دی. سایبري بریدونه نه یوازې زیاتېږي، بلکې ورځ تر بلې پیچلي کېږي. له همدې امله، که د دې بریدونو د مخنیوي لپاره مناسبې زیربناوې شتون ونلري، نو ډېره ممکنه ده چې دا بریدونه کشف نه شي. ملي سایبري امنیت پالیسي یوه ستراتیژي ده چې د هېواد د سایبري خطراتو او ګواښونو مخنیوي لپاره ډیزاین شوې. دا پالیسي د اقتصادي او ټولنیزې هوساینې د هڅولو او د سایبري اړوند ټولنو د سایبري خطراتو څخه د ساتنې لپاره کار کوي. د دې پالیسي مهم عناصر عبارت دي له: د حکومت د پالیسۍ ، ادارو همغږۍ پرمختګ او د عامه او خصوصي سکتورونو ترمنځ همکاري پیاوړې کول[٩].

پایلې

د څېړنې اړوند د کمي برخې پایلې په لاندې برخو کې تشریح او خلاصه شوې دي:

- د ګډونوالو پروفایل

ددې څېړنې ګډونوال د عمر له مخې، په درې برخو ویشل شوي دي. له ۱۸ تر ۲۰ کلونو د عمر لرونکي ګډونوال (٦) تنه چې د ټولو ګډونوالو څخه ۱۰،۳ سلنه جوړوي، چې تر ټولو لږ شمېره ده. همداشان له ۲۱ تر ۳۰ کلونو د عمر لرونکي ګډونوال ۲۱ تنه چې د ټولو ګډونوالو ۳٦،۲ سلنه دي، چې د عمر د منځنۍ ډلې استازیتوب کوي. له بلې خوا تر ټولو ډېره برخه ګډونوال د ۳۱ تر ۴۰ کلونو د عمر لرونکي دي، چې شمېر یې ۳۱ تنه چې د ټولو ګډونوالو ۵۳،۴ سلنه ته رسېږي. د زده کړو کچې له مخې، ډېری ګډونوال د ماسټر سند لرونکي دي، چې شمېر یې ۴۱ تنه چې د ټولو ګډونوالو ۷۰،۷ سلنه جوړه وی، په داسې حال کې چې د لیسانس سند لرونکي یوازې ۱۷ تنه چې د ټولو ګډونوالو ۲۹،۳ سلنه جوړوي برخه اخیستې. د دندې په برخه کې، استادان تر ټولو زیاته برخه ګډونوال دي، چې شمېر یې ۳۵ تنه چې د ټولو ګډونوالو ٦۰،۳ سلنه کېږي برخه اخیستې، همداشان د مسلکي کسانو شمېر ۱۱ تنه چې د ټولو ګډونوالو ۱۹،۰ سلنه دي، همدارنګه تخنیکي یا انجینري برخې کارکوونکي ۱۲ تنه چې د ټولو ګډونوالو ۲۰،۷۰ سلنه دي، چې ښیي د څېړنې ګډونوال د سایبري امنیت اړوند موضوعاتو سره پېژندګلوي لري. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۱ جدول کې ښودل شوې ده:

۱ جدول: د ګډونوالو پروفایل

عمومي شاخصونه	فرعي شاخصونه	شمېر	سلنه
عمر	له ۱۸ تر ۲۰ کلونو ترمنځ	٦	۱۰،۳
	له ۲۱ تر ۳۰ کلونو ترمنځ	۲۱	۳٦،۲
	له ۳۱ تر ۴۰ کلونو ترمنځ	۳۱	۵۳،۴
زده کړې	لیسانس	۱۷	۲۹،۳
	ماسټر	۴۱	۷۰،۷
دنده	استاد	۳۵	٦۰،۳
	مسلکي	۱۱	۱۹،۰
	تخنیکي کارکوونکي /انجینر	۱۲	۲۰،۷

د سایبري جرمونو د مخنیوی لپاره فرصتونه او اغېزمنتیا

- **د عامه پوهاوي کمپاینونه**

عامه پوهاوي کمپاینونه د سایبري جرمونو دکمولو لپاره په ېلابېلو کچو اغېزناک ګڼل شوي دي. د ۵۸ تنو ګډونوالو له ډلې څخه ۹ تنو چې د ټولو ګډونوالو ۱۵،۵ سلنه جوړوي، دوي په دې باور دي چې د عامه پوهاوي کمپاینونه د سایبري جرمونو د کمولو لپاره په منځنۍ کچه اغېزناک دي، چې دا د ګډونوالو لږه برخه جوړوي. په ورته وخت کې، ۲۱ ګډونوالو چې د ټولو ګډونوالو ۳٦،۲ سلنه کېږي په دې باور ټینګار کوي چې دا کمپاینونه ډېر اغېزناک دي، چې د ګډونوالو د پام وړ برخه تشکیلوي. د ټولو ګډونوالو تر ټولو زیاته برخه، یعنې ۲۸ تنه چې د ټولو ګډونوالو ۴۸،۳ سلنه کېږي، دوی په دې اند دي چې دا کمپاینونه ډېر زیات اغېزناک دي.

په ټوله کې، د ګډونوالو ګډ نظر څرګندوي چې د عامه پوهاوي کمپاینونه د سایبري جرمونو د کمولو لپاره په لوړه کچه اغېزناک دي، ځکه اکثریت ګډونوال یې د اغېزمنتیا کچه تأییدوي. دغه پایله دا ښیي چې د پوهاوي لوړولو لپاره داسې کمپاینونه کولای شي د خلکو امنیتي چلند کې مثبت بدلون راولي او د سایبري ګواښونو پر وړاندې یو قوي دفاعي دیوال جوړ کړي. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۲ جدول کې ښودل شوې ده:

۲ جدول : د عامه پوهاوي کمپاینونه د سایبري جرمونو د کمولو لپاره څومره اغېزمن دي؟

اندازه ګیری واحد	شمېر	سلنه
متوسط اغېزمن دي	۹	۱۵.۵
ډېر اغېزمن دي	۲۱	۳۶.۲
ډېرزیات اغېزمن دي	۲۸	۴۸.۳
ټول	۵۸	۱۰۰.۰

- **د نړیوالو سایبري امنیتي معیارونو تطبیق**

د نړیوالو سایبري امنیتي معیارونو تطبیق د سایبري جرمونو د کمولو لپاره په بېلابېلو کچو اغېزناک فرصت ګڼل شوی دی. د ۵۸ تنو ګډونوالو له ډلې ٦ تنه چې د ټولو ګډونوالو ۱۰،۳ سلنه کېږي، دوی په دې اند دي چې دا معیارونه لږ اغېزمن دي، چې دا د ګډونوالو لږه برخه جوړوي. په ورته وخت کې ۸ تنه چې د ټولو ګډونوالو ۱۳،۸ سلنه جوړوي، دا معیارونه په متوسطه کچه اغېزمن ګڼلي دي. د ګډونوالو د پام وړ برخه، یعنې ۲۴ تنه چې د ټولو ګډونوالو ۴۲،۴ سلنه کېږي باور لري چې د نړیوالو سایبري امنیتي معیارونو تطبیق ډېر اغېزمن دی. په ورته ډول، ۲۰ ګډونوالو چې د ټولو ګدونوالو۳۴،۵ سلنه جوړوي، دا معیارونه ډېر زیات اغېزمن ګڼلي دي، چې د ګډونوالو د پام وړ برخه تشکیلوي. په ټوله کې، د ګډونوالو ۷۵،۹ سلنه ډېر اغېزمن او یا ډېر زیات اغېزمن د دې معیارونو تطبیق د سایبري امنیت لپاره یو مهم فرصت ګڼلی دی. دغه پایله څرګندوي چې د نړیوالو معیارونو پلي کول کولای شي د سایبري جرمونو په مخنیوي کې مثبت او اغېزناک رول ولوبوي. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۳ جدول کې ښودل شوې ده:

اندازه ګیری واحد	شمېر	سلنه
لږ اغېزمن دي	٦	۱۰.۳
متوسط اغېزمن دي	۸	۱۳.۸
ډېر اغېزمن دي	۲۴	۴۱.۴
ډېرزیات اغېزمن دي	۲۰	۳۴.۵
ټول	۵۸	۱۰۰.۰

۳ جدول: د نړیوالو سایبري امنیتي معیارونو تطبیق

- **د سایبري امنیت لپاره د تخنیکي وړتیاوو لوړول**

د سایبري امنیت لپاره د تخنیکي وړتیاوو لوړول او د متخصصینو روزنه دګډونوالو له نظره په عمومي توګه یو ډېر اغېزناک اقدام ګڼل شوی دی. د ۵۸ ګډونوالو له ډلې ۵ تنو چې د ټولو ګډونوالو ۸،٦ سلنه کېږي دوی په دې نظر دي، چې دا کړنه په متوسطه کچه اغېزمنه ده، چې دا د ګډونوالو لپاره برخه جوړوي. په ورته وخت کې ۱۹ تنو چې د ټولو ګډونوالو ۳۲،۸ سلنه کېږي باور څرګند کړی. چې دا کړنه ډېره اغېزمنه ده، چې د پام وړ برخه ګډونوالو استازیتوب کوي .د ټولو څخه ډېره برخه، یعنې ۳۴ تنه چې دټولو ګډونوالو ۵۸،٦ سلنه جوړوي، باور لري چې د تخنیکي وړتیاوو لوړول او د متخصصینو روزنه ډېر زیات اغېزمنه ده، چې د ګډونوالو د اکثریت نظر ښیي .په ټوله کې، د ګډونوالو ګډ نظر څرګندوي چې د سایبري امنیت د پیاوړتیا لپاره د تخنیکي وړتیاوو لوړول او د متخصصینو روزنه یوه بنسټیزه او ډېره اغېزمنه لار ده، چې کولای شي د سایبري ګواښونو پر وړاندې د ټولنې دفاعي توان زیات کړي. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۴ جدول کې ښودل شوې ده.

۴ جدول : د سایبري امنیت لپاره د تخنیکي وړتیاوو لوړول او د متخصصینو روزنه

اندازه ګیری واحد	شمېر	سلنه
متوسط اغېزمن دي	۵	۸،٦
ډېر اغېزمن دي	۱۹	۳۲،۸
ډېرزیات اغېزمن دي	۳۴	۵۸،٦
ټول	۵۸	۱۰۰،۰

- **د سایبري جرمونو د مخنیوي لپاره د ټکنالوژۍ نوې حل لارې**

د سایبري جرمونو د مخنیوي لپاره د ټکنالوژۍ نوې حل لارې د ګډونوالو له نظره په ټوله کې ډېرې اغېزمنې ګڼل شوې دي. د ۵۸ ګډونوالو له ډلې، ۴ تنو چې د ټولو؛ ګډونوالو ٦،۹ سلنه کېږي، ویلي چې دا حل لارې په متوسطه کچه اغېزمنې دي، چې دا د ګډونوالو لپاره برخه تشکیلوي. په ورته وخت کې۱۷ تنو چې د ټولوګډونوالو ۲۹،۳ سلنه جوړوي باور څرګند کړی، چې دا حل لارې ډېر اغېزمنې دي، چې د پام وړ برخه ګډونوال استازیتوب کوي .د ګډونوالو اکثریت، یعنې ۳۷ تنه چې د ټولو ګډونوالو ٦۳،۸ سلنه کېږي ویلي چې د ټکنالوژۍ نوې حل لارې ډېر زیات اغېزمنې دي، چې د ګډونوالو غالب نظر څرګندوي .په ټوله کې، د ګډونوالو له نظره د ټکنالوژۍ نوې حل لارې د سایبري جرمونو د مخنیوي لپاره یو خورا مهم او اغېزناک اقدام دی، چې کولای شي د سایبري ګواښونو په وړاندې د ټولنې او سازمانونو مقاومت او خوندیتوب زیات کړي. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۵ جدول کې ښودل شوې ده.

۵ جدول: د سایبري جرمونو د مخنیوي لپاره د ټکنالوژۍ نوې حل لارې

اندازه ګیری واحد	شمېر	سلنه
متوسط اغېزمن دي	۴	٦.۹
ډېر اغېزمن دي	۱۷	۲۹.۳
ډېرزیات اغېزمن دي	۳۷	٦۳.۸
ټول	۵۸	۱۰۰.۰

سایبري جرمونو د محنیوي لپاره ننګونې او ستونزې

- د سایبري جرمونو لپاره د قوانینو نشتوالی

د سایبري جرمونو لپاره د ځانګړو قوانینو نشتوالی د ګډونوالو له نظره یوه لویه ننګونه ګڼل شوې ده. د ۵۸ ګډونوالو له ډلې، یواځې ۱ تن چې د ټولو کډونوالو ۱.۷ سلنه کېږي، ویلي چې د قوانینو نشتوالی هیڅ ننګونه نه ده، او بل اړخ ته ۱ تن چې د ټولو ګډونوالو ۱.۷ سلنه جوړوي، فکر کوي چې دا یوازې لږه ننګونه ده .په ټوله کې ۴ ګډونوالو چې د ټولو ګډونوالو ٦.۹ سلنه جوړوي باور لري چې د قوانینو نشتوالی د منځنۍ کچې ننګونه ده. په ورته وخت کې ۲۵ ګډونوالو چې د ټولو ګډونوالو ۴۳.۱ سلنه جوړوي، دوی په دې باور دي چې دا یوه لویه ننګونه ده. تر ټولو ډېره برخه، یعنې ۲۷ ګډونوالو چې د ټولو ګډونوالو ۴٦.٦ سلنه کېږي دوی باور لري چې د سایبري جرمونو لپاره د ځانګړو قوانینو نشتوالی ډېره لویه ننګونه ده.په ټوله کې، د ګډونوالو ۸۹.۷ سلنه لویه یا ډېره لویه ننګونه د قوانینو نشتوالی د سایبري جرمونو په مخنیوي کې یوه جدي او لویه ننګونه ګڼي. دا څرګندوي چې د ځانګړو قوانینو نشتوالی یو له اساسي مشکلاتو څخه دی، چې د سایبري جرمونو په وړاندې د اغېزمنو اقداماتو او چلندونو په رامنځته کولو کې خنډ ګرځېدلی دی. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ٦ جدول کې ښودل شوې ده.

٦ جدول: د سایبري جرمونو لپاره د قوانینو نشتوالی

اندازه ګیری واحد	شمېر	سلنه
هیڅ ننګونه نه ده	۱	۱.۷
لږه ننګونه ده	۱	۱.۷
منځنۍ کچه ننګونه ده	۴	٦.۹
لویه ننګونه ده	۲۵	۴۳.۱
ډېره لویه ننګونه ده	۲۷	۴٦.٦
ټول	۵۸	۱۰۰.۰

- **د قوانینو کمزوری تطبیق**

د قوانینو کمزوری تطبیق د سایبري جرمونو په مخنیوي کې د ګډونوالو له نظره یوه جدي ستونزه ګڼل شوې ده. د ۵۸ ګډونوالو له ډلې، یواځې ۲ تنو چې د ټولو ګډونوالو ۳،۴ سلنه جوړوي، ویلي چې د قوانینو کمزوری تطبیق هیڅ ننګونه نده، او ۱ تن چې د ټولو ګډونوالو ۱،۷ سلنه کېږي فکر کوي چې دا یوازې لږه ننګونه ده .په ټوله کې، ۲ ګډونوالو چې ۳،۴ سلنه کېږي باور لري چې د قوانینو کمزوری تطبیق د منځنۍ کچې ننګونه ده. په بل اړخ کې، ۱۷ ګډونوالو چې د ټولو ګډونوالو ۲۹،۳ سلنه کېږي په دې باور دي چې دا یوه لویه ننګونه ده. تر ټولو ډېره برخه، یعنې ۳۶ ګډونوالو چې د ټولو ګډونوالو ۶۲،۱ سلنه کېږي باور لري چې د قوانینو کمزوری تطبیق ډېره لویه ننګونه ده .په ټوله کې، د ګډونوالو ۹۱،۴ سلنه د قوانینو کمزوری تطبیق د سایبري جرمونو په مخنیوي کې یوه جدي ستونزه ګڼي. د پورته پایلو خلاصه د شمېر او سلنې له مخې په لاندې ۷ جدول کې ښودل شوې ده.

۷ جدول: د قوانینو د تطبیق کمزوري

اندازه ګیری واحد	شمېر	سلنه
هیڅ ننګونه نه ده	۲	۳،۴
لږه ننګونه ده	۱	۱،۷
منځنۍ کچې ننګونه ده	۲	۳،۴
لویه ننګونه ده	۱۷	۲۹،۳
ډېره لویه ننګونه ده	۳۶	۶۲،۱
ټول	۵۸	۱۰۰،۰

- **په قانون پلي کوونکو ادارو کې د تخنیکي پوهې کمښت**

د قانون پلي کونکو ادارو د تخنیکي پوهې کمښت د سایبري جرمونو په مخنیوي کې د ګډونوالو له نظره یوه جدي ننګونه ګڼل شوې ده. د ۵۸ ګډونوالو له ډلې، ۵ تنو چې د ټولو ګډونوالو ۸،۶ سلنه کېږي، ویلي چې د تخنیکي پوهې کمښت د منځنۍ کچې ننګونه ده. ۱۸ تنه چې د ټولو ګډونوالو ۳۱ سلنه جوړوي، باور لري چې دا یوه لویه ننګونه ده .تر ټولو ډېره برخه، یعنې ۳۵ ګډونوال چې د ټولو ګډونوالو ۶۰،۳ سلنه جوړوي باور لري چې د قانون پلي کونکو ادارو د تخنیکي پوهې کمښت ډېره لویه ننګونه ده. په ټوله کې، د ګډونوالو ۳،۹۱ سلنه د دې کمښت د سایبري جرمونو د مخنیوي لپاره یوه جدي ننګونه ګڼي، چې ښیي د قانون پلي کونکو ادارو د تخنیکي پوهې پراختیا د سایبري جرمونو د مخنیوي لپاره خورا اړینه ده. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۸ جدول کې ښودل شوې ده.

۸جدول: د تخنیکي پوهې کمښت په قانون پلي کونکو ادارو کې

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	۵	۸.٦
لویه ننګونه ده	۱۸	۳۱.۰
ډېره لویه ننګونه ده	۳۵	٦۰.۳
ټول	۵۸	۱۰۰.۰

- **د امنیتي ټکنالوژیو نشتوالی**

د پرمختللو امنیتي ټیکنالوژیو نشتوالی د سایبري جرمونو په مخنیوي کې د ګډونوالو له نظره یوه جدي ستونزه ګڼل شوې ده. د ۵۸ ګډونوالو له ډلې، ٦ تنو چې د ټولو ګډونوالو ۱۰.۳ سلنه کېږي، ویلي چې د پرمختللو امنیتي ټکنالوژیو نشتوالی د منځنۍ کچې ننګونه ده. ۲۱ ګډونوالو چې ۳٦.۲ سلنه کېږي، باور لري چې دا یوه لویه ننګونه ده. تر ټولو ډېره برخه، یعنې ۳۱ ګډونوالو چې ۵۳۰.۴ سلنه کېږي باور لري چې د پرمختللو امنیتي ټکنالوژیو نشتوالی ډېره لویه ننګونه ده .په ټوله کې، د ګډونوالو زیاته برخه د دې نشتوالي د سایبري جرمونو د مخنیوي لپاره یوه جدي ستونزه ګڼي، چې ښیي د پرمختللو امنیتي ټیکنالوژیو پراختیا او شتون د سایبري جرمونو په مخنیوي کې خورا مهم دی. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۹ جدول کې ښودل شوې ده.

۹ جدول: د امنیتي ټیکنالوژیو نشتوالی

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	٦	۱۰.۳
لویه ننګونه ده	۲۱	۳٦.۲
ډېره لویه ننګونه ده	۳۱	۵۳.۴
ټول	۵۸	۱۰۰.۰

- **د سایبري امنیت متخصصینو کمښت**

د سایبري امنیت متخصصینو کمښت د سایبري جرمونو په مخنیوي کې د یوې جدي ننګونې په توګه ارزول شوی دی. د ۵۸ ګډونوالو له ډلې، ۵ تنو چې ټولو ګډونوالو ۸.٦ سلنه جوړوي ویلي، چې د متخصصینو کمښت د منځنۍ کچې ننګونه ده. ۱۸ ګډونوال چې ۳۱ سلنه کېږي باور لري چې دا یوه لویه ننګونه ده. تر ټولو ډېره برخه، یعنې ۳۵ ګډونوال چې د ټولو ګډونوالو ٦۰.۳ سلنه جوړوي، باور لري چې د سایبري امنیت متخصصینو کمښت ډېره لویه ننګونه ده .په ټوله کې، د ګډونوالو ۳.۹۱ سلنه د سایبري امنیت متخصصینو کمښت د سایبري جرمونو د مخنیوي لپاره یوه جدي ننګونه ګڼي، چې ښیي د سایبري امنیت په برخه کې متخصصین مهم دي او د هغوی کمښت د ګواښونو د مخنیوي لپاره یوه

لویه ستونزه جوړوي. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۱۰ جدول کې ښودل شوې ده.

۱۰ جدول: د سایبري امنیت متخصصینو کمښت

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	۵	۸،٦
لویه ننګونه ده	۱۸	۳۱،۰
ډېره لویه ننګونه ده	۳۵	٦۰،۳
ټول	۵۸	۱۰۰،۰

- **د کافي وسایلو نشتوالی**

د سایبري بریدونو د کشف او غبرګون لپاره د کافي وسایلو نشتوالی د سایبري جرمونو په مخنیوي کې د جدي ننګونې په توګه ارزیابي شوی دی. د ۵۸ ګډونوالو له ډلې، ۵ تنو چې ۸،٦ سلنه کېږي ویلي چې د وسایلو نشتوالی د منځنۍ کچې ننګونه ده. ۱۷ ګډونوال چې د ټولو ګډونوالو ۲۹،۳ سلنه کېږي دا لویه ننګونه ګڼلې او تر ټولو ډېره برخه، یعنې ۳٦ تنه چې د ټولو ګډونوالو ٦۲،۱ سلنه جوړوي د دې نشتوالي یې ډېره لویه ننګونه بللې ده .په ټوله کې، اکثریتو ګډونوالو د کافي وسایلو نشتوالی د سایبري بریدونو د کشف او غبرګون لپاره یوه جدي ننګونه ګڼلې ده، چې ښیي د دې وسایلو شتون د سایبري جرمونو د مخنیوي لپاره ډېر مهم دی. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۱۱ جدول کې ښودل شوې ده.

۱۱ جدول: د کافي وسایلو نشتوالی

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	۵	۸،٦
لویه ننګونه ده	۱۷	۲۹،۳
ډېره لویه ننګونه ده	۳٦	٦۲،۱
ټول	۵۸	۱۰۰،۰

- **د خلکو ټیټ پوهاوی**

د خلکو ټیټ پوهاوی د سایبري جرمونو په مخنیوي کې یوه جدي ستونزه بلل شوې ده. د ۵۸ ګډونوالو له ډلې، ۵ تنو چې د ټولو ګډونوالو ۸،٦ سلنه کېږي ویلي چې ټیټ پوهاوی د منځنۍ کچې ننګونه ده. ۱۹ ګډونوال چې د ټولو ګډونوالو ۳۲،۸ سلنه کېږي دا ستونزه لویه ننګونه ګڼلې او تر ټولو ډېره برخه، یعنې ۳۴ ګډونوالو چې ۵۸،٦ سلنه جوړوي، دوی دا ډېره لویه ننګونه بللې ده. په ټوله کې، د څېړنې پایلې ښیي، چې اکثریت ګډونوال په دې باور دي چې د خلکو ټیټه پوهاوی د سایبري جرمونو د

مخنیوي لپاره یوه جدي ستونزه ده، چې ښیي د سایبري امنیت په اړه د خلکو پوهاوی زیاتول اړین دي. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۱۲ جدول کې ښودل شوې ده.

۱۲ جدول: د خلکو ټیټه پوهاوی او غیر مسؤلانه چلند

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	۵	۸.٦
لویه ننګونه ده	۱۹	۳۲.۸
ډېره لویه ننګونه ده	۳۴	۵۸.٦
ټول	۵۸	۱۰۰.۰

- **د افرادو غیر مسؤلانه سایبري چلند**

د افرادو غیر مسؤلانه سایبري چلند د سایبري جرمونو په مخنیوي کې یوه جدي ننګونه بلل شوې ده. د ۵۸ ګډونوالو له ډلې، ۵ تنو چې ۸.٦ سلنه جوړوي، ویلي چې غیر مسؤلانه سایبري چلند د منځنۍ کچې ننګونه ده. ۱۷ ګډونوال چې د ټولو ګډونوالو ۲۹.۳ سلنه جوړوي دا لویه ننګونه ګڼلې او تر ټولو ډېره برخه، یعنې ۳٦ تنه ګډونوال چې د ټولو ګډونوالو ٦۲.۱ سلنه جوړوي، دوی په دې نظر دي چې دا ډېره لویه ننګونه ده .په ټوله کې، د ګډونوالو ۴.۹۱ سلنه د افرادو غیر مسؤلانه سایبري چلند د سایبري جرمونو د مخنیوي لپاره یوه جدي ننګونه ګڼي، چې ښیي د سایبري چلند د مسؤولیت پوهاوي ته اړتیا ده. د پورته پایلو خلاصه په لاندې ۱۳ جدول کې ښودل شوې ده.

۱۳جدول: د افرادو غیر مسؤلانه سایبري چلند

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	۵	۸.٦
لویه ننګونه ده	۱۷	۲۹.۳
ډېره لویه ننګونه ده	۳٦	٦۲.۱
ټول	۵۸	۱۰۰.۰

- **د سایبري امنیت لپاره د بودیجې کموالی**

د سایبري امنیت لپاره د بودیجې کموالی د سایبري جرمونو په مخنیوي کې یوه جدي ستونزه بلل شوې ده. د ۵۸ ګډونوالو له ډلې، ۴ تنو چې ٦.۹ سلنه کېږي ویلي چې د بودیجې کموالی د منځنۍ کچې ستونزه ده. ۲۰ ګډونوالو چې دټولو ګډونوالو ۳۴.۵ سلنه ګیږي دا لویه ستونزه ګڼلې او تر ټولو ډېره برخه، یعنې ۳۴ تنه ګډونوال چې د ټولو ګډونوالو ۵۸.٦ سلنه جوړوي، دوی دا ډېره لویه ستونزه بللې ده .په ټوله کې، د ګډونوالو اکثریت د بودیجې کموالي ته د سایبري امنیت د پرمختګ لپاره یوه جدي ستونزه ګڼي. د پورته پایلو خلاصه په لاندې ۱۴ جدول کې ښودل شوې ده.

۱۴ جدول: د سایبري امنیت لپاره د بودیجې کموالی

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	۴	٦.۹
لویه ننګونه ده	۲۰	۳۴.۵
ډېره لویه ننګونه ده	۳۴	۵۸.٦
ټول	۵۸	۱۰۰.۰

- **د زیربناوو کمزورتیا**

د زیربناوو کمزورتیا د سایبري جرمونو په مخنیوي کې یوه جدي ستونزه ګڼل شوې ده. د څېړنې یایلې ښیي، چې د ۵۸ ګډونوالو له ډلې، ۵ تنو چې د ټول ګډونوالو ۸.٦ سلنه کېږي، ویلي چې دا موضوع د منځنۍ کچې ستونزه ده. همداشان ۲۰ ګډونوالو چې د ټول ګډونوالو ۳۴.۵ سلنه جوړوي دوی په دې باور دي چې دا "لویه ستونزه" ده. ورته ډول تر ټولو ډېره برخه، یعنې ۳۳ تنو ګډونوالو چې د ټولو ګډونوالو ۵٦.۹ سلنه کېږي، دوی په دې نظر دي چې دا ډېره لویه ستونزه ده .په ټوله کې، د ګډونوالو ۴.۹۳ سلنه د زیربناوو کمزورتیا یوه جدي ستونزه ګڼي چې د سایبري امنیت په ښه کولو او سایبري جرمونو د مخنیوي په لاره کې خنډ جوړوي. د پورته پایلو خلاصه او د شمېر او سلنې له مخې په لاندې ۱۵ جدول کې ښودل شوې ده.

۱۵ جدول: د زیربناوو کمزورتیا

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې ننګونه ده	۵	۸.٦
لویه ننګونه ده	۲۰	۳۴.۵
ډېره لویه ننګونه ده	۳۳	۵٦.۹
ټول	۵۸	۱۰۰.۰

- **د سایبري امنیت د پوهاوي کمپاینونو اړتیا**

د دې پوښتنې له مخې، د ګډونوالو لویه برخه (۴.۹۱) په افغانستان کې د سایبري امنیت د پوهاوي کمپاینونو ته اړتیا ګڼي. د ۵۸ ګډونوالو له ډلې، ۵ تنه چې د ټولو ګډونوالو ۸.٦ سلنه جوړوي ویلي، چې دې کمپاینونو ته د منځنۍ کچې اړتیا ده، ۱۷ ګډونوال چې د ټولو ګډونوالو ۲۹.۳ سلنه جوړوي دا یې ډېره اړتیا بللې او تر ټولو ډېره برخه، یعنې ۳٦ ګډونوال چې د ټولو ګډونوالو ٦۲.۱ سلنه جوړوي دا یې ډېره زیاته اړتیا بللې ده .په ټوله کې، د ګډونوالو ټولیز نظر ښیي، چې د سایبري امنیت د پوهاوي کمپاینونو ته په افغانستان کې یوه جدي اړتیا شته، چې باید د خلکو پوهاوی زیات شي ترڅو د سایبري جرمونو مخه ونیول شي. د پورته پایلو خلاصه په لاندې ۱٦ جدول کې ښودل شوې ده.

۱۶ جدول: د سایبري امنیت د پوهاوي کمپاینونو اړتیا

اندازه گیری واحد	شمېر	سلنه
د منځنۍ کچې اړتیا ده	۵	۸.۶
ډېره اړتیا ده	۱۷	۲۹.۳
ډېره زیاته اړتیا ده	۳۶	۶۲.۱
ټول	۵۸	۱۰۰.۰

مناقشه

په افغانستان کې د سایبري امنیت د ننګونو او فرصتونو په اړه زموږ څېړنه څرګندوي، چې د سایبري جرمونو د مخنیوي لپاره د عامه پوهاوي، قوانین، ټکنالوژۍ او زیربناوو د کمښت په برخه کې ګڼې جدي ننګونې شتون لري. د معلوماتو تحلیل ښیي چې په ګډونوالو کې ډېری باور لري چې د سایبري جرمونو د مخنیوي لپاره د نړیوالو سایبري امنیتي معیارونو تطبیق، د متخصصینو روزنه او د پرمختللو ټکنالوژیو کارونه ډېر اغېزمن فرصتونه دي. خو په ورته وخت کې، د خلکو ټیټه پوهه، د قانون پلي کونکو ادارو تخنیکي کمزورتیا، او د بودیجې کمبالی د سایبري امنیت د ښه والي په وړاندې جدي ننګونې ګڼل شوي دي. د سایبري بریدونو د کشف او غبرګون لپاره د کافي وسایلو نشتوالی هم د ګډونوالو له نظره یوه جدي ستونزه ګڼل شوې ده. سربېره پر دې، د زیربناوو کمزورتیا او د سایبري امنیت لپاره د بودیجې نشتوالی د سایبري امنیت په برخه کې د جدي ستونزو په توګه یاد شوي دي. په افغانستان کې د سایبري امنیت د پوهاوي کمپاینونو ته اړتیا د ګډونوالو له نظره په لوړه کچه ارزول شوې، چې ۶۲.۱ سلنه یې دا ډېره زیاته اړتیا بولي. دا څرګندوي چې د سایبري جرمونو په وړاندې د عامه پوهاوي کچه لوړول د دې ستونزې د حل لپاره اړین دي.

نتیجه‌گیري

د څېړنې پایلې څرګندوي چې د سایبري امنیت د ښه والي لپاره په افغانستان کې جدي ستونزې او فرصتونه شتون لري. د خلکو ټیټ پوهاوی، د متخصصینو کمښت، د زیربناوو کمزورتیا او د قوانینو کمزوری تطبیق هغه ننګونې دي چې د سایبري جرمونو د زیاتېدو سبب شوي دي. له بلې خوا، د نړیوالو سایبري امنیتي معیارونو تطبیق، د ټکنالوژۍ پرمختللې حل‌لارې، او د متخصصینو روزنه هغه فرصتونه دي چې د سایبري امنیت د ښه‌والي لپاره کولای شي ګټور ثابت شي. دغه څېړنه وړاندیز کوي چې د سایبري امنیت د پوهاوي کمپاینونه دې زیات شي، د قانون پلي کوونکو ادارو تخنیکي وړتیاوې لوړې شي او د سایبري جرمونو د مخنیوي لپاره کافي بودیجه ځانګړې شي. په ورته وخت کې، د نړیوالو معیارونو منل او د پرمختللو ټکنالوژیو کارونه باید په لومړیتوب کې راوستل شي.

خلاصه

دغه څېړنه په افغانستان کې د سایبري جرمونو د مخنیوي لپاره اغېزمنو لارو چارو ته کتنه کوي او د دې لارو چارو سره تړلې ننګونې او فرصتونه تحلیل کوي. د څېړنې پایلې څرګندوي، چې په افغانستان کې د

سایبري جرمونو زیاتوالی د ټیټ پوهاوي، د متخصصینو کمښت، د زیربناوو کمزورتیا او د قوانینو د کمزوري تطبیق له امله رامنځته شوی دی. دغه ننګونې د سایبري امنیت په برخه کې د جدي ستونزو سبب ګرځي. له بلې خوا، د نړیوالو سایبري امنیتي معیارونو تطبیق، د پرمختللې ټکنالوژۍ کارول او د متخصصینو روزنه هغه فرصتونه دي چې د سایبري امنیت د ښه‌والي لپاره اغېزمنې او ګټورې لارې چارې برابرولی شي. څېړنه وړاندیز کوي چې د سایبري امنیت د پوهاوي کمپاینونه باید زیات شي، د قوانینو پلي کول باید قوي شي او کافي بودیجه دې ځانګړې شي، ترڅو د سایبري جرمونو مخه ونیول شي. همدارنګه، د سایبري ګواښونو سره مبارزه کې د نړیوالې همکارۍ زیاتوالی او د پرمختللو ټکنالوژیو کارول باید د لومړیتوب په توګه ونیول شي.

مأخدونه

1. Oloyede A, Ajibade I, Phillips A, Shittu O, Taiwo E, Kizor-Akaraiwe S. A Review of Cybersecurity as an Effective Tool for Fighting Identity Theft Across the United States. A. Oloyede, I. Ajibade, C. Obunadike, Phillips, O. Shittu, E. Taiwo and S. Kizor-Akaraiwe (2023): A Review of Cybersecurity as an Effective Tool for Fighting Identity Theft across United States, International Journal on Cybernetics and Informatics (IJCI). 2023 Oct 14;12(5).

2. Phillips A, Ojalade I, Taiwo E, Obunadike C, Oloyede K. Cyber-Security Tactics in Mitigating Cyber- Crimes: A Review and Proposal. International Journal on Cryptography and Information Security (IJCIS). 2023;13(2/3).

3. Awhefeada UV, Bernice OO. Appraising the laws governing the control of cybercrime in Nigeria. Journal of Law and Criminal Justice. 2020 Jun;8(1):30-49. Nigeria," J. LAW Crim. JUSTICE, vol. 8, no. 1, 2020, doi: 10.15640/jlcj.v8n1a3.

4. Chaubey RK. An Introduction to Cyber Crime and Cyber Law. Kamal Law House; 2009.

5. Okutan A. A framework for cyber-crime investigation. Procedia Computer Science. 2019 Jan 1;158:287-94.

6. Viraja VK, Purandare P. A qualitative research on the impact and challenges of cybercrimes. In Journal of Physics: Conference Series 2021 Jul 1 (Vol. 1964, No. 4, p. 042004). IOP Publishing.

7. Siahaan AP. Yasmirah Mandasari-Cyber Crime Prevention Strategy in Indonesia.

8. Buono L. Fighting cybercrime through prevention, outreach and awareness raising. InERA Forum 2014 Jun (Vol. 15, No. 1, pp. 1-8). Berlin/Heidelberg: Springer Berlin Heidelberg.

9 Alghamdi MI. A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security. Webology. 2020 Dec 1;17(2)

Effective Strategies for Preventing Cybercrimes in Afghanistan: Challenges and Opportunities

Teaching assistant Samiullah Hassan[1], Shaikh Zayed University, Faculty of Computer Science, Department of Information Technologies.
Teaching assistant Habibullah Slimanzai[2], Shaikh Zayed University, Faculty of Computer Science, Department of Information Technologies
Emails: samiullah.szu@gmail.com and habibullah.slimanzai@gmail.com

Abstract
The development of technology worldwide has led to advancements, but it has also created opportunities for the expansion of cybercrimes. This research examines the challenges and opportunities in implementing effective strategies to prevent cybercrimes in Afghanistan, intending to identify practical solutions. The research was conducted using a quantitative method, including a survey of 58 experts in the field. The findings reveal that significant cyber security challenges include a shortage of cyber security professionals, a lack of advanced technologies and infrastructure, weak law enforcement, and low public awareness. Despite these challenges, the study highlights several important opportunities, such as adopting international cyber security standards, fostering technological innovations, increasing public awareness, and allocating budgets specifically for security technologies. The study underscores how crucial it is to improve cyber security to prevent cybercrimes. It also provides insightful information for policymakers involved in cyber security. The research being conducted is essential because it uncovers significant challenges and opportunities to enhance Afghanistan's cyber security landscape.

Keywords: Afghanistan, Challenges, Cybercrimes, Cybersecurity, Opportunities, Prevention.